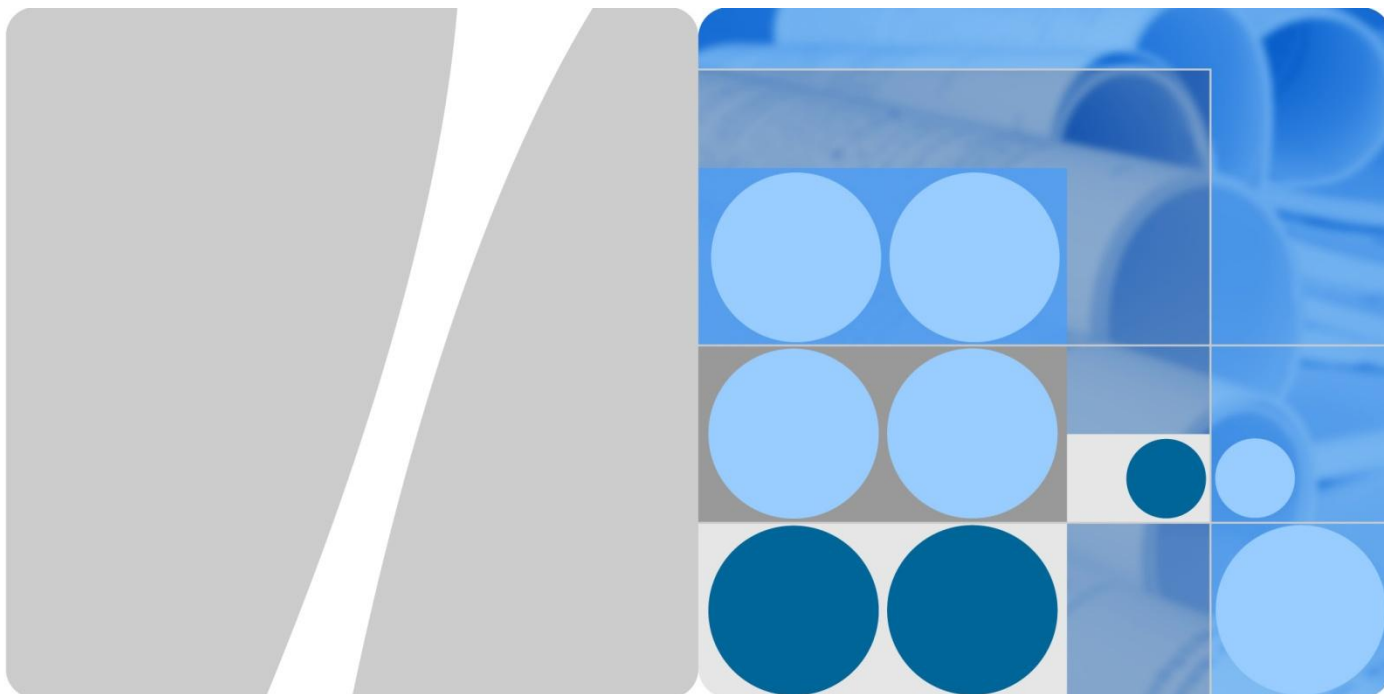




Huawei eSight V200R002C01 Operation Guide

Issue 02
Date 2012-09-11

Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

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

Email: support@huawei.com

About This Document

Related Versions

This document describes basic concepts and operations of eSight. This document includes operation processes on security management, resource management, topology management, report management, NTA, service management and so on.

This document provides guidance on how to use eSight.

Intended Audience

The intended audiences of this document are:

- Network Monitoring Engineer
- Data Configuration Engineer
- NM Administrator
- System Maintenance Engineer

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 that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Symbol	Description
 TIP	Indicates a tip that may help you solve a problem or save you time.

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 .
<i>Italic</i>	Command arguments are in <i>italic</i> .
[]	Items (keywords or arguments) in square brackets [] are optional.
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x y ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x y ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x y ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A maximum of all or none can be selected.

GUI Conventions

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 versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 02 (2012-09-11)

Modified:

5 Fault Management

8 NE Management

9 Network Traffic Analysis

Issue 01 (2012-07-30)

This issue is used for first office application.

<i>Author/ID</i>	<i>zhengyuyan/00101709</i>
<i>Department</i>	<i>Enterprise Design Dept</i>
<i>Group Email Address</i>	<i>ask_eSight_MKT@huawei.com</i>
<i>Co-author/ID</i>	
<i>Approver/ID</i>	<i>liyi /64206</i>
<i>Release Data</i>	<i>2012-09-27</i>

Contents

About This Document.....	ii
1 Getting Started.....	1
1.1 Basic Commissioning.....	1
1.1.1 Commissioning Process	1
1.1.2 Verifying Ports	3
1.1.2.1 Service Ports	3
1.1.3 Determining License Capacity	3
1.1.4 Client Running Environment Required for the eSight	5
1.1.5 Logging In to and Out of the eSight.....	5
1.1.6 Main Page	7
1.1.7 Create User Accounts and Configure the Basic Information	8
1.1.8 NE Adding	14
1.1.8.1 Setting SNMP Parameters on the NE Side	14
1.1.8.2 Adding NEs to eSight	15
1.1.8.3 Setting NE SNMP Parameters on the eSight Side	17
1.1.8.4 Setting NE Telnet Parameters on the eSight Side	19
1.1.9 Setting Trap Parameters on an NE	20
1.1.10 Back Up Device Configuration Files	21
1.1.11 Add a Lower-layer NMS	23
1.2 Basic Concepts	24
1.2.1 Basic Concepts of Security Management.....	24
1.2.2 Basic Concepts of Resource Management	29
1.2.3 Basic Concepts of Topology Management.....	30
1.2.4 Basic Concepts of Fault Management.....	32
1.2.5 Basic Concepts of Performance Management.....	34
1.2.6 Basic Concepts of Report Management	35
1.2.7 Basic Concepts of Ne Management	35
1.2.8 Basic Concepts of Service Management.....	36
1.2.8.1 Basic Concepts of IPSec VPN Management	36
1.2.9 Basic Concepts of Smart Configuration Tool.....	38

1.2.10 Basic Concepts of Backing Up and Restoring Device Configuration Files	38
1.2.11 Basic Concepts of User-Defined Devices Management.....	39
2 Security Management.....	41
2.1 Overview of Security Management Operations	41
2.2 Security Policy Management	43
2.2.1 Setting an Account Policy	44
2.2.2 Setting a Password Policy	46
2.2.3 Setting an Access Control Policy	47
2.2.3.1 Setting a Login Time Control Policy	47
2.2.3.2 Setting a Client IP Address Control Policy	49
2.2.4 Setting the Client to Be Logged Out Automatically.....	51
2.2.5 Changing the Password of an User	52
2.3 Creating Users and Assigning Rights	58
2.3.1 Setting a User-Defined Managed Domain	58
2.3.2 Creating a Role	60
2.3.3 Creating Users.....	67
2.4 Monitoring the User	73
2.4.1 Monitoring User Sessions	73
2.4.2 Forcing a User to Log Out	76
2.5 Example: Typical Security Management Operations	77
3 Resource Management.....	81
3.1 Overview of Resource Management Operations.....	82
3.2 Creating a Subnet	84
3.3 Auto Discovery for NEs	86
3.4 Creating an NE Manually.....	88
3.5 Importing NEs Manually in Batches	90
3.6 Adjusting the Relationships Between NEs and Subnets.....	92
3.7 Adjusting the Relationships Between Subnets	94
3.8 Physical Resource Management.....	95
3.9 Creating an SNMP Template.....	96
3.10 Link Management	98
3.11 Electronic Labels Management	101
3.12 Example: Typical Resource Management Operations.....	102
4 Topology Management	105
4.1 Overview of Topology Management Operations	105
4.2 Physical Topology Management	107
4.2.1 Designing a Physical View.....	107
4.2.2 Adjusting a Physical View	108
4.2.2.1 Setting the Topology Background.....	108

4.2.2.2 Changing the Position of an NE.....	109
4.2.2.3 Changing the Position of a subnet	111
4.2.2.4 Deleting an NE or Subnet	113
4.2.2.5 Rearranging Topology Objects in a Physical View	114
4.2.3 Browsing a Physical View	116
4.2.3.1 Searching for a Topology Object	116
4.2.3.2 Zooming In or Out on a Physical View.....	118
4.2.3.3 Saving Changes to Topology Object Positions in the Physical View.....	119
4.2.3.4 Viewing the Physical View in Full Screen or Aerial View.....	120
4.2.3.5 Showing Topology Legends.....	122
4.2.3.6 Setting a Device Label.....	123
4.2.3.7 Printing the Physical View	124
4.2.3.8 Exporting the Physical View.....	125
4.2.4 Example: Typical Topology Management Operations	126
4.3 IP Topology Management	128
4.3.1 IP Topology Management Functions.....	128
4.3.2 IP Topology Operations	129
4.3.3 Example: Typical Operations for IP Topology Management	133
5 Fault Management	135
5.1 Overview of Fault Management Operations	135
5.2 Setting Remote Alarm Notifications	138
5.2.1 Procedure for Setting Remote Notification	138
5.2.2 Setting the Email Server	140
5.2.3 Setting the SMS Server	141
5.2.4 Setting a Notification Template.....	144
5.2.5 Setting a Recipient Group	145
5.2.6 Setting a Remote Alarm Notification Rule	147
5.2.6.1 Creating a Remote Notification Rule by Alarm Severity.....	148
5.2.6.2 Creating a Remote Notification Rule by Alarm.....	150
5.3 Setting a Fault Monitoring Rule	156
5.3.1 Creating an Alarm Mask Rule.....	156
5.3.2 Setting the Alarm Sound	163
5.3.3 Creating an Alarm Filter Rule	165
5.3.4 Redefining the Severity of an Alarm.....	167
5.4 Monitoring Alarms	170
5.4.1 Browsing Current Alarms	170
5.4.2 Monitoring Alarms on the Alarm Panel	174

5.4.3 Monitoring Alarms in the Physical View	175
5.4.4 Monitoring Alarms by Using the NE Management Window	176
5.4.5 Handling Alarms	177
5.4.5.1 Procedure for Handling Alarms	177
5.4.5.2 Viewing the Details about an Alarm	179
5.4.5.3 Acknowledging an Alarm	181
5.4.5.4 Clearing an Alarm	182
5.5 Alarm Analysis	184
5.5.1 Querying a Historical Alarm	184
5.5.2 Querying an Event	186
5.5.3 Querying a Masked Alarm	187
5.6 Example: Typical Fault Management Operations	188
6 Performance Management.....	192
6.1 Overview of Performance Management Operations	192
6.2 Performance Monitoring Process	194
6.3 Setting Performance Monitoring	196
6.3.1 Configuring a Performance Monitoring Template	196
6.3.2 Creating a Performance Monitoring Task	199
6.3.3 Adding a Performance Monitoring View	207
6.4 Browsing Performance Monitoring Data	211
6.4.1 Querying Real-Time Performance Data	211
6.4.2 Querying Historical Performance Data	212
6.4.3 Viewing the Performance Data of an NE	217
6.5 Example: Typical Performance Management Operations	220
7 Report Management	222
7.1 Overview of Report Management Operations	223
7.2 Setting the Report System Parameters	224
7.2.1 Setting the Busy Time Range	224
7.2.2 Configuring the Report System	225
7.3 Creating a Report	226
7.4 Viewing Reports	229
7.5 Viewing Quick Reports	230
7.6 Maintaining the Report System	232
7.6.1 Modifying a Report Task	232
7.6.2 Managing Report Storage Space	233
7.6.3 Managing Report Task Status	235
8 NE Management.....	237
8.1 Overview of NE Management Operations	237
8.2 Querying an NE	239

8.2.1 Querying Basic Information.....	239
8.2.2 Viewing the Device Panel	240
8.2.3 Querying the Alarm List	242
8.2.4 Querying Performance Status	245
8.3 Configuring an NE	246
8.3.1 Logging In to Web NMS	246
8.3.2 Setting Protocol Parameters	247
8.3.2.1 Setting NE Telnet Parameters on eSight	248
8.3.2.2 Setting NE SNMP Parameters on eSight	249
8.3.3 Managing Interfaces.....	251
8.3.3.1 Understanding an Interface	251
8.3.3.2 Configuring Interfaces	252
8.3.3.3 Querying Interface Parameters	254
8.3.4 Querying IP Addresses.....	255
8.3.5 Restoring a Configuration File.....	257
9 Network Traffic Analysis	259
9.1 NTA Panorama	260
9.2 NTA Overview	260
9.3 NTA Overview and Configuration Prerequisites.....	261
9.4 Monitoring Network Traffic.....	263
9.4.1 Viewing Dashboard.....	264
9.4.2 Traffic Analysis	265
9.5 Creating a Traffic Report.....	267
9.6 Creating Traffic Forensics Tasks	270
9.7 Configuring NTA	272
9.7.1 Configuring a Collector	272
9.7.2 Setting Protocols	273
9.7.3 Configuring Application	274
9.7.4 Configuring DSCP	276
9.7.5 Configuring an IP Group.....	276
9.7.6 Configuring an Application Group.....	277
9.7.7 Configuring a DSCP Group	278
9.7.8 Configuring an Interface Group	280
10 Service Management	282
10.1 IPsec VPN Service Monitoring and Management	282
10.1.1 IPsec VPN Application.....	282
10.1.2 Overview of IPsec VPN Management Operations	283
10.1.3 Creating a Network Domain	284
10.1.4 Discovering the IPsec VPN Service in the Network Domain.....	285

10.1.5 Monitoring the IPSec Service	286
10.1.5.1 Viewing the Topology Structure of the IPSec Service	286
10.1.5.2 Querying the Running State of the IPSec VPN Service.....	288
10.2 WLAN Management	288
10.2.1 Basic Concepts.....	289
10.2.2 Network Scheme and Principle	289
10.2.3 Overview.....	294
10.2.4 Configuring the Log Function.....	296
10.2.5 Configuring Services.....	299
10.2.5.1 Configuring the WLAN Service in Wizard Mode	299
10.2.5.2 Setting Basic AC Information.....	303
10.2.5.3 Connecting an AP to a WLAN.....	305
10.2.5.4 Configuring an AP Profile.....	310
10.2.5.5 Configuring a RF Profile	313
10.2.5.6 Configuring an ESS Profile	315
10.2.5.7 Configuring an AP Region	318
10.2.5.8 Binding Profiles to an AP	321
10.2.6 Management and Maintenance	323
10.2.6.1 Viewing AC Information.....	324
10.2.6.2 Viewing AP Information	325
10.2.6.3 Browsing STAs	328
10.2.6.4 Browsing SSIDs Throughout the Network	330
10.2.6.5 Browsing Rogue APs	331
10.2.6.6 Browsing STA Access History	333
10.2.6.7 Managing Regions and Locations.....	334
10.2.6.8 Viewing the Service Topology	337
10.2.6.9 Viewing the Location Topology	339
10.2.6.10 Diagnosing Faults	344
10.2.6.11 Rectifying AP Faults	347
10.2.7 Example: Typical WLAN Management Operations	349
10.3 BGP/MPLS VPN Management	353
10.3.1 Understanding BGP/MPLS VPN	353
10.3.1.1 Terms	353
10.3.1.2 Functions.....	354
10.3.1.3 Application Scenarios	355

10.3.2 Overview	361
10.3.3 Automatic Discovery	363
10.3.3.1 Automatic Discovery Process	363
10.3.3.2 Discovering Services Automatically	364
10.3.3.3 Modifying Services	367
10.3.4 Monitoring Services	369
10.3.4.1 Viewing Service List	369
10.3.4.2 Viewing a Service Topology View	371
10.3.4.3 Managing Regions	375
10.3.4.4 Managing Alarms	377
10.3.4.5 Managing Performance	379
10.3.4.6 Managing Reports	381
10.3.4.7 Viewing L3VPN SLA Data	383
10.3.5 Diagnosing Service Faults	384
10.3.6 Example: Typical BGP/MPLS VPN Management Operations	387
10.4 SLA Management	390
10.4.1 What Is SLA?	390
10.4.1.1 SLA Terms	390
10.4.1.2 SLA Functions	391
10.4.1.3 SLA Default Settings and Device Configurations	392
10.4.2 Overview of SLA Management Operations	404
10.4.3 Configuring SLA Tasks	405
10.4.3.1 Creating an SLA Service	405
10.4.3.2 Creating an SLA Task	407
10.4.3.3 Quick Diagnosis	409
10.4.4 Monitoring SLA Tasks	411
10.4.4.1 Accessing the SLA Task Management Page	411
10.4.4.2 Viewing SLA Historical Data of an SLA Task	411
10.4.5 Typical SLA Applications	413
10.4.5.1 Example: Creating a Predefined Task	413
10.4.5.2 Example: Creating a User-Defined Task	413
11 Smart Configuration Tool	415
11.1 Overview	415
11.2 Functions	417
11.3 Function Panorama	418

11.3.1 Delivery by Template	418
11.3.2 Delivery by Plan Sheet.....	419
11.3.3 Delivery Record Management	420
11.4 Configuring Tasks	420
11.4.1 Template Management and Delivery.....	420
11.4.1.1 Creating a Template	420
11.4.1.2 Delivering a Template	422
11.4.2 Plan Sheet Management and Delivery	426
11.4.2.1 Exporting a Plan Sheet.....	426
11.4.2.2 Delivering a Plan Sheet.....	428
11.5 Examples	431
11.5.1 Example: Delivery by Template	432
11.5.2 Example: Delivery by Plan Sheet.....	432
12 Device Configuration File Management	434
12.1 Overview of Device Configuration File Management Operations.....	434
12.2 Setting FTP Parameters	436
12.3 Backing Up NE Configuration Files	438
12.3.1 Backing Up NE Configuration Files Automatically.....	438
12.3.1.1 Creating a Backup Task	438
12.3.1.2 Enabling a Backup Task.....	441
12.3.1.3 Maintaining a Backup Task.....	442
12.3.2 Backing Up NE Configuration Files Manually	444
12.4 Managing NE Configuration Files	445
12.4.1 Viewing an NE Configuration File.....	445
12.4.2 Browsing the Backup NE Configuration File List	447
12.4.3 Comparing NE Configuration Files	449
12.4.4 Setting NE Configuration Files to the Baseline File	451
12.4.5 Setting the Maximum Number of Backup NE Configuration Files	453
12.5 Restoring NE Configuration Files	454
13 User-Defined Device Management	458
13.1 Overview of user-defined device management	459
13.2 User-defined Device Functions	460
13.3 Customization Process	464
13.4 Discovering a User-defined Device.....	465
13.4.1 Creating a User-Defined Device Manually	465
13.4.2 User-Defined Device Auto-Discovery	467
13.4.3 Importing User-Defined Devices Manually in Batches	469
13.5 Customizing the Vendor Name and Device Type	471

13.6 NE Management Capability	473
13.6.1 Customizing SNMP Alarm Parameters	473
13.6.2 Customizing Performance Counters.....	476
13.6.3 Customizing a Device Configuration File.....	481
13.6.4 Customizing the Device Panel	485
13.7 Checking the Network Status of User-Defined Devices	488
13.7.1 Performing a Ping Test.....	488
13.7.2 Performing a Trace Test	490
13.7.3 Query Basic Interface Information.....	492
13.7.4 Viewing IP Address List.....	493
13.8 Invoking the Web NMS of User-Defined Devices	495
14 System Management	497
14.1 Overview of System Management Operations	497
14.2 Setting eSight Data Overflow Dump.....	499
14.2.1 Configuring a Log Overflow Dump Rule	500
14.2.2 Configuring an Alarm Overflow Dump Rule.....	501
14.2.3 Configuring a Performance Overflow Dump Rule	503
14.2.4 Configuring an SLA Overflow Dump Rule	505
14.3 Querying logs	507
14.3.1 Log Types.....	507
14.3.2 Querying a Security Log	508
14.3.3 Querying a System Log.....	510
14.3.4 Querying an Operation Log	512
14.4 Lower-Layer NMS	514
14.4.1 Lower-Layer NMS Management	514
14.4.1.1 Lower-Layer NMS Application	514
14.4.1.2 Lower-Layer NMS Function.....	515
14.4.2 Managing a Lower-Layer NMS	515
14.4.2.1 Adding a Lower-Layer NMS	516
14.4.2.2 Querying Lower-Layer NMS Information.....	516
14.4.2.3 Testing the Connectivity of Lower-Layer NMSs	517
14.5 Managing Licenses.....	518
14.5.1 Querying License Information About the eSight	518
14.5.2 Obtaining an ESN	520
14.5.3 Importing a License File	522
15 Routine Maintenance	524
15.1 Maintenance Item List.....	525
15.2 Obtaining Technical Support.....	525
15.3 Daily Maintenance	526

15.3.1 Browsing Current Alarms	526
15.3.2 Querying Security Logs	529
15.4 Weekly Maintenance	531
15.4.1 Checking the Disk Status of the eSight Server	531
15.4.2 Checking the Disk Space of the eSight Server	532
15.4.3 Checking Oracle Database Logs	533
15.4.4 Checking the Running Status of Anti-Virus Software.....	533
15.4.5 Checking the Logs of the OS	533
15.4.6 Checking MySQL Database Logs	534
15.5 Monthly Maintenance	535
15.5.1 Changing the Password of an eSight User	535
15.5.2 Checking the Server Time of the eSight.....	536
15.5.3 Releasing the Disk Space of the eSight Server	537
15.6 Quarterly Maintenance	537
15.6.1 Checking the Equipment Room Environment.....	538
15.6.2 Checking the Power Supply of the eSight Server	538
15.6.3 Checking Hardware and Peripherals of the eSight Server	539
16 FAQs	541
16.1 How Do I Solve the Problem When Internet Explorer 8 Displays a Message Indicating that No Alarm Sound Is Selected?	542
16.2 How to Solve the Problem That the Web Browser Displays a Message Indicating That the Security Certificate Is Incorrect During Login to the eSight?	542
16.3 How Do I Resolve the Problem That A Security Alarm Is Generated When Logging In to the eSight By Internet Explorer 8?.....	553
16.4 What Do I Do When a Few English Fields Cannot Be Displayed Completely During the Process of Accessing the eSight GUI in English by Mozilla Firefox in Chinese?	560
16.5 What Do I Do When Adobe Flash Player Provided by the eSight Cannot Be Installed in Internet Explorer?	563
16.6 How to Resolve the Problem that the Flash Plug-in Is Down When the eSight Flash Is Opened Using a Browser	564
16.7 What Do I Do When Arabic Characters Appear Garbled After Being Copied?	565
16.8 How Do I Resolve the Nesting Problems of the eSight Page after Clearing the Cache from Firefox?	566
16.9 How Do I Install an SSL Certificate for the Email Server?.....	567
16.10 How Do I Customize Connection Rules for Ports Required by eSight?	568
16.11 How Do I Solve the Problem When eSight Cannot Manage an NE Due to Junk Data Caused by Unexpected Database Stop?	576
16.12 How Do I Solve the Problem When the eSight GUI Fails to Display Properly and the GUI Displays Page-wide Code When I Log Out?.....	578
16.13 How Do I Set SNMP Parameters on a PC?	579
16.14 How Do I Prevent Problems Caused by eSight Server System Time Change?.....	590
16.15 When I Use IE8 to Import Sheets, the System Displays an Incorrect Path. How Do I Solve the Problem?	590
16.16 How Do I Solve the Service Session Failure That Occurs When I Log In to eSight?	591

A Glossary 593

1 Getting Started

About This Chapter

This topic describes the eSight commissioning process, functions provided by eSight, and eSight main page.

[1.1 Basic Commissioning](#)

[1.2 Basic Concepts](#)

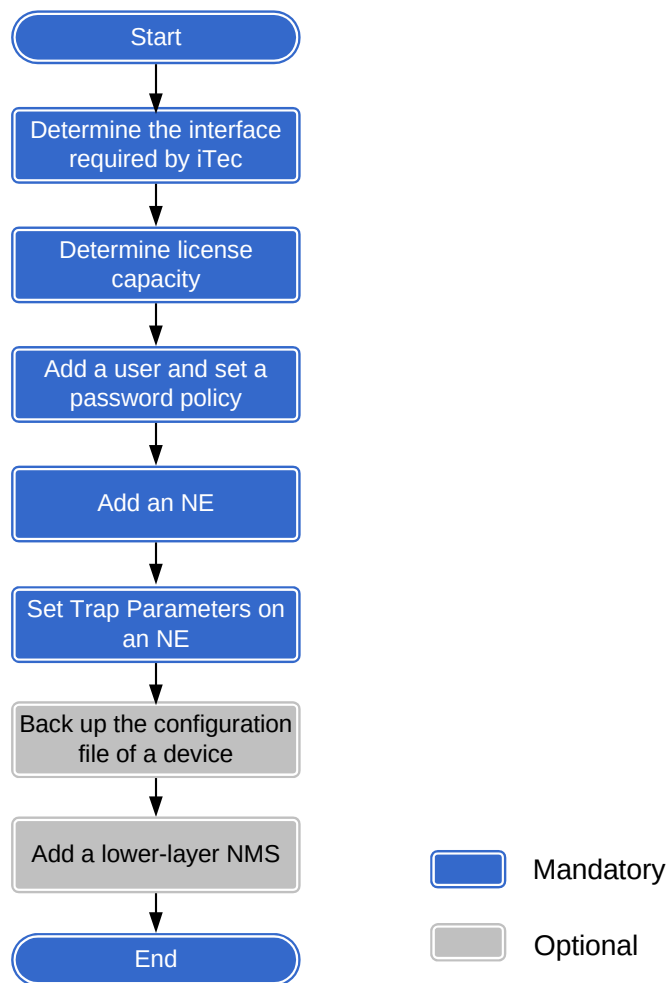
Before using the eSight, you need to be familiar with the basic concepts of each module of the eSight. The modules are the resource, topology, security, fault, and performance modules. The basic concepts of these modules help you quickly and accurately operate the eSight.

1.1 Basic Commissioning

1.1.1 Commissioning Process

This topic verifies eSight basic functions.

[Figure 1-1](#) shows the commissioning process.

Figure 1-1 Commissioning process**Table 1-1** Commissioning process description

Operation	Remarks
1. 1.1.2 Verifying Ports	Verify that the required ports in the eSight port list are enabled so that eSight can use these ports properly.
2. 1.1.3 Determining License Capacity	Check the license capacity so that eSight can function properly.
3. 1.1.7 Create User Accounts and Configure the Basic Information	Create user accounts for maintenance personnel and configure the basic information and operation rights of each user. Assign different maintenance personnel with different operation rights to enhance operation security.
4. 1.1.8.2 Adding NEs to eSight	Add network elements (NEs) to eSight and manage the NEs.

Operation	Remarks
5. 1.1.9 Setting Trap Parameters on an NE	A trap receiver is used to receive trap messages of the NE. This topic describes how to set trap parameters on the NE. The NE actively sends fault information to the eSight through trap packets defined by SNMP after the trap function is configured.
6. (Optional) 1.1.10 Back Up Device Configuration Files	Back up device configuration files in a timely manner so that you can use the device configuration files for restore in case of accidents or misoperations. This helps enhance the configuration file security.
7. (Optional) 1.1.11 Add a Lower-layer NMS	You can define lower-layer NMSs or each upper-layer NMS to implement the function of monitoring performance and alarms of lower-layer NMSs.

1.1.2 Verifying Ports

Verify that the required ports in the port list are enabled so that eSight can use these ports properly.

1.1.2.1 Service Ports

This topic describes the service ports used by the eSight. The eSight allocates port numbers for services in a centralized manner, which avoids port conflicts. All ports communicate between the server and client over Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

eSight Service Ports

In the firewall security policy, traffic is filtered based on IP addresses and TCP or UDP port numbers.

TCP or UDP port numbers can be used to separate data packages and transmit data packages to appropriate application programs.

TCP or UDP port numbers range from 0 to 65535, and the range is classified into the following three segments:

- Port 0 to port 1023 are used to identify some standard services such as FTP, Telnet, and Trivial File Transfer Protocol (TFTP).
- Port 1024 to port 49151 are allocated to the registered application processes by the Internet Assigned Number Authority (IANA).
- Port 32768 to port 65535 can be dynamically allocated to any applications as private port numbers.

For details about eSight service ports, see the *eSight Communication Matrix*.

1.1.3 Determining License Capacity

Determine whether the license capacity meets the requirements of the existing network.

Prerequisites

You have imported a license file into eSight.

Context

Table 1-2 describes the license information.

Table 1-2 License information

Item	Attribute	Description	Example
Basic License Information	Validity period	Date when the license file expires	2011-04-14
	Reminding days ahead	An alarm reporting that the license file will expire after the specified days is generated, and you need to import a new license file.	15
License Resource Control	Resource Name	Name of the resource for license file management	Client Count
	License Usage	Resource usage for license management	30/2000 indicates that the number of resources managed by the license is 2000, and 30 resources are used.
	Major Alarm Threshold	An alarm is generated if the resource usage exceeds the specified alarm threshold.	80%
License Function Control	Function Name	Functions provided by eSight	SLA Manager Function
	Supported or Not	Whether the function is supported by the license file	Supported

Procedure

Step 1 Choose **System** > **License Management**.

The information about the current license file is displayed.

----End

1.1.4 Client Running Environment Required for the eSight

A personal computer (PC) must meet requirements of the client running environment so that users can operate the eSight properly.

Table 1-3 describes the client running environment required for the eSight.

Table 1-3 Client running environment required for the eSight

Configuration Item	Minimum Configuration Requirements
Hardware configuration requirements	Inter(R) Pentium(R) Dual CPU E2180 @ 2.00GHz, 2 GB
Operating system	Windows XP, Windows 7 or Windows Server 2008
Browser	Mozilla Firefox 3.6 or Windows Internet Explorer 8.0 NOTE • If Windows Internet Explorer 8.0 is used, you need to set the browsing mode by performing the following steps: • Open Windows Internet Explorer 8.0, and choose Tools > Compatibility View Settings from the main menu. • In the Compatibility View Settings dialog box, deselect Include updated website lists from Microsoft, Display intranet sites in Compatibility view, and Display all websites in Compatibility View. • Click Close. • On a PC that runs Windows Server 2008, if you cannot use Windows Internet Explorer 8.0 to log in to the eSight installed on another server, disable certain security policies of the operating system. • eSight does not support the refresh function provided by the browser.
Resolution	1024 x 768

1.1.5 Logging In to and Out of the eSight

This topic describes how to log in to and log out of the eSight.

Prerequisite

eSight works in browser/server mode, the connection between the current PC and the eSight server is normal, and the eSight server works properly.

Context

The eSight provides an initial user name **admin** and user password Changeme123. The user has the operation rights of all managed objects of the eSight.



CAUTION

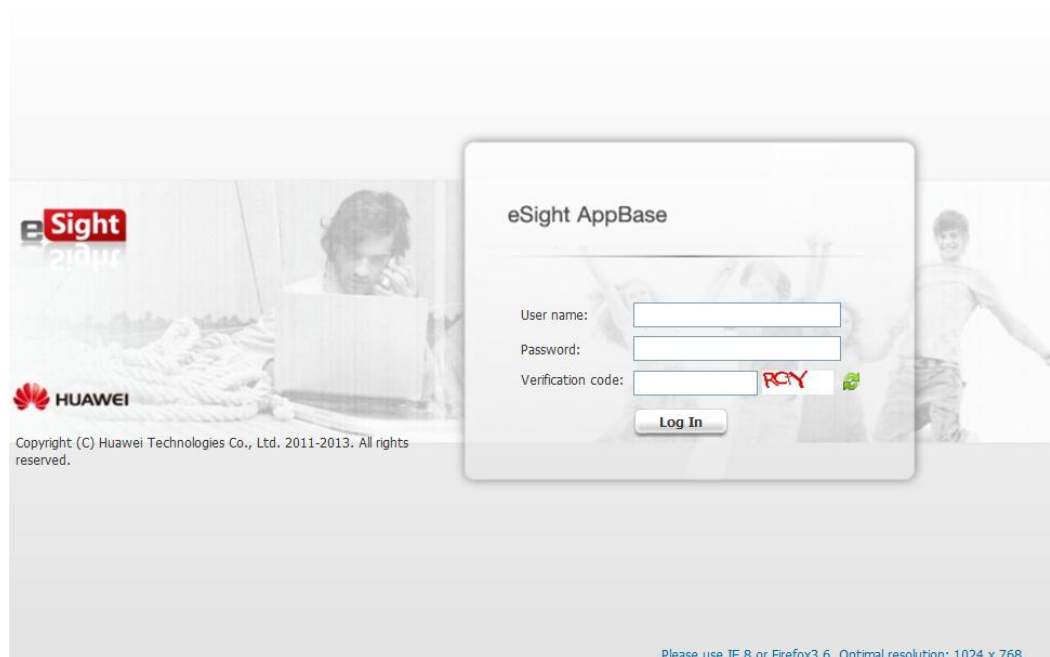
- After the first successful login, you need to change the password to ensure the eSight security.
- On one PC, only one user can log in to the eSight in one browser. For example, if user A has logged in to the eSight, user B will automatically switch to the operation page of user A even if user B enters its user name and password on the login page.
- If a rollback is required during operations, you are not advised to use the browser's back button. Otherwise, the current data is lost and the eSight exits.

Logging In to the eSight

Step 1 Open a browser window. In the address bar, type `http://eSight server IP address :eSight server port number/` (for example, `http://12.10.10.1:8080/`), and press **Enter**.

The eSight login page is displayed.

Figure 1-2 login page



NOTE

- The default port number of the eSight is **8080**.

Step 2 Enter the **User name**, **Password** and **Verification code**.

Step 3 Click **Log In**.



NOTE

- When the password will expire, you are prompted to change the password within the password expiration warning days.
- If the number of online users reaches the maximum allowed by the license, the eSight displays a message indicating that you cannot log in. In this case, contact the system administrator.
- When you log in to the eSight, if the system displays a message indicating an invalid license, you can update the license, log in, or apply for a new license by obtaining the electronic serial number (ESN) in the displayed dialog box. For details about how to update a license and how to obtain an ESN, see [14.5.3 Importing a License File](#) and [14.5.2 Obtaining an ESN](#) respectively.

----End

Logging Out of the eSight

Step 1 Click  in the upper right corner of the eSight.

Log out of the eSight.

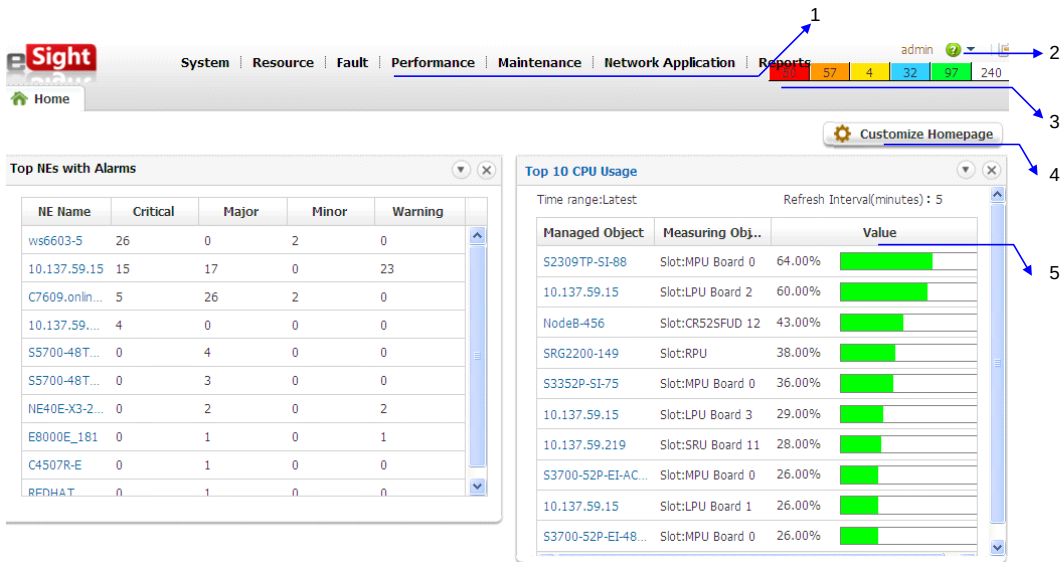
----End

1.1.6 Main Page

This topic describes eSight main page.

[Figure 1-3](#) shows eSight main page.

Figure 1-3 eSight main page



1. Main menu	The menu bar contains System, Resource, Fault, Performance, Maintenance, Network Application, and Reports.
2. Common information and buttons	Displays the current user name, eSight help button, and logout button.

3. Alarm indicator area	Displays number and levels of alarms.
4. Button for adding a Portal	User-defined home page.
5. Statistical area	Display statistical graphs. The following statistics are collected: • Top NEs with Alarms • Top 10 CPU Usage • Top 10 Memory Usage • Top 10 Inbound bandwidth usage on interface • Top 10 outbound bandwidth usage on interface • Subnets • Lower-Layer NMs

1.1.7 Create User Accounts and Configure the Basic Information

This topic describes how to create users. When the default user of the eSight cannot meet the network management requirements, you can create users to ensure security of the eSight and facilitate network management.

Prerequisite

- You have the operation rights for **Security Management**.
- You learn about the user account policy and password policy.

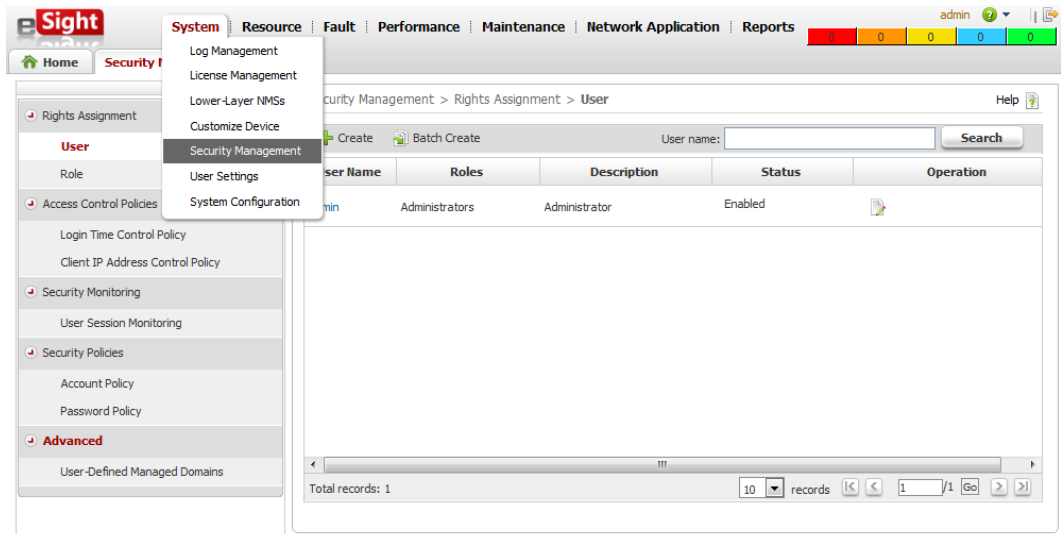
For details about how to set an account policy or a password policy, see [2.2.1 Setting an Account Policy](#) and [2.2.2 Setting a Password Policy](#).

Context

- Users can be created one by one or in batches. To create users in batches, import a template in .xls format to the eSight.
- A maximum of 1000 users can be created. When the number of users to be created reaches 1000, the eSight stops creating the remaining users.
- You must manually set the user name and password. For the other properties, you can use default values or set them after you create the user account successfully.

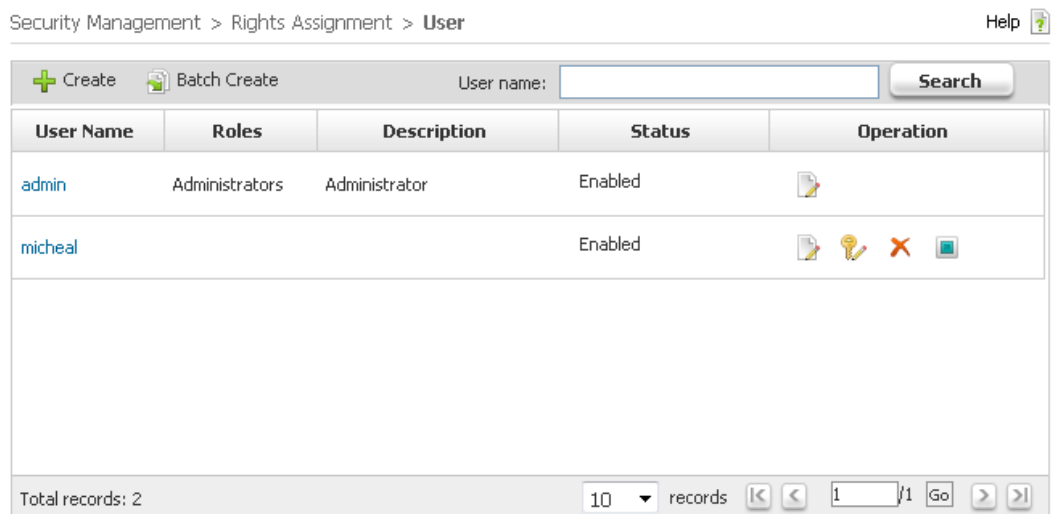
Procedure

Step 1 Choose **System > Security Management** from the main menu.

Figure 1-4 Security management

Step 2 In the **Security Management** window, choose **Rights Assignment > User**.

Step 3 On the **User** page, select a method of creating users.

Figure 1-5 Creating users

- **Create users one by one.**

If only a few users are required, create the users one by one.

1. Click **Create**.
2. On the **Create User** page, set the basic information.
 - a. In the **Basic Info** step, set **User name**.

Figure 1-6 Setting basic information

Security Management > Rights Assignment > User > **Create User** Help ?

Progress: Basic Info Roles Access Control Policies

* User name:	user_a
* Password:	Set Password
Account status:	☒ Enabled ☐ Disabled
Description:	area_a

Next Cancel

- b. Click **Set Password** next to **Password**. In the displayed window, set **Password** and **Confirm password**.

Figure 1-7 Setting a password

* Password:	••••••••
* Confirm password:	••••••••

OK Cancel

The password must meet the following rules:

- 1, The password is different from the user name.
- 2, The length ranges from 6 to 32 characters.
- 3, The number of occurrences of a character in a password cannot exceed 3.
- 4, The password contains uppercase and lowercase letters and digits.

- c. Set **Account status** to **Enabled**.
- d. Click **Next**.
3. On the **Create User** page, set a role for the user. The user has the management rights and operation rights of the role.
 - a. In the **Roles** step, select the role.

Figure 1-8 Selecting the role

Security Management > Rights Assignment > User > **Create User** Help ?

Basic Info Roles Access Control Policies

Select roles:

☐	Role Name	Description
☐	Administrators	Administrator role
☒	role_a	own the Security Management rights of area_a

Total records: 2

**NOTE**

In the **Role Name** column, click the required role name. In the **View Role** dialog box, view the details of the role.

b. Click **Next**.

4. On the **Create User** page, set an access control policy for the user. The user can login the eSight by using a specified IP address within the specified period of time.
 - a. In the **Access Control Policies** step, select a login time control policy and an IP address range.

Figure 1-9 Setting access control policies

Security Management > Rights Assignment > User > **Create User** Help ?

Basic Info Roles Access Control Policies

Select a time control policy: + Create

	Policy	Description	Start and End Dates	Daily start and end times	Week
☒	Default Policy	The default policy allows you to log in at any time.	--	00:00~23:59	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
☐	Time_policy_a		2012-07-10~2013-07-10	09:00~18:30	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Total records: 2

Select a range of IP addresses you access: + Create

☒	IP Address Range	Description
☒	12.64.54.25~23.64.54.255	IP_policy_a

Total records: 1

Previous Finish Cancel

**NOTE**

- If the required login time control policy does not exist in the **Policy** list, you can click **Create** to create it. For details about how to create a login time control policy, see [2.2.3.1 Setting a Login Time Control Policy](#).
- If the required client IP address control policy does not exist in the **IP Address Range** list, you can click **Create** to create it. For details about how to create a client IP address control policy, see [2.2.3.2 Setting a Client IP Address Control Policy](#).

b. Click **Finish**.

- **Create users in batches.**

If a large number of users are required, create the users in batches to improve operation efficiency.

1. Click **Batch Create**.
2. On the **Batch Create Users** page, click **Template.xls** next to **Download template** to download the template to a local disk.

Figure 1-10 Creating users in batches

Security Management > Rights Assignment > User > **Batch Create Users** Help 

 The maximum allowable number of users in the system is 1000, you can import 997 users.

Download template: [Template.xls](#)

* Upload user information:   

Operation result

User Name	Disable or Not	Description	Role	Time Profile	Terminal Profile	Import Result
No record.						

- Open the template on the local disk, enter the user information, and save the template.

**NOTE**

A user cannot be created if the user information is incorrect.

- On the **Batch Create Users** page, click  next to **Upload user information** to import the template saved on the local disk.

You can click  to remove the selected template and select another one.

- Click  to upload the template.

The eSight automatically creates users based on the user information in the template.

- In the **Operation result** dialog box, confirm the result of creating users in batches, and click **OK**.

The detailed information about the created users is displayed in the operation result list.

**NOTE**

You can view user details in the user list on the **User** page.

----End

Follow-up Procedure

The following table describes the operations that you can perform on the **User** page after you create a user.

User Maintenance Operation	Procedure
View user information	You can learn about the details of a user. In the User Name column, click the required user name. On the View User page, view the details of the user.
Modify user information	You can modify user information as required. - Click  in the Operation column where the required user information is located, and then modify it. - On the Modify User page, modify the settings of

User Maintenance Operation	Procedure
	Basic Info, Roles, and Access Control Policies. 3. Click OK .
Delete a user	You can delete an unused user. 1. Click  in the Operation column where the required user information is located. 2. In the Confirm dialog box, click Yes .
Reset password	If a user forgets the password when logging to the eSight, the user can use the new password to log in after the password is reset. 1. Click  in the Operation column where the required user information is located. 2. In the displayed window, set New password and Confirm password based on the password rules. 3. Click OK .
Enable a user	If an account is not used for a long time and maximum number of days the account is not used continuously is reached, the account is disabled. To use the account again, you can enable the user account. Click  in the Operation column where the required user information is located.
Disable a user	You can disable a user account when you do not use the user account. Click  in the Operation column where the required user information is located.

1.1.8 NE Adding

This topic describes how to add NEs to eSight and manage them.

1.1.8.1 Setting SNMP Parameters on the NE Side

Before creating an NE on eSight, you must set the SNMP parameters on the NE side on the command-line interface (CLI).

Context

The prerequisites for eSight to detect and manage NEs over the SNMP protocol are as follows:

- The SNMP parameters are correctly configured on the NE side.
- The SNMP parameters configured on the eSight side are the same with those configured on the NE side.

Procedure

Step 1 Run the **system-view** command to open the system view.

Step 2 Run the **snmp-agent** command to enable the SNMP Agent service.

Step 3 For the SNMPv1/v2c, perform this step. For the SNMPv3, go to [Step 4](#).

1. Run the **snmp-agent sys-info version { { v1 | v2c }* }** command to set the SNMP version.
2. Run the following command to set **read community name**:
snmp-agent community read community-name [[mib-view view-name] | [acl acl-number]]*
3. Run the following command to set **write community name**:
snmp-agent community write community-name [[mib-view view-name] | [acl acl-number]]*

Step 4 For the SNMPv3, perform this step.

1. Run the **snmp-agent sys-info version v3** command to set the SNMP version.
2. Run the following command to set an SNMP user group:
snmp-agent group v3 group-name [authentication | privacy] [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]
3. Run the following command to add a user into the SNMPv3 user group.
snmp-agent usm-user v3 user-name group-name [[authentication-mode { md5 | sha } password] [privacy-mode des56 password]] [acl acl-number]

----End

Follow-up Procedure

Run the following commands to check SNMP parameters.

- In SNMPv1/v2c, run the **display snmp-agent community [read | write]** command to view the read-write community.
- In SNMPv3, run the **display snmp-agent group** command to view the configured user group and run the **display snmp-agent usm-user** command to view the configured user.

1.1.8.2 Adding NEs to eSight

If you want a few different types of NEs to access the eSight, you can create these NEs one by one.

Prerequisites

You have the operation rights for **Access Resource**.

Procedure

Step 1 Choose **Resource > Add Device** from the main menu.

Figure 1-11 Adding Device

The screenshot shows the 'Add Device' page in the Huawei eSight interface. The left sidebar lists various resource categories, with 'NE Resources' expanded. A dropdown menu is open under 'Resource Management', highlighting 'Add Device'. The main content area contains a form for adding a new device. The form includes fields for IP address, Subnet, Name, SNMP version (V2c), Read community (public), Write community (private), Port (161), Time-out period (3), Telnet optional settings (Protocol Type: Telnet, Authentication mode: No authentication, Port: 23, Password, Timeout interval: 60), and buttons for OK, Cancel, and Apply.

Step 2 On the **Add Device** page, configure basic information about the NE to be created and SNMP parameters.

**NOTE**

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. To add an SNMP template, see [3.9 Creating an SNMP Template](#).

Figure 1-12 Setting SNMP parameters

The screenshot shows the 'Basic Information' and 'SNMP' sections of the 'Add Device' page. The 'Basic Information' section includes fields for IP address (10.137.59.10), Subnet (/8), and Name. The 'SNMP' section includes a 'Select Protocol Template' button, SNMP version (V2c), Read community (public), Write community (private), Port (161), Time-out period (3), and a 'Telnet(optional)' section with Protocol Type (Telnet), Authentication mode (No authentication), Port (23), Password, and Timeout interval (60).

Step 3 Click **OK**.

**NOTE**

Click **Apply** to create more NEs.

- If the NE is created successfully, the NE is displayed in the list.
- If the NE cannot be created, the **Error** dialog box is displayed, indicating the reason for the failure. Click **OK** to set the parameters again.

----End

1.1.8.3 Setting NE SNMP Parameters on the eSight Side

When eSight and an NE communicate over SNMP and the SNMP parameters on the NE change, you must set the NE SNMP parameters concurrently on eSight.

Prerequisites

The SNMP parameters on eSight and the NE are the same.

A device is added to eSight.

Context

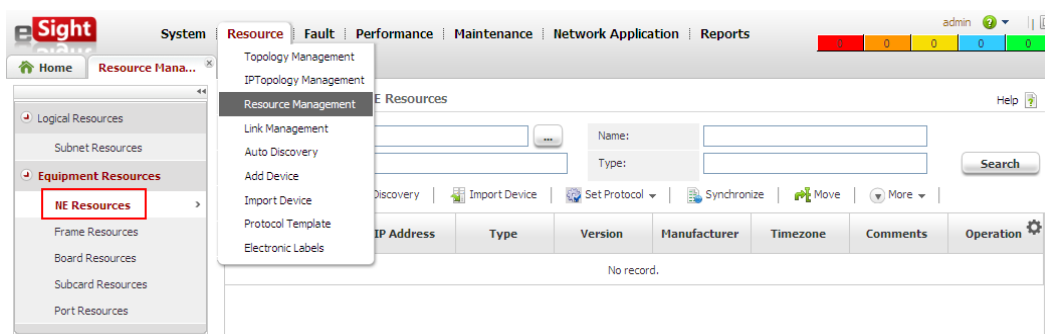
eSight accesses a managed NE over SNMP. When you manually create an SNMP NE or an SNMP NE is automatically created, eSight adapts a specified NE by using the default SNMP profile to determine the SNMP parameters supported by the managed NE. If adaptation is successful, the default profile is the SNMP parameters for the NE configured on eSight. The operations on the NE must be based on the SNMP parameters. When the SNMP parameters for NE access change, the SNMP parameters for a specified NE must be changed accordingly.

Procedure

Step 1 Access the NE manager page.

1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

Figure 1-13 Resource Management



Step 2 In the navigation tree on the left, choose **Protocol Parameters** > **SNMP Parameters**.

Figure 1-14 SNMP Parameters

The screenshot shows the 'SNMP Parameters' configuration window in Huawei eSight. The left sidebar has a tree view with the following items: View, Basic Information, Device Panel, Alarm List, Performance Status, Device Config, Web NMS, Interface Manager, IP Address, Configuration File, Protocol Parameters, Telnet Parameters, and SNMP Parameters (highlighted with a red box). The main configuration area on the right contains the following fields:

Name:	1220-10
SNMP version:	V2c
* Read community:	public
Write community:	private
* NE port:	161
* Timeout interval (s):	4
* Resending times:	3

At the bottom right of the main area are two buttons: 'Test' and 'Apply'.

Step 3 On the right of the window, set the SNMP parameters.

- **SNMP version:** Currently, the SNMPv1, SNMPv2c, and SNMPv3 versions are supported. The SNMPv3 version is applied in the scenario requiring high parameter security level.
- **Read community:** The read community name for eSight to send a read request to an NE. The read operation is available when the read community name is the same as that acknowledged by the NE.
- **Write community:** The write community name for eSight to send a write request to an NE. The write operation is available when the write community name is the same as that acknowledged by the NE.
- **Timeout interval(s):** The time when eSight waits for a response for an operation request.
- **Resending times:** The maximum number of times for eSight to resend an operation requests when eSight configures SNMP parameters for an NE in the case that the timer expires. If the actual number of times exceeds this value, operation fails.
- **NE port:** SNMP communication port of the NE.
- **Security name:** NE user name used for accessing the NE.
- **Context name:** Name of the environment engine.
- **Context engine ID:** Uniquely identifies an SNMP engine. The ID must be used with the environment name to uniquely identify an SNMP entity environment. An SNMP packet is processed only when the transmit environment and the receive environment are matching. Otherwise, the SNMP packet is discarded.
- **Authentication protocol:** A protocol used for message verification. You can choose the HMACMD5 or HMACSHA protocol or do not use any protocol. When you use the HMACMD5 or HMACSHA protocol, you must set an authentication password.
- **Privacy protocol:** Encryption protocol used for data encapsulation. You can choose the DES or AES encryption protocol or do not use encryption. When you use the DES or AES encryption protocol, you must set an encryption password.

Step 4 Click **Test**.

Step 5 After the test, click **Apply**.

----End

1.1.8.4 Setting NE Telnet Parameters on the eSight Side

When eSight and an NE communicate over Telnet and the Telnet parameters on the NE change, you must set the NE Telnet parameters concurrently on eSight.

Prerequisites

The Telnet parameters on eSight and NE are the same.

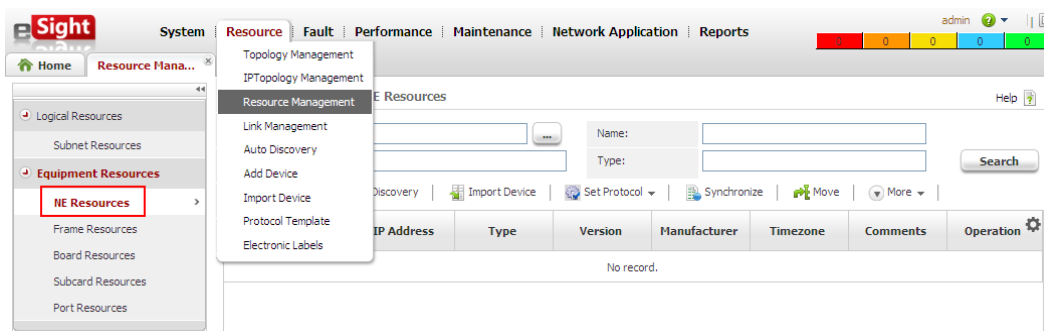
A device is added to eSight.

Procedure

Step 1 Access the NE manager page.

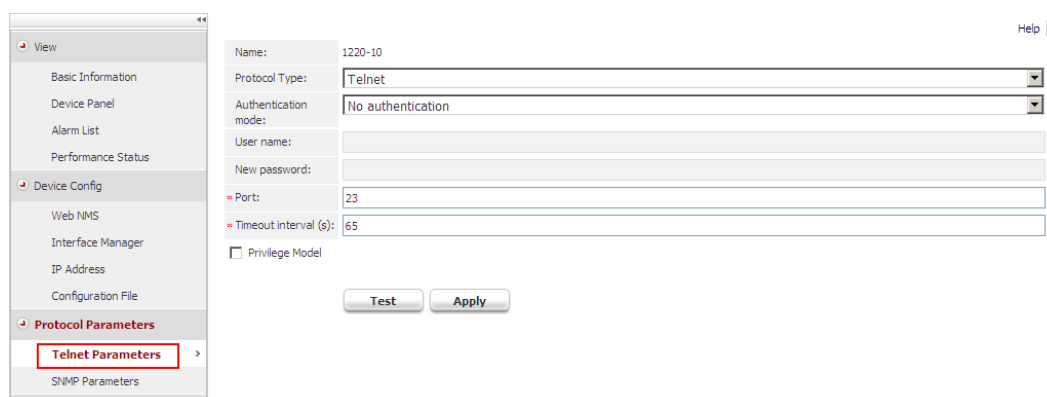
1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

Figure 1-15 Resource Management



Step 2 In the navigation tree on the left, choose **Protocol Parameters** > **Telnet Parameters**.

Figure 1-16 Telnet Parameters



Step 3 On the right of the window, set the Telnet parameters.

- Protocol type: The value can be Telnet or STelnet. STelnet is used in scenarios demanding high security.
- Authentication mode: authentication mode used by eSight to access network elements.
- Port: communication port. BY default, the Telnet port number is 23 and the STelnet port number is 22.
- Timeout interval (s): period for waiting for a response after eSight sends a request to a network element.
- Privilege model: right for eSight to deliver commands to network elements. When you select **Privilege model** and log in to a network element using Telnet or STelnet, eSight switches to the corresponding privilege model.
- Privilege level: A larger value indicates a higher priority. Users can use only the commands at the same or lower level than their own levels.

**NOTE**

Currently, the privilege model can only be set on Huawei devices.

Figure 1-17 Setting Telnet parameters

Name:	S9303_3
Protocol Type:	Telnet
Authentication mode:	Password
User name:	client001
* Password:	*****
* Port:	23
* Timeout interval (s):	60

TestApply

Step 4 Click **Test**.

Step 5 After the test, click **Apply**.

----End

1.1.9 Setting Trap Parameters on an NE

A trap receiver is used to receive trap messages of the NE. This topic describes how to set trap parameters on the NE. The NE actively sends fault information to the eSight through trap packets defined by SNMP after the trap function is configured.

Prerequisites

- Ensure that the source port of trap packets configured on the NE is consistent with the source port for sending packets configured on the NMS. Otherwise, the NMS cannot receive trap packets.

Context

The trap receiver is started on the eSight by fault.

Procedure

Step 1 Run the following command to enter the system view.

```
system-view
```

Step 2 Run the following command to enable the function of sending trap packets:

```
snmp-agent trap enable
```

Step 3 Run the following command to set the target host, that is, the NMS server:

```
snmp-agent target-host trap address udp-domain ip-address [ udp-port port-number |  
source interface-type interface-number { public-net | vpn-instance vpn-instance-name } ]  
params securityname security-string [ v1 | v2c | v3 [ authentication | privacy ] ]
```



NOTE

v1 | v2c | v3 in the command must be the same as the SNMP version used by the NE. Otherwise, the eSight cannot receive trap packets sent by the NE.

Using SNMPv3 is recommended because of its higher security than SNMPv1 and SNMPv2c.

Step 4 Run the following command to specify the source interface for sending trap packets:

```
snmp-agent trap source interface-type interface-number
```

```
----End
```

1.1.10 Back Up Device Configuration Files

You can back up NE configuration files manually for instant backup.

Prerequisites

eSight communicates with NEs normally.

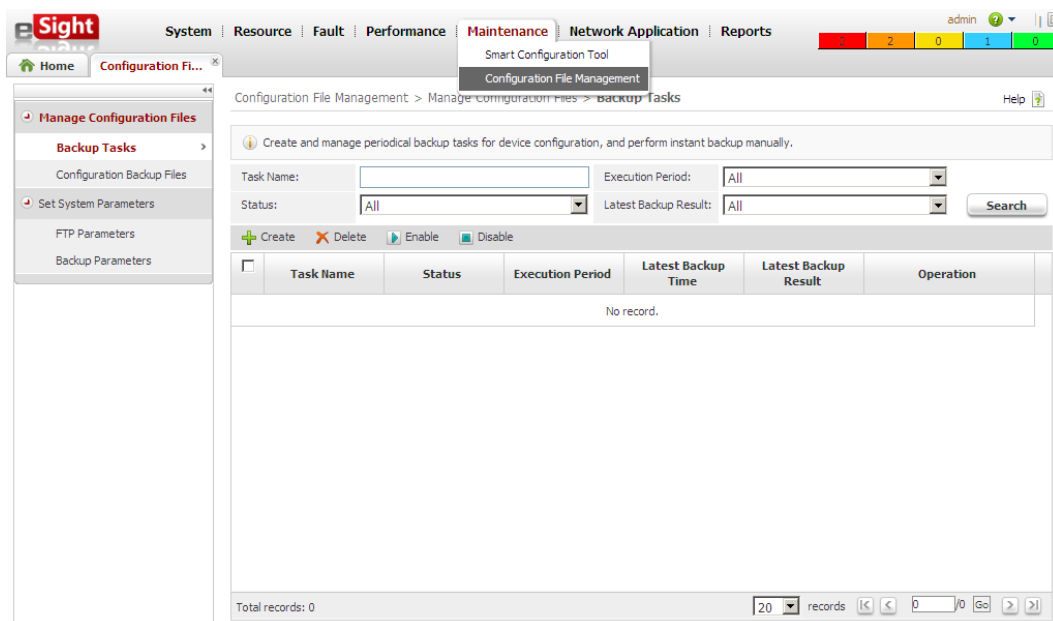
The FTP service is configured and started. For details on how to configure the FTP service, see [12.2 Setting FTP Parameters](#).

The Telnet parameters on eSight and the NE are set to be the same.

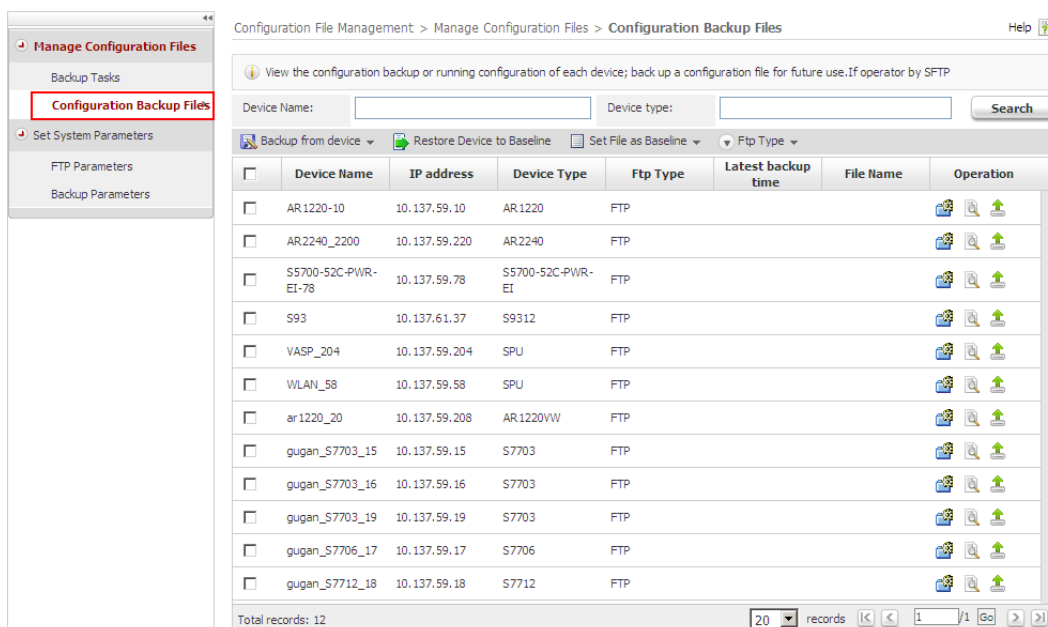
SNMP write permission is set.

Procedure

Step 1 Choose **Maintenance > Configuration File Management**.

Figure 1-18 Configuration File Management

Step 2 In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.

Figure 1-19 Configuration Backup Files

Step 3 Select one or more devices and choose **Backup from device > Backup Select** to back up the device information; If you want to back up all devices, choose **Backup from device > Backup All**. If you set search criteria, only the devices meeting the search criteria can be backed up.

----End

Result

When the configuration file used by an NE is the same as the backup configuration file, eSight remains the configuration file in use and discards the backup configuration file by default.

When the configuration file used by an NE is different from each backup configuration file and the number of backup configuration files reaches the maximum, eSight discards the earliest non-baseline configuration file by default.

1.1.11 Add a Lower-layer NMS

You can add a lower-layer NMS to enable eSight to manage it.

Prerequisites

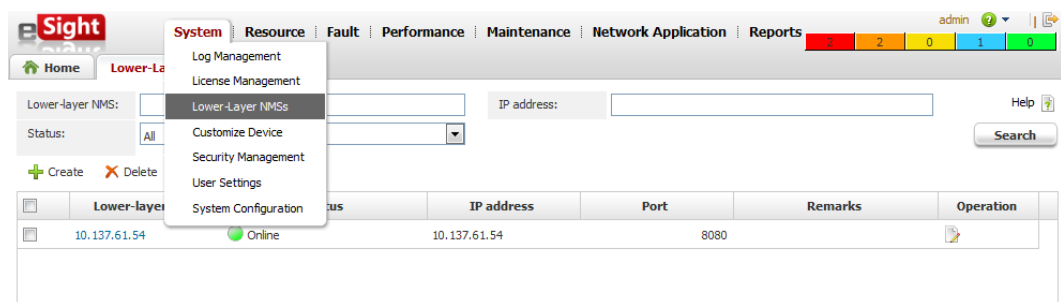
The lower-layer NMS runs properly.

A user has the permission to add a lower-layer NMS.

Procedure

Step 1 Choose **System > Lower-Layer NMSs** from the main menu.

Figure 1-20 Lower-Layer NMSs



Step 2 Click **Create**, and set **Lower-layer NMS**, **IP address**, **Port**, and **Remarks** in the window that is displayed.

Figure 1-21 New record

* Lower-layer NMS:	
* IP address:	
* Port:	
Remarks:	

Step 3 Click **OK**.

----End

1.2 Basic Concepts

Before using the eSight, you need to be familiar with the basic concepts of each module of the eSight. The modules are the resource, topology, security, fault, and performance modules. The basic concepts of these modules help you quickly and accurately operate the eSight.

1.2.1 Basic Concepts of Security Management

Before performing security management operations, you must familiarize yourself with the basic concepts related to security management, such as the user, role, operation rights, and access control. Understanding these concepts will help you avoid errors when performing security management operations.

Table 1-4 describes the basic concepts about security management.

Table 1-4 Basic concepts

Concept	Description
User	The user name and password of the user uniquely determine the operation management rights. The default super administrator is admin , who can manage all devices and possesses all the operation rights of the eSight.
Role	A role defines a set of users. Also, a role is a set of permission that provide a user with the ability to perform a predefined set of functions. Managing user rights based on roles makes rights management more effective. Administrators is the default super administrator role provided by the eSight, and the role has the operation rights of all managed objects.
Managed object	Managed objects are the devices managed by the eSight, including NEs and subnets.
Managed domain	A managed domain is a group of managed objects. Users can perform operations on the NEs in a managed domain only

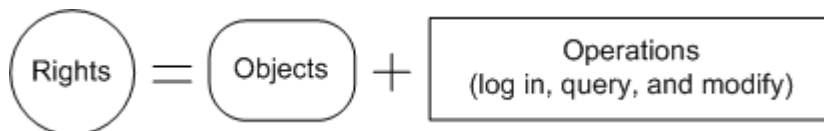
Concept	Description
	when they have the operation rights of the managed domain. NOTE You can create user-defined managed domains as required.
Operation rights	Operation rights mean the rights associated with a user to perform a specific operation. After the operation rights are assigned to a user, the user can perform a specific operation. Operation rights are related to managed domains. Users can perform operations on the NEs in a managed domain only when they have the operation rights of the managed domain.
Access control policy	It is used to limit users to only have access to the eSight in the specified time segment or by using an IP address within the specified IP address range. If a user account is hacked, the hacker cannot use the account to log in to the server. This is because that users can log in only by using the IP addresses that are included in the access control list (ACL). Nobody can log in to the server with an IP address that is not included in the ACL.

Rights

Rights define which operations can be performed on objects. The operations that users can perform on objects vary according to their rights.

Figure 1-22 shows the rights elements: objects and operations.

Figure 1-22 Rights elements



eSight Users can perform operations on the eSight only they have access rights and operation rights of the eSight.

Figure 1-23 shows the operations that can be performed on the eSight.

Figure 1-23 Operations that can be performed on the eSight

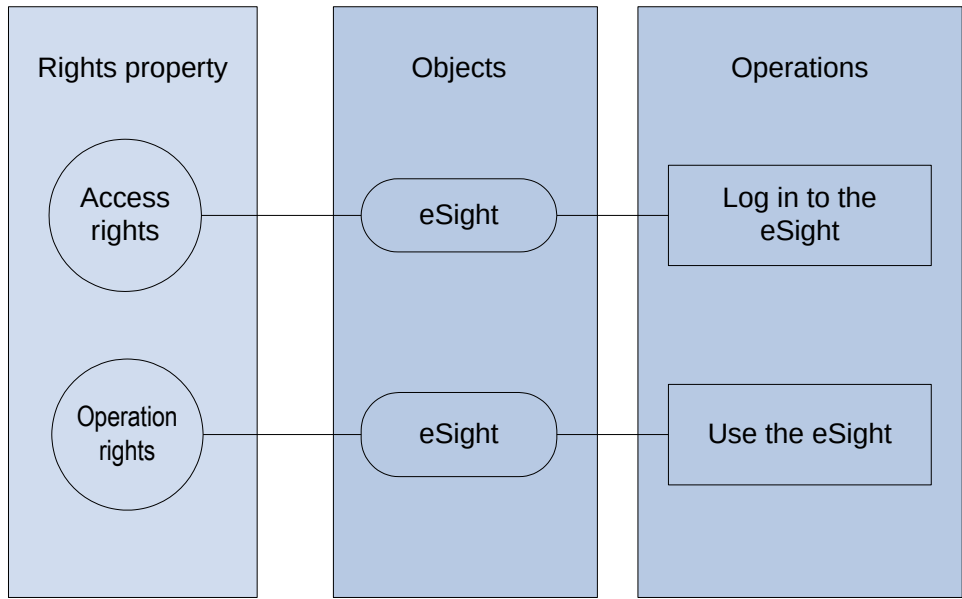


Table 1-5 describes the rights of the eSight users.

Table 1-5 Rights description

Rights	Operation	Description
Access rights	Log in to the eSight	Users can log in to the eSight only when they have valid accounts.
Operation rights	Perform operations on the eSight	Users can perform related management operations on the eSight client only when they have management rights, such as querying system logs and creating a role.

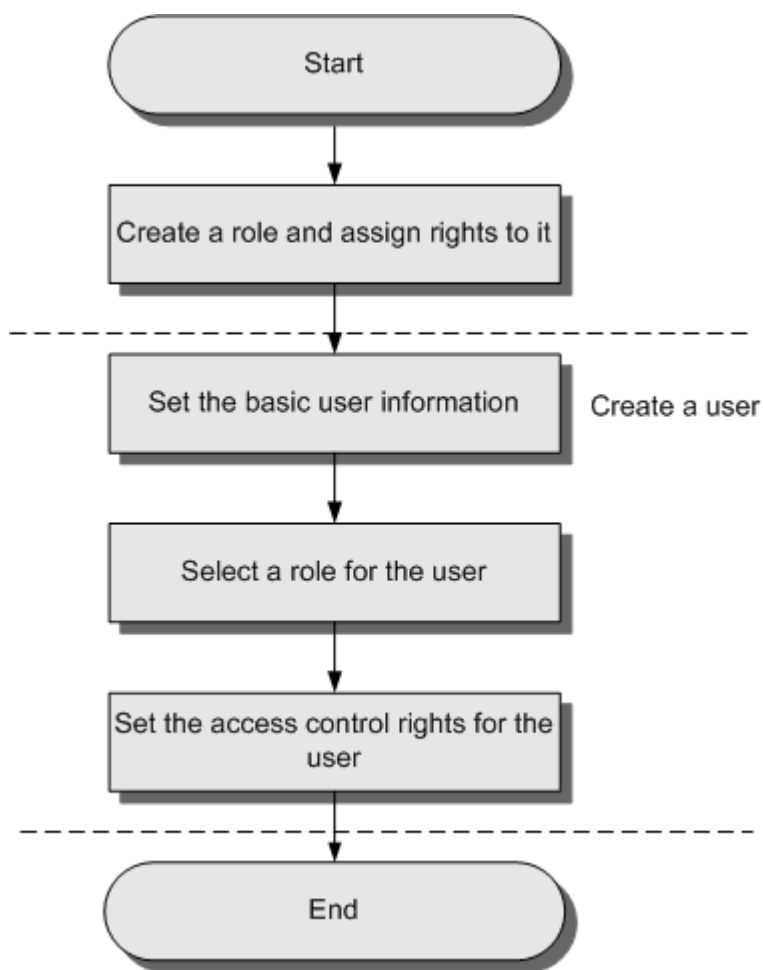
Authorization Principles

Authorization is the function of assigning rights to users.

Authorization is to allocate the eSight operation rights for users. eSight assign rights to users by adding the users to roles.

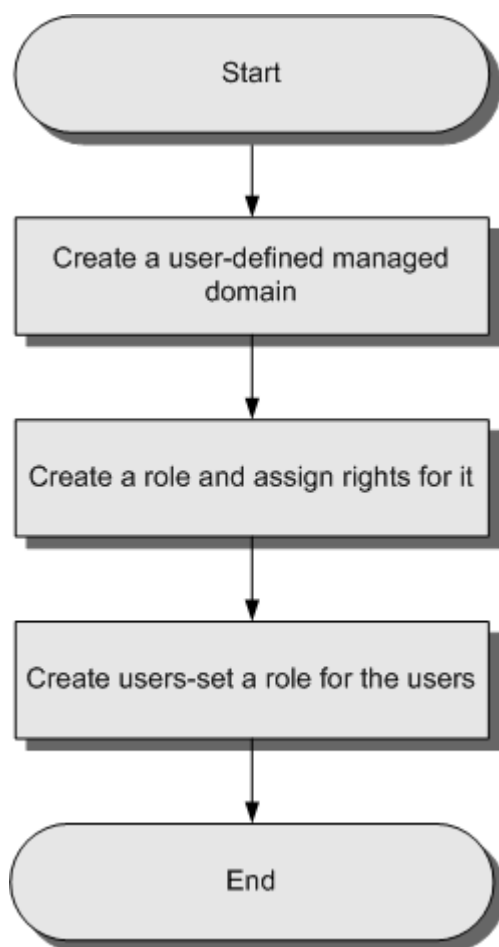
After some operations and objects are allocated to a role, the role has the rights of the operations on the objects. If a user is added to the role, the user has the rights of the role. The eSight provides two authorization modes: select roles while creating users and select users while creating rules.

- Select roles while creating users.
Roles are already created. If you select roles when creating users, the users have the rights of the selected roles after successful creation. Figure 1-24 shows the process of selecting roles while creating users.

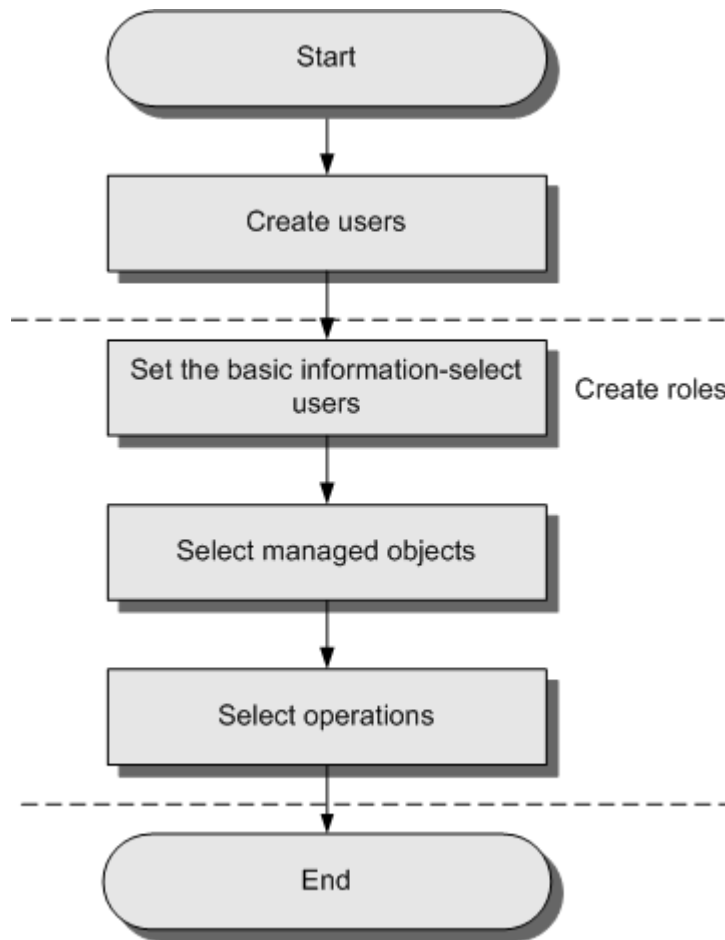
Figure 1-24 Common authorization process

In the process shown in [Figure 1-24](#), objects and operations must be specified for a role one by one. Too many objects may cause complex authorization operations. To improve authorization efficiency, you need to plan managed domains before authorization. [Figure 1-25](#) shows the authorization process by creating managed domains.

Figure 1-25 Complete authorization process



- Select users while creating roles.
Users are already created. If you select users when creating roles, the selected users have the rights of the roles after successfully creation. [Figure 1-26](#) shows the process of selecting users while creating roles.

Figure 1-26 Process

1.2.2 Basic Concepts of Resource Management

Before performing resource management operations, you need to be familiar with the basic concepts about resource management. Understanding these concepts helps you avoid errors when performing resource management operations.

[Table 1-6](#) describes the basic concepts about resource management.

Table 1-6 Basic concepts

Concept	Description
Subnet	A large network is divided into several smaller networks based on a specific rule (by region or device type), which facilitates network management. In the eSight, these smaller networks are called subnets.
NE	An NE is an actual physical device, and its basic information includes the IP address, port number, user name, and password.

1.2.3 Basic Concepts of Topology Management

Before performing topology management operations, you need to be familiar with the basic concepts about topology management. Understanding these concepts helps you avoid errors when performing topology management operations.

Topology Objects

Topology objects are used to identify entities on the network. Each element managed by eSight is called an object. An object can be a subnet, an NE, or a link between NEs. [Table 1-7](#) describes the basic concepts about topology management.

Table 1-7 Topology objects

Concept	Description
Subnet	A large network is divided into several smaller networks based on a specific rule (by region), which facilitates network management. These smaller networks are called subnets in the eSight.
Blank subnet	A blank subnet refers to a subnet where no device is deployed.
Layer 3 topology view	The Layer 3 topology view displays the real-time status of Layer 3 devices, subnets, and IP links between Layer 3 devices and subnets. NOTE Subnets in the Layer 3 topology view are classified by network segment. Devices on the same network segment belong to the same subnet.
Layer 2 topology view	The Layer 2 topology view displays the structure and status information such as connections between Layer 2 devices, link status, and device status based on Bridge Protocol Data Unit (BPDU) and neighboring protocols such as LLDP, NDP, CDP, and STP.
NE	The NE is used to identify actual devices. The NEs are classified into physical NEs and virtual NEs. Physical NEs: These NEs can be managed by the eSight include the SEE and USAU NEs in the service network and hosts, ATAE NEs, and routers in the physical network.
Link	Links indicate the connections between NEs in the physics view. All links in the eSight are virtual links. Virtual links indicate logical connections between NEs (including physical NEs and virtual NEs), and you need to manually create virtual links in the eSight.
Subordinate Resources	Subordinate resources are physical or logical objects under an NE, such as ports, links, and services.

Physical View

Physical views are the topology views supported by the eSight. In a physical view, the topology objects such as the subnets, NEs, links, and their status are represented by different icons. [Figure 1-27](#) shows a physical view.

Figure 1-27 Physical View

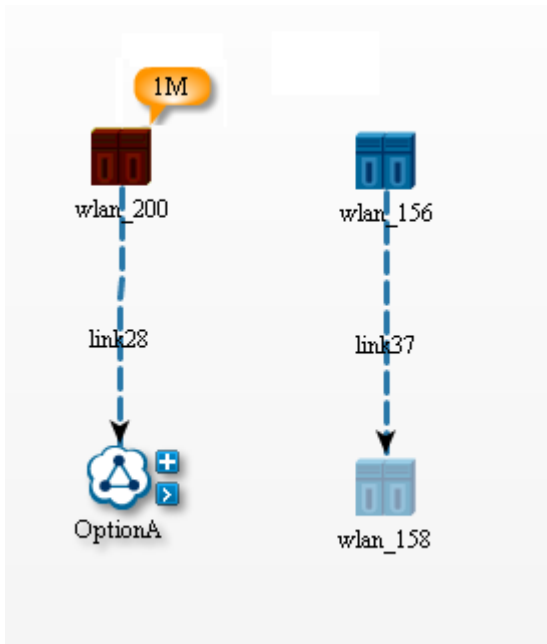


Table 1-8 describes the topology object icons.

Table 1-8 Topology object icons

Icon	Meaning
	Subnet
	NE

In a physical view, the NE alarm status is represented by pop-up icons of different colors. When an NE generates an alarm, the color of the pop-up icon changes to indicate the alarm of the corresponding severity. If an NE generates multiple alarms at a time, the color of the pop-up icon is subject to the color corresponding to the alarm of the highest severity. The number on the pop-up icon indicates the number of alarms of the highest severity. Table 1-9 describes the pop-up icons.

Table 1-9 Pop-up Icons for NE Alarms

Color	Meaning	Description
	Critical	The critical alarm occurs in the NE.
	Major	The major alarm occurs in the NE.
	Minor	The minor alarm occurs in the NE.
	Warning	The warning alarm occurs in the NE.

1.2.4 Basic Concepts of Fault Management

Before performing fault management operations, you must be familiar with the basic concepts about fault management, such as alarm severity, alarm status. Understanding these concepts will help you avoid errors when performing fault management operations.

Alarm Severities

There are four alarm severities: **Critical**, **Major**, **Minor**, and **Warning**, as shown in [Table 1-10](#). You can take different measures for different severities of alarms.

Table 1-10 Alarm severities

Alarm Severity	Description
Critical	An alarm severity that indicates a severe resource problem disrupting or severely impeding normal use.
Major	An alarm severity that indicates the possibility of some service-related problems with the resource. The severity of the problem is relatively high and the normal use of the resource is likely to be impaired.
Minor	An alarm severity that indicates the problems without affecting services. The problems of this severity may result serious faults, and therefore you need to take some corrective actions.
Warning	An alarm severity that indicates a condition exists that could potentially cause a problem with the resource.

Alarm Status

The alarm status contains acknowledgment and clearance. You can take proper measures for different alarms.

- Alarm status
Alarms can be classified into different status based on whether the alarms are cleared or acknowledged. [Table 1-11](#) describes the four alarm status.

Table 1-11 Alarm status

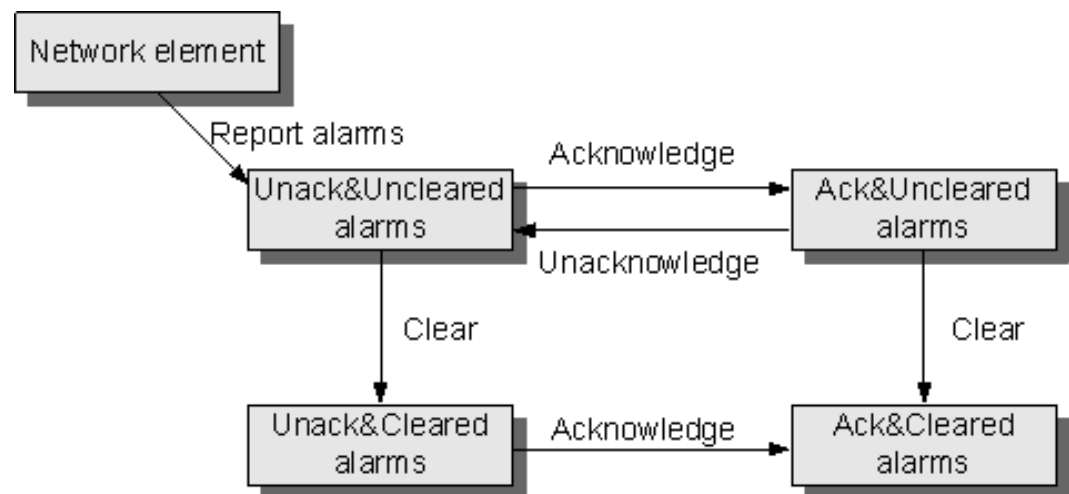
Alarm Type	Alarm Status
Current Alarms	Unacknowledged and uncleared
	Acknowledged and uncleared
	Unacknowledged and cleared
Historical Alarms	Acknowledged and cleared

- Status Change
Table 1-12 describes the alarm status change description.

Table 1-12 Status change

Status Change Type	Description
Clearance status change	If the condition that generated the alarm disappears, and the NE becomes normal, the NE server reports a clear alarm and the alarm status is changed from uncleared to cleared.
Acknowledgment status change	The acknowledged alarms refer to alarms that have already been handled, or will be handled. When the alarm is acknowledged, the alarm is changed from unacknowledged to acknowledged. If you want to have concerns over the acknowledged alarm again, you can unacknowledge the alarm. When the alarm is unacknowledged, the alarm is changed from acknowledged to unacknowledged.

Figure 1-28 shows the relationship between alarm status.

Figure 1-28 Alarm status relationship

Faults, Alarms and Events

- Faults and Alarms
An alarm is a message reported when a fault is detected. Not all faults result in alarms. Only the faults that the system can detect result in alarms. The others do not result in alarms, but they still persist.
- Similarities Between Alarms and Events
Both alarms and events are the presence of anything that takes place on the managed object detected by the eSight.
- Differences Between Alarms and Events

An alarm is a message reported when a fault is detected.

An event is anything that takes place on a managed objects.

The differences are:

- The alarm is a special event. When an alarm is generated, you need to troubleshoot the fault. Otherwise, the services may run abnormally.
- If an event occurs, the managed object has changes but the service may not be affected.

1.2.5 Basic Concepts of Performance Management

Before performing performance management operations, you need to be familiar with the basic concepts about performance management, such as performance indicators and thresholds. Understanding these concepts helps you avoid errors when performing performance management operations.

Table 1-13 describes the basic concepts about performance management.

Table 1-13 Performance management concepts

Concept	Description
Performance indicators	Performance indicators are used to monitor the performance of resources. For example, the CPU usage and memory usage are performance indicators, and CPU and memory are resources. Monitoring the performance indicators of NEs helps measure the deterioration in the service processing performance and resolve problems before faults occur.
Indicator thresholds	Indicator thresholds allow you to configure whether to report alarms and the severities of the reported alarms. When the value of a performance indicator exceeds a specified threshold, the measurement object generates a QoS alarm, indicating that deterioration in the performance requires your attention. When the value falls within the range allowed, the QoS alarm is automatically cleared. Setting approximate indicator thresholds ensures normal running of services. To ensure that problems can be detected in advance, you are advised to set performance indicator thresholds as greater values than the standard values.
Measurement objects	Measurement objects are the physical or logical resources corresponding to measurement indicators. When a managed object has multiple resources, for example, when a device provides multiple CPUs, you need to specify a specific resource for the measurement indicator.
Collection period	Collection period indicates the data collection interval. If the collection period is set to 1min , the eSight collects data for the measurement indicators of measurement objects every one minute.

1.2.6 Basic Concepts of Report Management

The report system provides flexible and easy-to-use application services such as developing reports based on design documents and generating, forwarding, and managing reports based on the Web. The report system provides the functions such as monitoring, analyzing, optimizing, and formulating policies for network performance, storage, and alarms. The report system supports instant reports, periodical reports and quick reports and has an excellent report forwarding mechanism by using emails. The report system features powerful data collection and display capabilities.

Instant Report, Periodical Report and Quick Report

The report system can generate instant reports , periodical reports and quick report.

- **Instant report**
The report system manages instant reports. You can export instant reports to files in Excel, Word, PDF, and PowerPoint formats.
- **Periodical report**
Periodical tasks are performed periodically. You can export periodical reports manually to files in Excel, Word, PDF, and PowerPoint formats. Periodical tasks generate reports such as a daily report, weekly report, monthly report, quarterly report, semiannual report, and annual report.
- **Quick report**
You can use quick reports to rapidly view statistics about a single counter of an object without creating tasks or preparing design files. You can export quick reports to files in Excel format.

Report Forwarding Mechanism

You can send reports to external email boxes. The report forwarding mechanism is easy to use.

Report Storage and Management Function

The report system provides the functions of storing and managing reports. You can perform the following operations:

- Store reports to the report storage area. And store only periodical reports to the report folder of the report storage area.
- Configure the report storage area.
- Print reports in the report storage area in the report system.

1.2.7 Basic Concepts of Ne Management

This topic describes basic functions of NE explorer.

Feature	Description
Panel management	eSight provides the functions of displaying board and port status on device panels.
Alarm	eSight provides the function of viewing the alarm list of NE. You can perform the

Feature	Description
	following operations on alarms such as locking, unlocking, acknowledging, unacknowledging, clearing, suppressing, topology locating, and exporting. You can also view alarm details and alarm log information.
Performance	eSight provides the function of displaying NE KPIs in graphics.
Interface management	eSight provides the function of viewing basic information about interfaces, such as IP addresses of interfaces.
IP address management	eSight provides the function of managing IP addresses of NE and IP addresses of interfaces on NE.
Configuration file management	eSight provides the function of viewing, comparing, and restoring device configuration files.
Protocol parameter management	eSight provides the function of setting SNMP and Telnet parameters of NE on eSight so that eSight can properly communicate with the NE.

1.2.8 Basic Concepts of Service Management

1.2.8.1 Basic Concepts of IPSec VPN Management

Before configuring and managing the IPSec VPN service by using eSight, you need to understand the basic concepts of the IPSec VPN service to successfully perform related operations.

Data Flow

A data flow is a set of data with common features, such as source address/mask, destination address/mask, protocol number in an IP packet for encapsulating upper-layer protocols, source port number, and destination port number.

A data flow is generally defined by an access-list. All packets that match a single access-list are logically considered as a data flow. A data flow can be data transmitted between two hosts that are connected to each other using Transmission Control Protocol (TCP) or all data traffic transmitted between two subnets.

IPSec VPN can protect data flows as required. For example, IPSec VPN can protect data flows based on different security protocols, algorithms, and keys.

Security Association (SA)

You need to establish an SA before using IPSec VPN to protect data flows. You can establish an SA manually or in automatic negotiation mode.

Internet Key Exchange (IKE) is used for establishing SAs in automatic negotiation mode. An IPSec VPN SA is a convention on tunnel parameters between two communication parties that need to establish an IPSec VPN tunnel. The tunnel parameters include IP addresses of both ends of a tunnel, authentication mode, authentication algorithm, authentication key, encryption algorithm, encryption key, shared key, and life cycle of keys.

To establish an IPSec VPN tunnel, two communication parties need to negotiate about the tunnel parameters, that is, to establish an SA. An SA is unidirectional. Therefore, you need to establish at least two SAs for two-way communication between two parties so that data flows transmitted in both directions are protected.

SA Negotiation Mode

The negotiation modes of an IPSec VPN SA are as follows:

- Internet Security Association and Key Management Protocol (ISAKMP) negotiation
The IKE automatic negotiation mode, that is, ISAKMP negotiation mode, is quite simple. You only need to configure the security policy information about which the IKE negotiated. ISAKMP establishes and maintains SAs in automatic negotiation mode.



NOTE

ISAKMP defines the procedure for negotiating, establishing, modifying, and deleting an SA and the packet format. IKE uses ISAKMP to define key exchange, and provides algorithms and key negotiation services for communication protocols that need to be encrypted and authenticated over the Internet.

- Manual negotiation
The advantage of establishing an SA by manually setting tunnel parameters is that the IPSec VPN functions are implemented independently. The disadvantage is that you need to manually configure all information required for establishing an SA. The configuration is complex, and advanced features, such as regular key update, are not supported.

You can configure SAs manually if the number of peer devices is small or in a small static environment. However, in medium and large dynamic network environments, you are advised to establish SAs in IKE automatic negotiation mode.

Data Protection Mode

IPSec VPN provides high-quality, interoperable, and cryptography-based security services for IP packets by using the Authentication Header (AH) protocol and Encapsulating Security Payload (ESP) protocol.

The AH protocol protects data integrity, and the ESP protocol protects data confidentiality and integrity.

- AH packet authentication mode
 - Data integrity check
 - Data source authentication
 - Replay protection function
- ESP protection mode
 - Data integrity check
 - Data encryption
 - Data source authentication
 - Replay protection function

1.2.9 Basic Concepts of Smart Configuration Tool

Before performing smart configuration tool operations, you must be familiar with the basic concepts about smart configuration tool, such as template, plan sheet and verification. Understanding these concepts will help you avoid errors when performing smart configuration tool operations.

Table 1-14 describes the basic concepts about smart configuration tool.

Table 1-14 Basic concepts

Concept	Description
Template	A template is a set of commands. eSight provides predefined general templates based on configuration scenarios. You can select a predefined template and set parameters to generate scripts.
Plan Sheet	A plan sheet allows you to deliver multiple parameters to multiple devices using the same template. The smart configuration tool allows you to export a template to generate a plan sheet, set parameters, and import the plan sheet. Then the smart configuration tool can automatically generate a script based on the planned information and deliver the script to devices in batches.
Verification	The smart configuration tool allows you to modify scripts offline and can automatically verify the modified scripts and display the verification results in different colors. In this manner, the smart configuration tool ensures that all configurations are compliant with command line standards.

1.2.10 Basic Concepts of Backing Up and Restoring Device Configuration Files

To implement disaster recovery, back up device configuration files and save the backup files to eSight so that you can restore the device configuration files in case of accidents or misoperations.

Table 1-15 shows the basic concepts of backing up and restoring device configuration files.

Table 1-15 Concepts of Backing Up and Restoring Device Configuration Files

Concepts	Description
Backing Up Configuration Files	You need to back up device configuration files and save the backup files to eSight. This helps ensure the security of device configuration and prevent configuration data loss. The device configuration can be copied easily. Backup configuration files can be transferred by using only FTP.
Restoring Configuration Files	You can use the backup files on eSight and restore the device configuration files as required. eSight provides the function of restoring device configuration files in batches.
Setting a Configuration	You can save a device configuration file to baseline file for future configuration file restoration.

Concepts	Description
ion File to Baseline File	

1.2.11 Basic Concepts of User-Defined Devices Management

eSight provides the functions such as monitoring performance, configuration files, topology, NE panels, alarms, and resources of user-defined devices.

Performance Monitoring

- Central Processing Unit (CPU) usage, including the board CPU.
- Memory usage, including the board memory.
- Device response time and percentage of devices that fail to reach the standard.
- Indicator statistics based on the standard Management Information Base (MIB) of RFC1213: IP packet statistics, interface packet statistics, routing address discard rate, Transmission Control Protocol (TCP) packet statistics, User Datagram Protocol (UDP) packet statistics, SNMP packet statistics, and Point-to-Point Protocol (PPP) packet statistics.
- Customized counters for monitoring performance of user-defined devices. You can import counters by customization. eSight supports basic calculation formulas. Counters are generated based on calculation for multiple MIB objects.

Configuration File Management

You can back up and restore configuration files by using scripts.

Topology Management

You can display the topology of user-defined devices. Different icons are displayed for different types of devices for easy identification. You can perform different operations on devices based on the device type.

NE Panel Management

eSight provides default images and displays panel information about network devices based on the public MIB. eSight does not provide the high-fidelity panel function for non-network devices such as printers, personal computers (PCs), and servers. You can customize the functions of user-defined device panels. eSight provides the function of drawing profiles based on the device photos or high-fidelity pictures so that the displayed panels look more real. eSight provides the function of displaying private MIB information about non-Huawei devices on panels. You can perform the operations such as activating an interface, deactivating an interface, and querying alarm information on panels.

Alarm Management

eSight parses standard alarms reported by user-defined devices by default. You need to customize private alarm parameters for private alarms reported by user-defined devices by

using the provided customization tool. eSight parses private alarms based on the private alarm parameters.

Resource Management

eSight supports operations based on the standard MIB. eSight also provides the functions such as managing interfaces, querying and modifying basic information about devices, and querying IP address table (IPv4), IP routing table, and entity data based on the RFC1213. You can customize basic information about the device manufacturer, logo, and device model.

2 Security Management

About This Chapter

Security management provides the functions of managing user rights and eSight security policies. These functions can prevent unauthorized users from performing malicious operations on the eSight, ensuring data security of the eSight.

2.1 Overview of Security Management Operations

This topic describes the security management operations.

2.2 Security Policy Management

Security policies include **Account Policy**, **Password Policy**, and **Access Control Policy**. To increase access security, you need to plan and configure security policies during initial installation eSight.

2.3 Creating Users and Assigning Rights

The eSight provides the functions of creating users, roles, and user-defined managed domains as required. After you create a user, set the basic information about the user, and assign rights for the user, the user has the operation rights for a specified managed domain.

2.4 Monitoring the User

You can learn about the information about sessions and operations by monitoring the sessions and operations of the users who are logged in to the eSight. When some unauthorized sessions or operations are detected, you can force the related users to log out, ensuring security of the eSight.

2.5 Example: Typical Security Management Operations

In the eSight, only after you set a role for a user, the user has the operation rights of the role in its managed domains. This topic describes how to create an eSight user and assign rights to the user.

2.1 Overview of Security Management Operations

This topic describes the security management operations.

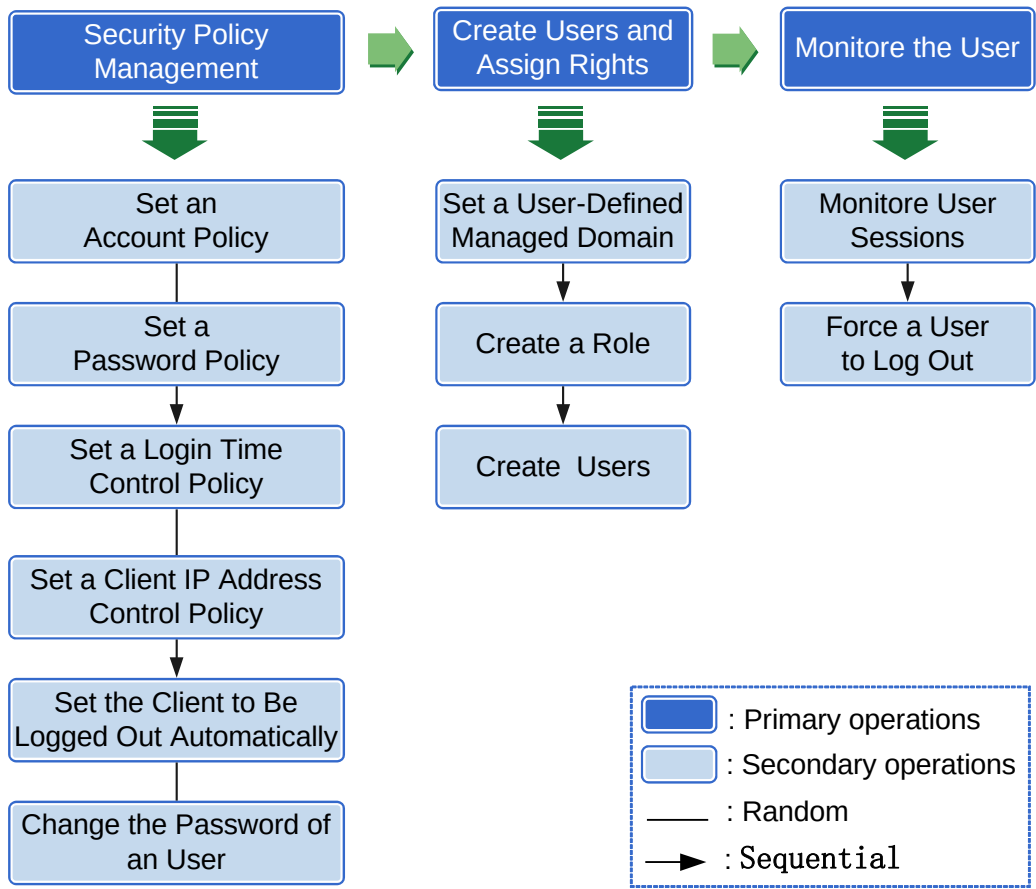
Context

Before performing security management operations, you must familiarize yourself with the basic concepts related to security management, such as the user, role, operation rights, and access control. For details, see [1.2.1 Basic Concepts of Security Management](#). Understanding these concepts will help you avoid errors when performing security management operations.

Overview of Security Management Operations

[Figure 2-1](#) shows the overview of security management operations. For more details, click the operation in the overview.

Figure 2-1 Overview of security management operations



[Table 2-1](#) describes the security management operations.

Table 2-1 Security management operations

Operation	Description
2.2.1 Setting an Account Policy	This topic describes how to set an account policy to improve access security of the eSight. The account policy settings include the length of the user name and the policies related to user login.
2.2.2 Setting a Password	This topic describes how to set a password policy to improve

Operation	Description
Policy	access security of the eSight. The password policy settings include the user password complexity rules and password change interval.
2.2.3.1 Setting a Login Time Control Policy	This topic describes how to set a login time control policy to ensure access security of the eSight.
2.2.3.2 Setting a Client IP Address Control Policy	This topic describes how to set a client IP address control policy to allow some users only to log in to the eSight by using specified IP addresses.
2.2.4 Setting the Client to Be Logged Out Automatically	This topic describes how to set the client to be logged out automatically. To prevent other users from performing unauthorized operations, the eSight allows you to set related idle parameters. The client is automatically logged out after being left idle for a specified period of time.
2.2.5 Changing the Password of an User	To ensure account security, you need to change the initial password the first time you log in. Periodically changing the password improves security of user information.
2.3.2 Creating a Role	This topic describes how to create a role. When the default roles of the eSight cannot meet the user authorization requirements, you can create roles to ensure security of the eSight and facilitate network management.
2.3.3 Creating Users	This topic describes how to create users. When the default user of the eSight cannot meet the network management requirements, you can create users to ensure security of the eSight and facilitate network management.
2.3.1 Setting a User-Defined Managed Domain	You can set a user-defined managed domain as required. After you can specify a user-defined managed domain for a role, the role can manage the objects in the managed domain.
2.4.1 Monitoring User Sessions	This topic describes how to monitor user sessions. This function helps you learn about the information about the users who log in to the eSight.
2.4.2 Forcing a User to Log Out	This topic describes how to force a user to log out. You can force the corresponding users to log out when some dangerous operations or invalid sessions are detected during the monitoring or session.

2.2 Security Policy Management

Security policies include **Account Policy**, **Password Policy**, and **Access Control Policy**. To increase access security, you need to plan and configure security policies during initial installation eSight.

2.2.1 Setting an Account Policy

This topic describes how to set an account policy to improve access security of the eSight. The account policy settings include the length of the user name and the policies related to user login.

Prerequisites

You have the operation rights for **Security Management**.

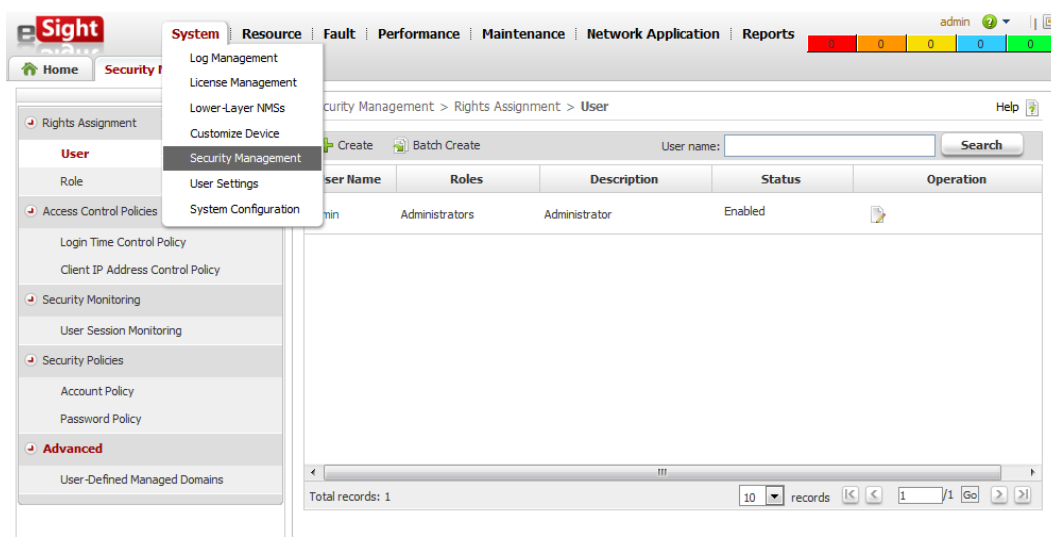
Context

- The account policy is applicable to all users.
- The eSight provides the default account policy, and you can modify it as required.

Procedure

Step 1 Choose **System > Security Management** from the main menu.

Figure 2-2 Security management



Step 2 In the **Security Management** window, choose **Security Policies > Account Policy**.

Step 3 On the **Account Policy** page, set the account policy as required.

Figure 2-3 Setting account policy

Security Management > Security Policies > **Account Policy** Help 

Minimum length of a user name:

☒ Enable the account disabled policy

Number of consecutive days an account is not used:

☒ Enable the account lock policy

Auto-lock conditions (both of the following must be met)

Allowed time (mins):

Consecutive failed login attempts:

Account lock duration

☒ Lock duration (mins):

☐ Permanent lock

Apply

Step 4 Click **Apply**.

----End

Follow-up Procedure

The following table describes the operations that you can perform if the user is disabled or locked.

Operation	Procedure
Enable a user	1. Choose Rights Assignment > User. 2. Click  in the Operation column where the user information is located.
Unlock a user account	• Unlock the user account within the lock duration. The user account is automatically unlocked after the lock duration limit is reached. • Unlock a user account that is locked permanently. – Choose Rights Assignment > User. – Click  in the Operation column where the user information is located.

2.2.2 Setting a Password Policy

This topic describes how to set a password policy to improve access security of the eSight. The password policy settings include the user password complexity rules and password change interval.

Prerequisites

You have the operation rights for **Security Management**.

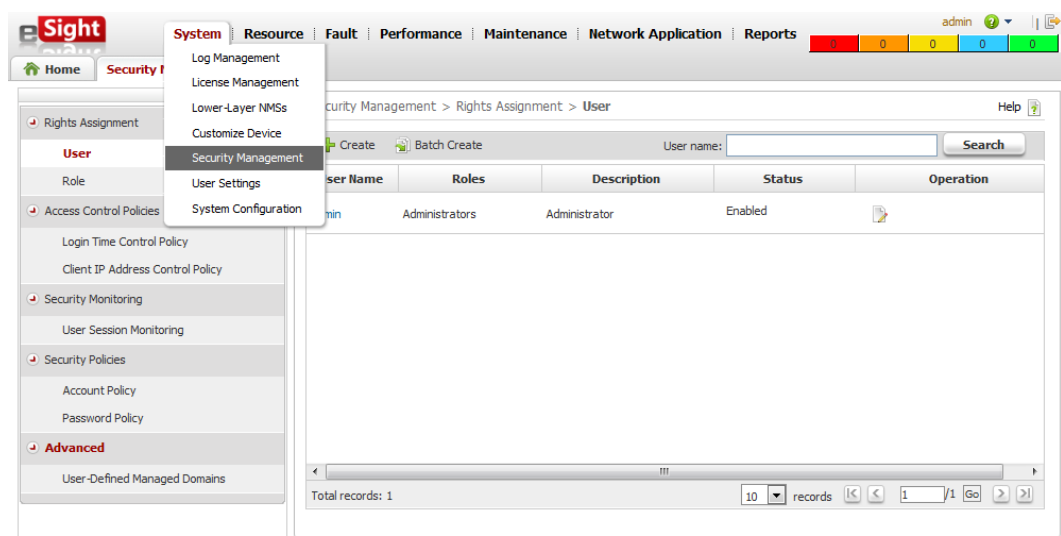
Context

- A password policy applies to all users once it is configured. After the minimum length of the user password is specified and validated, if an online user wants to change the password, the user needs to set the new password based on the specified minimum password length requirements.
- You need to set a password based on the password policy when you create a user.
- A new password policy does not affect the configured password.
- The eSight provides the default password policy, and you can modify it as required.

Procedure

Step 1 Choose **System > Security Management** from the main menu.

Figure 2-4 Security management



Step 2 In the **Security Management** window, choose **Security Policies > Password Policy**.

Step 3 On the **Password Policy** page, set the password policy as required.

Figure 2-5 Setting password policy

Security Management > Security Policies > **Password Policy** Help ?

Minimum password length:	6
Maximum attempts to enter the password the same as old passwords:	3
☒ Maximum number of occurrences of a character in a password:	3
☒ Minimum time interval between password change attempts (mins):	5
☐ Allow at least one of the following special characters:space!"#\$%&'()*+,-./:;<=>?@...	
☒ Forcibly change an expired password.	
Password valid for (days):	90
Days remaining:	7
Apply	

Step 4 Click **Apply**.

----End

2.2.3 Setting an Access Control Policy

The access control policy controls login time and client IP addresses. To ensure access security, you can set an access control policy to allow some users to log in to the eSight by using a specified IP address within the specified period of time.

2.2.3.1 Setting a Login Time Control Policy

This topic describes how to set a login time control policy to ensure access security of the eSight.

Prerequisites

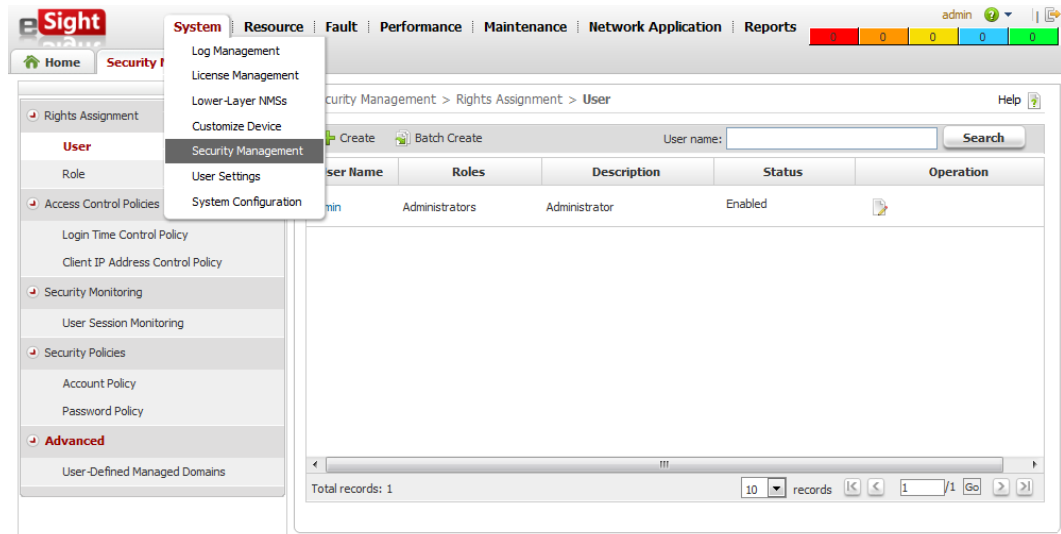
You have the operation rights for **Security Management**.

Context

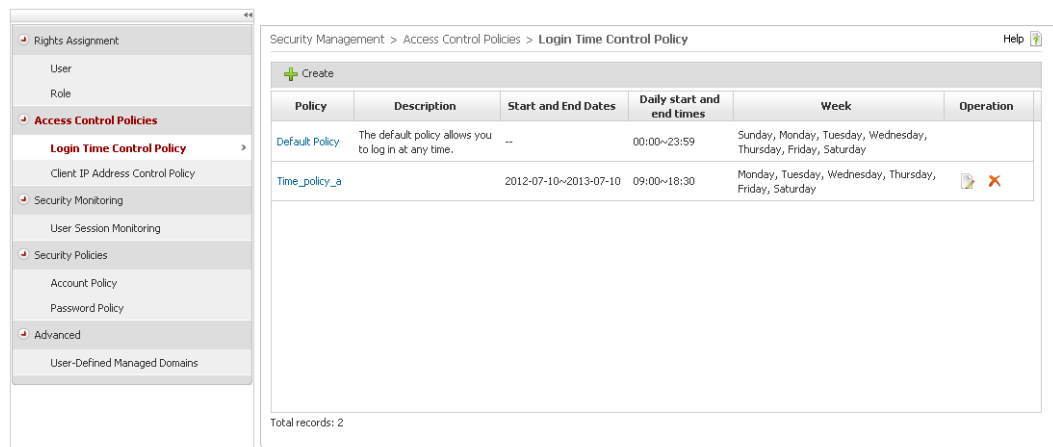
- The default policy allows you to log in at any time.
- Login time control policies are not applicable to the default user **admin**.

Procedure

Step 1 Choose **System > Security Management** from the main menu.

Figure 2-6 Security management

Step 2 In the **Security Management** window, choose **Access Control Policies > Login Time Control Policy**.

Figure 2-7 Setting login time control policy

Step 3 On the **Login Time Control Policy** page, perform the operations shown in the following table.

Set a Login Time Control Policy	Operation
Create a login time control policy	When the default policy cannot meet the management requirements, you can create a login time control policy as required. 1. Click Create. 2. On the Create Login Time Control Policy page, set Name, Start and end dates, Daily start and end times, Week, and Description. 3. Click OK.
View a login time control policy	You can learn about the details by viewing the login time control policy. Click the required policy name in the Policy column. On the View Login Time Control Policy page, view the details of the policy.
Modify a login time control policy	You can modify a login time control policy as required. 1. Click  in the Operation column where the required policy is located. 2. On the Modify Login Time Control Policy page, change the values of Start and end dates, Daily start and end times, Week, and Description. 3. Click OK. NOTE The default policy cannot be modified.
Delete a login time control policy	You can delete an unused login time control policy. 1. Click  in the Operation column where the required policy is located. 2. In the Confirm dialog box, click Yes. NOTE The default policy cannot be deleted.

----End

2.2.3.2 Setting a Client IP Address Control Policy

This topic describes how to set a client IP address control policy to allow some users only to log in to the eSight by using specified IP addresses.

Prerequisites

You have the operation rights for **Security Management**.

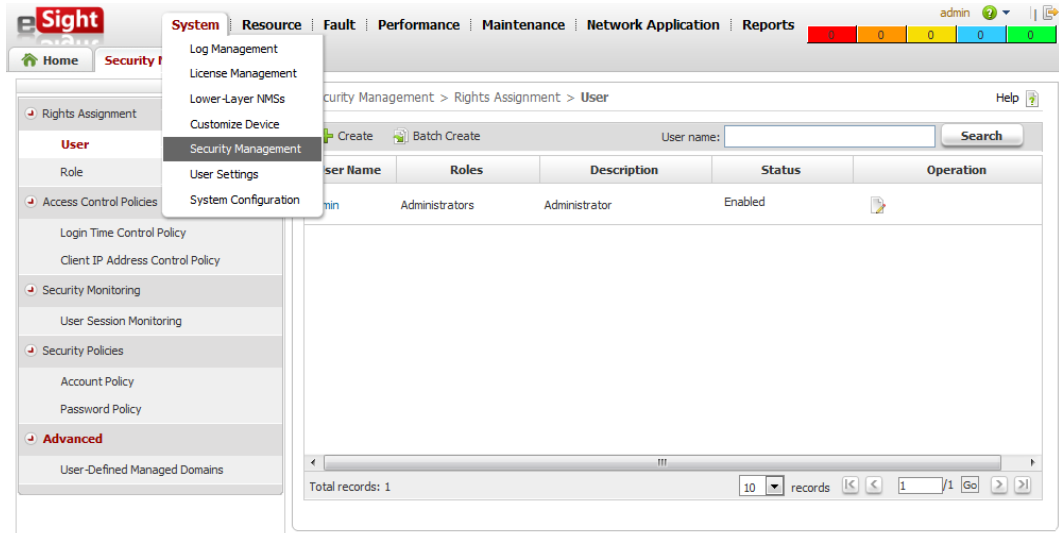
Context

You can set a client IP address control policy for the default user **admin** to allow **admin** only to log in to the eSight by using specified IP addresses.

Procedure

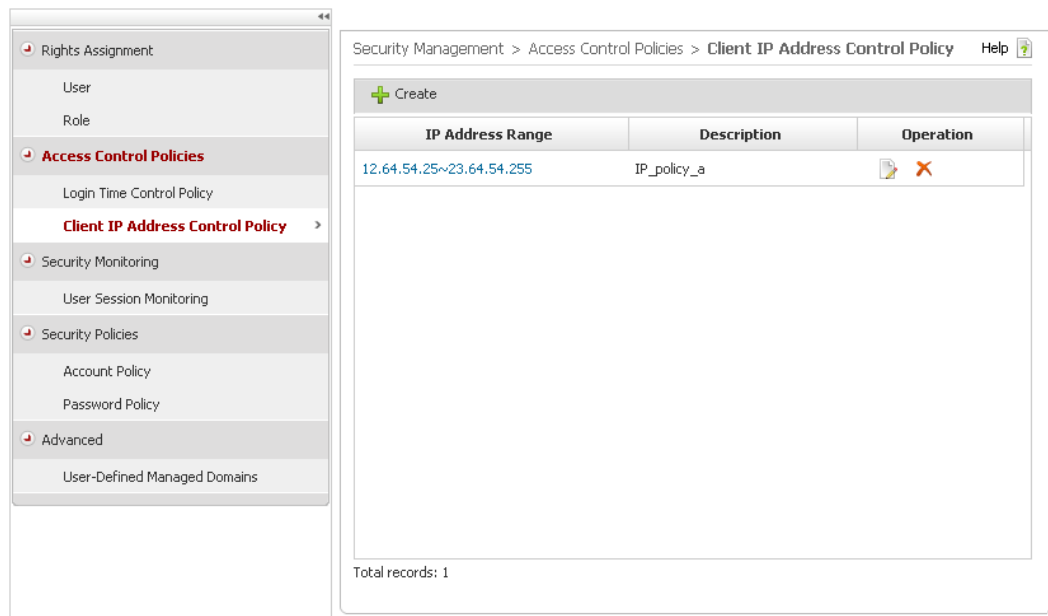
Step 1 Choose **System > Security Management** from the main menu.

Figure 2-8 Security management



Step 2 In the **Security Management** window, choose **Access Control Policies > Client IP Address Control Policy**.

Figure 2-9 Setting client IP address control policy



Step 3 On the **Client IP Address Control Policy** page, perform the operations shown in the following table.

Setting an IP Address Control Policy	Operation
Create a client IP address control policy	Create a client IP address control policy as required to allow users to log in eSight using specified IP addresses. 1. Click Create. 2. On the Create Client IP Address Control Policy page, set Start IP address, End IP Address, and Description. 3. Click OK.
View a client IP address control policy	You can learn about the details by viewing the client IP address control policy. Click the range where the required IP address is located in the IP Address Range column. On the View Client IP Address Control Policy page, view the details.
Modify a client IP address control policy	You can modify a client IP address control policy as required. 1. Click  in the Operation column where the required policy is located. 2. On the Modify Client IP Address Control Policy page, set Start IP address, End IP Address, and Description. 3. Click OK.
Delete a client IP address control policy	You can delete an unused client IP address control policy. 1. Click  in the Operation column where the required policy is located. 2. In the Confirm dialog box, click Yes.

----End

2.2.4 Setting the Client to Be Logged Out Automatically

This topic describes how to set the client to be logged out automatically. To prevent other users from performing unauthorized operations, the eSight allows you to set related idle parameters. The client is automatically logged out after being left idle for a specified period of time.

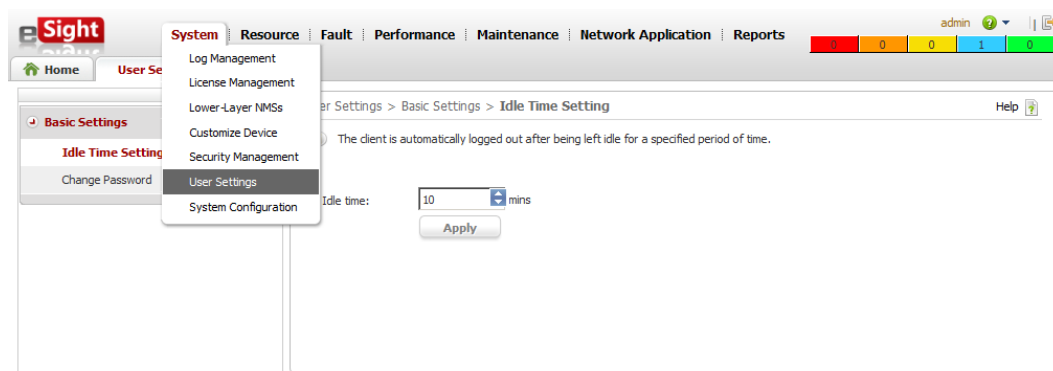
Context

This operation is valid for the current user.

Procedure

Step 1 Choose **System > User Settings** from the main menu.

Figure 2-10 Setting a user



Step 2 In the **User Settings** window, choose **Basic Settings > Idle Time Setting**.

Step 3 On the **Idle Time Setting** page, select **Idle time**.

Figure 2-11 Setting idel time



Step 4 In the **Idle time** text box, enter a value or select a value.

Step 5 Click **Apply**.

----End

Follow-up Procedure

After the client is automatically logged out, the current user needs to log in to the eSight again.

2.2.5 Changing the Password of an User

To ensure account security, you need to change the initial password the first time you log in. Periodically changing the password improves security of user information.

You need to change the following user passwords:

- [Changing the eSight User Password](#)
- [Changing the Maintenance Tool User Password](#)
- [Changing the Password of the Administrator User for Windows](#)

- [Changing the Password of the root User for Linux](#)
- [Changing the Password of FTP or FTPS](#)
- [Changing the Default Password of SBUS](#)
- [Changing the Password for Northbound SNMP V3](#)

Changing the eSight User Password

After logging in to the eSight for the first time, you need to change the initial password to ensure the eSight security. Periodically changing the eSight can improve user information security.

Prerequisite

You have logged in to the eSight client.

Background

By default, the eSight provides an initial user **admin**, its initial user password is **Changeme123**. The **admin** user has the operation rights of all managed domains of the eSight.

Procedure

- Change the initial password

At first login to the eSight, the page for changing the initial password is displayed.

1. On the **Change Password** page, set **Old password**, **New password**, and **Confirm password**.
2. Click **Apply**.
- Periodically change the password
 1. Choose **System > User Settings** from the main menu.
 2. In the **User Settings** window, choose **Basic Settings > Change Password**.
 3. On the **Change Password** page, click **Set**.
 4. In the displayed window, set **Old password**, **New password**, and **Confirm password**.
 5. Click **OK**.

----End

Changing the Maintenance Tool User Password

You need to change the initial password the first time you log in to the maintenance tool. Periodically changing the user password of the maintenance tool can improve user information security.

Prerequisite

You have logged in to the maintenance tool client.

Background

By default, the maintenance tool provides an initial user **sys**, and its initial user password is **Changeme123**. The **sys** user has the operation rights of all managed domains of the maintenance tool.

Procedure

- Change the initial password

At first login to the maintenance tool, the page for changing the initial password is displayed.

1. On the **Change Password** page, set **Old password**, **New password**, and **Confirm password**.
 2. Click **Apply**.
- Periodically change the password
1. Choose **System > User Settings** from the main menu.
 2. In the **User Settings** window, choose **Basic Settings > Change Password**.
 3. On the **Change Password** page, click **Set**.
 4. In the displayed window, set **Old password**, **New password**, and **Confirm password**.
 5. Click **OK**.

----End

Changing the Password of the AdministratorUser for Windows

You are advised to change the initial password the first time you log in to the eSight server that runs Windows. Periodically changing the user password of Windows can improve user information security.

Prerequisites

You have logged in to the server as the **Administrator** user.

Procedure

- Step 1** Press **Ctrl+Alt+Delete** to lock the current login page.
- Step 2** Click **Change Password**.
- Step 3** In the displayed dialog box, enter **Old password**, **New password**, and **Confirm New Password** of the **Administrator** user.
- Step 4** Click **OK**.

----End

Changing the Password of the rootUser for Linux

You are advised to change the initial password the first time you log in to the server that runs Linux. Periodically changing the user password of Linux can improve user information security.

Prerequisites

You have logged in to the server as user **root**.

Procedure

- Step 1** Run the following command to change the password of the **root** user:
- ```
passwd
```
- Step 2** Enter and then confirm the password as prompted.

----End

## Changing the Password of FTP or FTPS

You can use the BME tool to generate the ciphertext and then copy it to the configuration file for changing the password of FTP or FTPS.

### Prerequisites

Before using the BME tool, install JDK. The installation path of JDK cannot contain blank space.

### Background

- The initial user name for FTP or FTPS is **admin**, and its initial password is **Changeme123**.
- The encrypt tool is stored in **eSight\_ROOT\AppBase\tools\encrypt**.



#### NOTE

**eSight\_ROOT** is the installation directory of the eSight system.

- The password for FTP or FTPS is stored in **ftpusers.properties** in **eSight\_ROOT\AppBase\etc**.



#### NOTE

**eSight\_ROOT** is the installation directory of the eSight system.

- **Windows**

1. Run the following command to open the directory of the encrypt tool:  
**cd /d eSight\_ROOT\AppBase\tools\encrypt**
2. Run the following command to generate the ciphertext:  
**encrypt.bat 0 password**
3. Replace the password stored in the specified path with the generated ciphertext.



#### NOTE

You can open the **ftpusers.properties** configuration file in **eSight\_ROOT\AppBase\etc**, and then replace the value of **admin.password** in **ftpusers.properties** with the generated password.

4. Restart the eSight.

- **Linux**

1. Run the following command to open the directory of the encrypt tool:  
**cd eSight\_ROOT/AppBase/tools/encrypt**
2. Run the following command to generate the ciphertext:  
**./encrypt.sh 0 password**
3. Replace the password stored in the specified path with the generated ciphertext.



#### NOTE

You can open the **ftpusers.properties** configuration file in **eSight\_ROOT/AppBase/etc**, and then replace the value of **admin.password** in **ftpusers.properties** with the generated ciphertext.

4. Restart the eSight.

----End

## Changing the Default Password of SBUS

You can use the BME tool to generate the ciphertext and then copy it to the configuration file for changing the password of SBUS.

### Prerequisites

Before using the BME tool, install JDK. The installation path of JDK cannot contain blank space.

### Background

- The initial password for SBUS is **Changeme123**.
- The encrypt tool is stored in **eSight\_ROOT\AppData\tools\encrypt**.



#### NOTE

**eSight\_ROOT** is the installation directory of the eSight system.

- The password for SBUS is stored in **oms.xml** in **eSight\_ROOT\AppData\etc**.



#### NOTE

**eSight\_ROOT** is the eSight installation directory.

### Procedure

#### • Windows

1. Run the following command to open the directory of the encrypt tool:

```
cd /d eSight_ROOT\AppData\tools\encrypt
```



#### NOTE

**eSight\_ROOT** is the installation directory of the eSight system.

2. Run the following command to generate the ciphertext:

```
encrypt.bat 0 password
```

3. Replace the password stored in the specified path with the generated ciphertext.



#### NOTE

You can open the **oms.xml** configuration file in **eSight\_ROOT\AppData\etc**, and then replace the value of **name=password** in **oms.xml** with the generated password.

4. Restart the eSight.

#### • Linux

1. Run the following command to open the directory of the encrypt tool:

```
cd eSight_ROOT/AppBase/tools/encrypt
```

2. Run the following command to generate the ciphertext:

```
./encrypt.sh 0 password
```

3. Replace the password stored in the specified path with the generated ciphertext.



#### NOTE

You can open the **oms.xml** configuration file in **eSight\_ROOT/AppBase/etc**, and then replace the value of **name="password"** in **oms.xml** with the generated ciphertext.

4. Restart the eSight.

----End

## Changing the Password for Northbound SNMP V3

You can use the BME tool to generate the ciphertext and then copy it to the configuration file for changing the password of Northbound SNMP V3.

### Prerequisites

Before using the encrypting tool **encrypt.bat**, install JDK. The installation path of JDK cannot contain blank space.

### Background

- The initial user name for northbound SNMP V3 is **nbi**, and its initial password is **Changeme123**.
- The encrypt tool is stored in **eSight\_ROOT\AppData\tools\encrypt**.



**NOTE**

**eSight\_ROOT** is the installation directory of the eSight system.

- The password for northbound SNMP V3 is stored in **nbi.xml** in **eSight\_ROOT\AppData\etc\oms.nbi**.
- The passwords for the northbound SNMP V3 include the authentication key and private key.

**Procedure**

- **Windows**

- Change the authentication key.
1. Run the following command to open the directory of the encrypt tool:  
**cd /d eSight\_ROOT\AppData\tools\encrypt**
  2. Run the following command to generate the ciphertext:  
**encrypt.bat 0 old password**
  3. Replace the password stored in the specified path with the generated ciphertext.



**NOTE**

You can open the **nbi.xml** configuration file in **eSight\_ROOT\AppData\etc\oms.nbi**, and then replace the value of **V3AuthPwd** in **nbi.xml** with the generated password.

4. Restart the eSight.
- Change the private key.
1. Run the following command to open the directory of the encrypt tool:  
**cd /d eSight\_ROOT\AppData\tools\encrypt**
  2. Run the following command to generate the ciphertext:  
**encrypt.bat 0 old password**
  3. Replace the password stored in the specified path with the generated ciphertext.



**NOTE**

You can open the **nbi.xml** configuration file in **eSight\_ROOT\AppData\etc\oms.nbi**, and then replace the value of **V3PrivPwd** in **nbi.xml** with the generated password.

4. Restart the eSight.
- **Linux**
  - Change the authentication key.
1. Run the following command to open the directory of the encrypt tool:  
**cd eSight\_ROOT/AppBase/tools/encrypt**
  2. Run the following command to generate the ciphertext:  
**./encrypt.sh 0 password**
  3. Replace the password stored in the specified path with the generated ciphertext.



**NOTE**

You can open the **nbi.xml** configuration file in **eSight\_ROOT/AppBase/etc/oms.nbi**, and then replace the value of **V3AuthPwd** in **nbi.xml** with the generated ciphertext.

4. Restart the eSight.
- Change the private key.
1. Run the following command to open the directory of the encrypt tool:

```
cd eSight_ROOT/AppBase/tools/encrypt
```

2. Run the following command to generate the ciphertext.  

```
./encrypt.sh 0 password
```
3. Replace the password stored in the specified path with the generated ciphertext.



**NOTE**

You can open the **nbi.xml** configuration file in **eSight\_ROOT/AppBase/etc/oms.nbi**, and then replace the value of **V3PrivPwd** in **nbi.xml** with the generated ciphertext.

4. Restart the eSight.

----End

## 2.3 Creating Users and Assigning Rights

The eSight provides the functions of creating users, roles, and user-defined managed domains as required. After you create a user, set the basic information about the user, and assign rights for the user, the user has the operation rights for a specified managed domain.

### 2.3.1 Setting a User-Defined Managed Domain

You can set a user-defined managed domain as required. After you can specify a user-defined managed domain for a role, the role can manage the objects in the managed domain.

#### Prerequisites

You have the operation rights for **Security Management**.

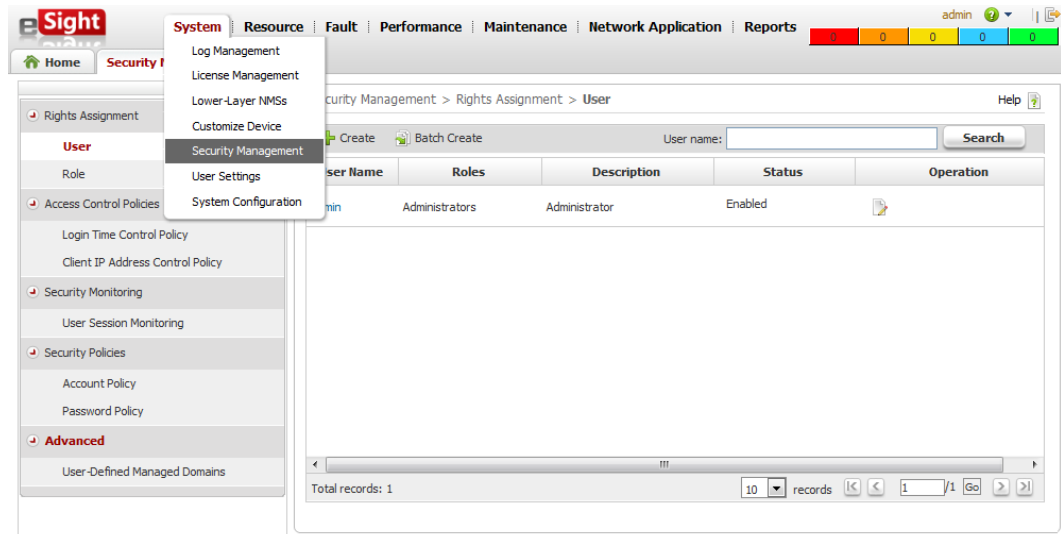
#### Context

You can select user-defined managed domains from the managed domain list when creating and maintaining a role.

#### Procedure

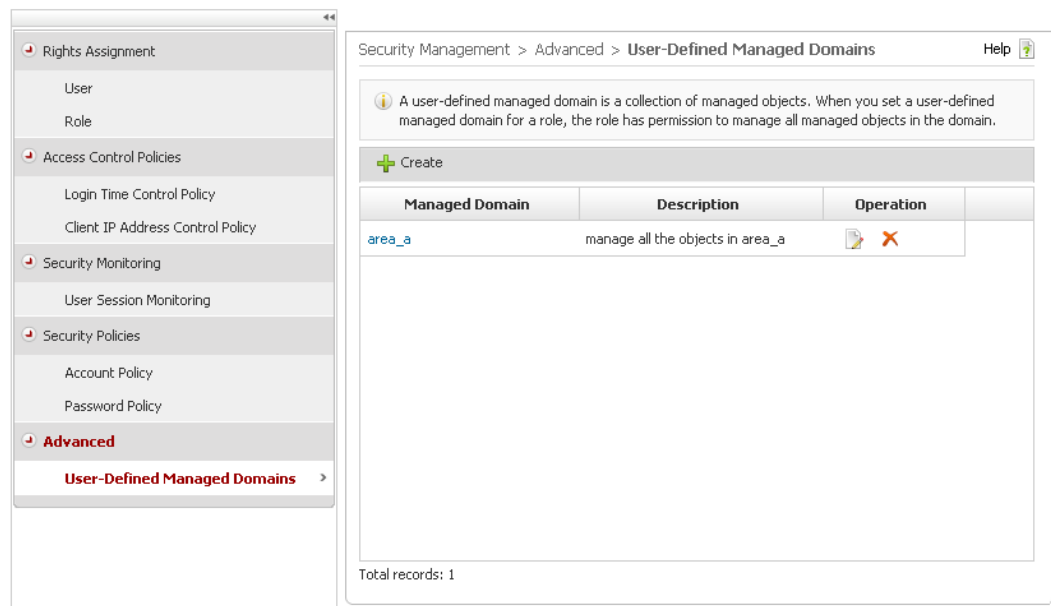
- Step 1** Choose **System > Security Management** from the main menu.

Figure 2-12 Security management



**Step 2** In the **Security Management** window, choose **Advanced > User-Defined Managed Domains**.

Figure 2-13 Setting user-defined managed domains



**Step 3** In the **User-Defined Managed Domains** page, perform the operations described in the following table.

| Operation                                   | Method                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create a user-defined managed domain</b> | Create a user-defined managed domain as required to manage managed objects in a centralized manner.<br><ol style="list-style-type: none"><li>1. Click <b>Create</b>.</li><li>2. On the <b>Create User-Defined Managed Domain</b> page, Set <b>Name</b> and <b>Description</b>.</li><li>3. Click <b>Add</b>. In the <b>Select Managed Objects</b> dialog box, select managed objects. Click <b>OK</b>.</li><li>4. Click <b>OK</b>.</li></ol> |
| <b>View a user-defined managed domain</b>   | You can learn about the details by viewing a user-defined managed domain.<br>Click the required managed domain name in the <b>Managed Domain</b> column. On the <b>View User-Defined Managed Domain</b> page, view the details of the managed domain.                                                                                                                                                                                       |
| <b>Modify a user-defined managed domain</b> | You can modify a user-defined managed domain as required.<br><ol style="list-style-type: none"><li>1. Click  in the <b>Operation</b> column where the required managed domain is located.</li><li>2. On the <b>Modify User-Defined Managed Domain</b> page, modify the user-defined managed domain.</li><li>3. Click <b>OK</b>.</li></ol>                  |
| <b>Delete a user-defined managed domain</b> | You can delete an unused user-defined managed domain.<br><ol style="list-style-type: none"><li>1. Click  in the <b>Operation</b> column where the required managed domain is located.</li><li>2. Click <b>Yes</b> in the <b>Confirm</b> dialog box.</li></ol>                                                                                            |

----End

## 2.3.2 Creating a Role

This topic describes how to create a role. When the default roles of the eSight cannot meet the user authorization requirements, you can create roles to ensure security of the eSight and facilitate network management.

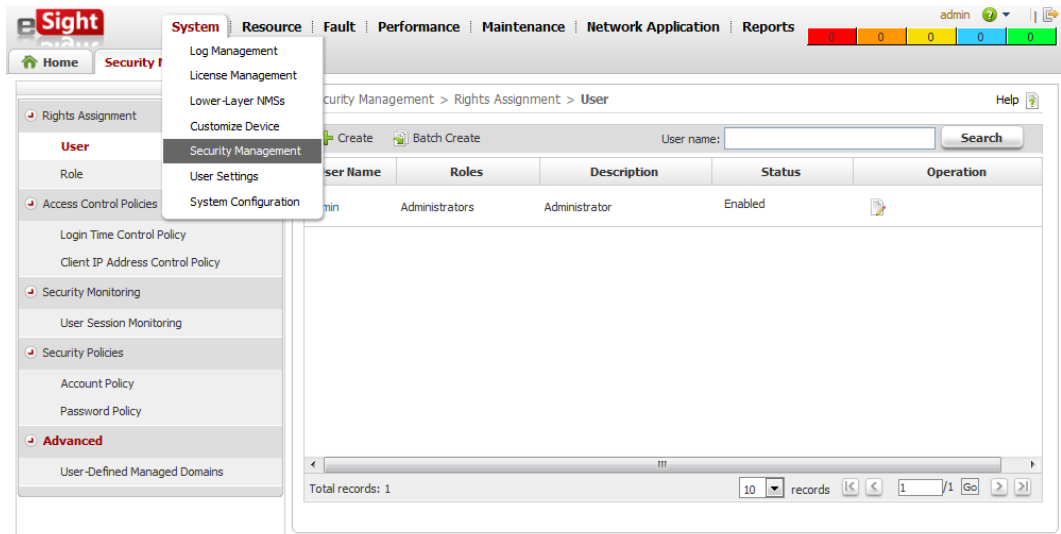
### Prerequisites

You have the operation rights for **Security Management**.

### Procedure

**Step 1** Choose **System > Security Management** from the main menu.



**Figure 2-14** Security management

**Step 2** In the **Security Management** window, choose **Rights Assignment > Role**.

**Step 3** On the **Role** page, click **Create**.

**Figure 2-15** Creating a role

**Step 4** Set the basic information on the **Create Role** page.

1. In the **Basic Info** step, set **Role name** and **Description**.

**Figure 2-16** Setting basic information

Security Management > Rights Assignment > Role > **Create Role** Help ?

Basic Info   Select Managed Objects   Select Operations   Summary

\* Role name:

Description:

Select users:

User name:

|                          | User Name | Description   |
|--------------------------|-----------|---------------|
| <input type="checkbox"/> | admin     | Administrator |
| <input type="checkbox"/> | micheal   |               |

Total records: 2   10 records   1 / 1  

| Selected Users: |           |
|-----------------|-----------|
| User Name       | Operation |
| No record.      |           |

2. **Optional:** Select users.

- You can select users from the user list. After a role is created, a specified user has the management rights and operation rights of the role.



**NOTE**

- You can select users from the list or by searching for user names.
  - You can delete the selected users in the **Selected Users** area.
  - After a role is created, when you create users, you can allocate the role to these users. These users have the management rights and operation rights of the role.
3. Click **Next**.

**Step 5** Select managed objects to enable the role to have the management rights of a specified managed domain.

- In the **Select Managed Objects** step, click **Add**.

**Figure 2-17** Adding managed objects

Security Management > Rights Assignment > Role > **Create Role** Help ?

Basic Info **Select Managed Objects** Select Operations Summary

 Add  Delete

| <input type="checkbox"/> | Managed Object | Type | Path |
|--------------------------|----------------|------|------|
| No record.               |                |      |      |

Total records: 0

Previous

Next

Cancel

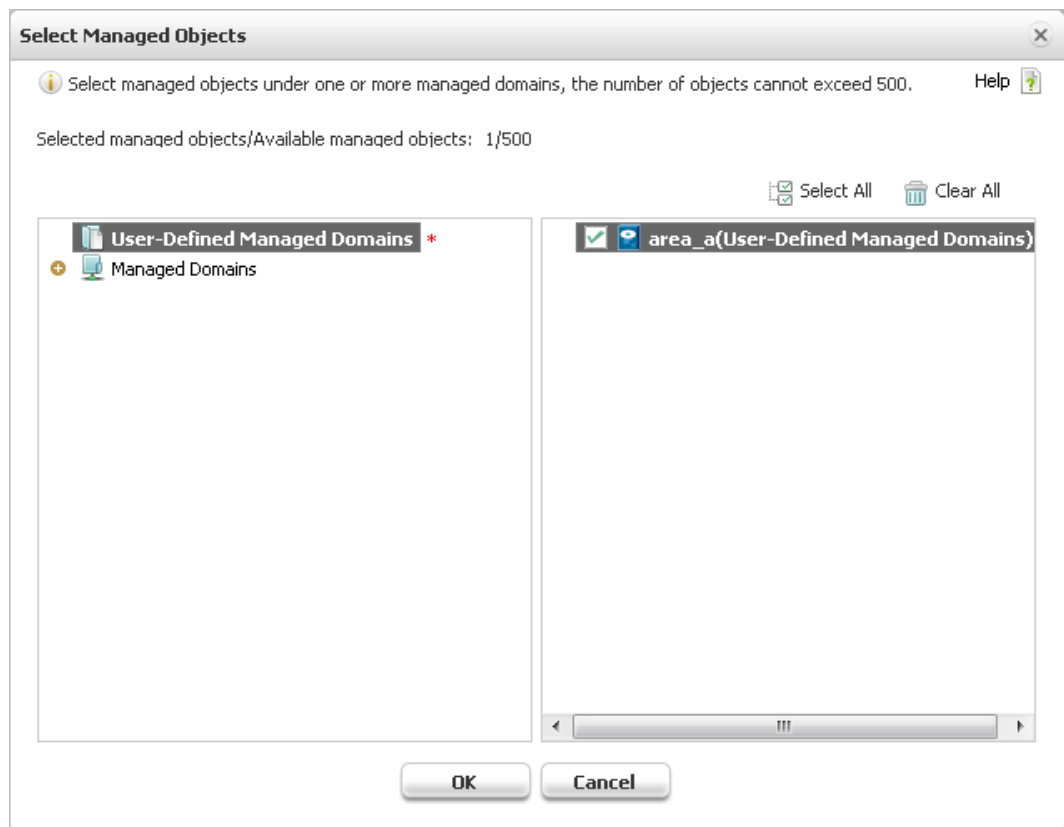


**NOTE**

You can select managed objects in the default managed domain or user-defined managed domain. For details about how to create a user-defined managed domain, see [2.3.1 Setting a User-Defined Managed Domain](#).

2. In the **Select Managed Objects** dialog box, select managed objects.

**Figure 2-18** Selecting managed objects

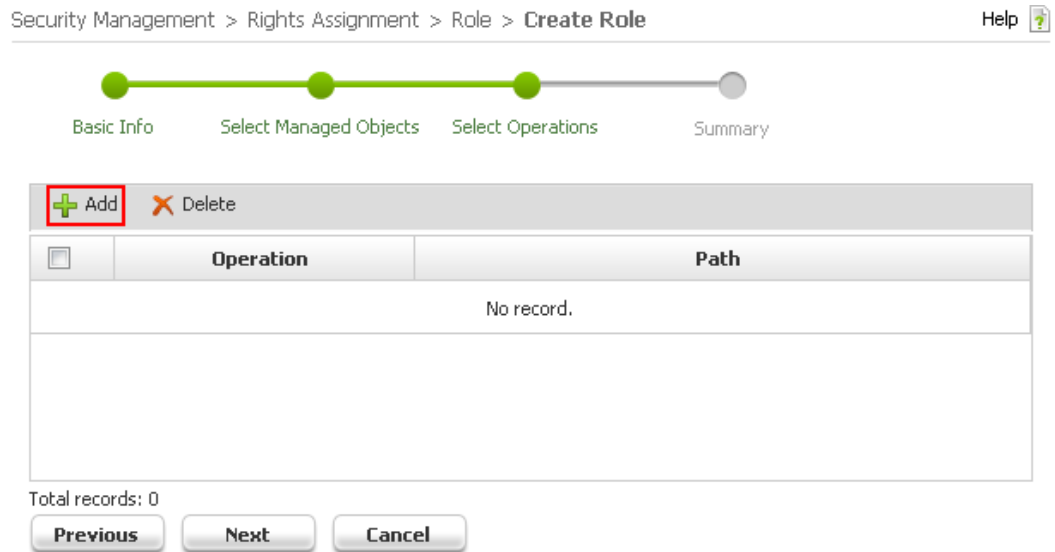


3. Click **OK**.
4. Click **Next**.

**Step 6** Select operations to make the role have the specified operation rights.

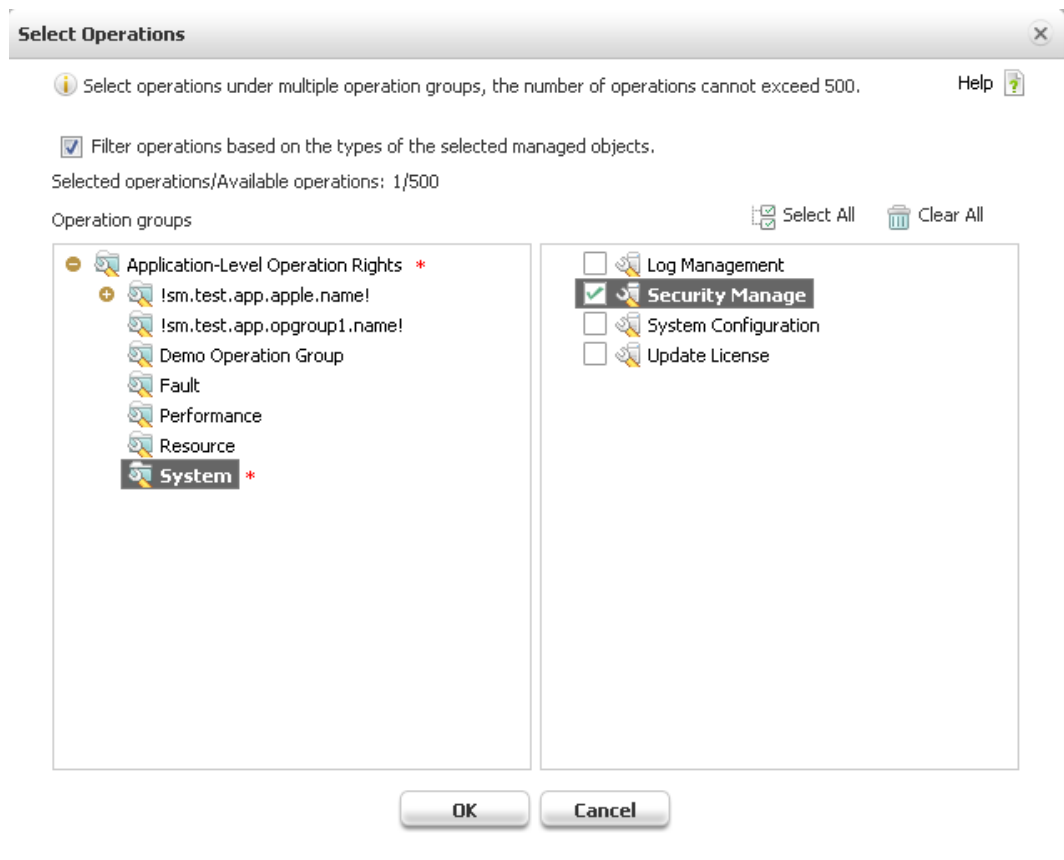
1. In the **Select Operations** step, click **Add**.

**Figure 2-19** Adding operations



2. In the **Select Operations** dialog box, select operations.

**Figure 2-20** Selecting operations



3. Click **OK**.

4. Click **Next**.

### Step 7 Summary.

1. In the **Summary** step, check the role settings.

**Figure 2-21** Confirmation

Security Management > Rights Assignment > Role > **Create Role** Help ?

Basic Info   Select Managed Objects   Select Operations   **Summary**

Role name: role\_a

Description: own the Security Management rights of area\_a

**Users**   Managed Objects   Operation Rights

| User Name  | Description |
|------------|-------------|
| No record. |             |

Total records: 0

**Previous**   **Finish**   **Cancel**

2. Click **Finish**.

----End

## Follow-up Procedure

The following table describes the operations that you can perform on the **Role** page after you create a role.

| Role Maintenance Operation | Procedure                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View role information      | You can learn about the details of a role.<br>In the <b>Role Name</b> column, click the required role name. On the <b>View Role</b> page, view the details of the role.                                                                                                                                                                                                       |
| Modify role information    | You can modify role information as required.<br><ol style="list-style-type: none"><li>1. Click  in the <b>Operation</b> column where the required role information is located.</li><li>2. On the <b>Modify Role</b> page, change the values of <b>Description</b>, <b>Users</b>,</li></ol> |

| Role Maintenance Operation | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <p><b>Managed Objects</b>, and <b>Operation Rights</b>. For details about how to change the value of <b>Users</b>, see step <a href="#">Step 4</a> under <b>Create Role</b>; for details about how to change the value of <b>Managed Objects</b>, see step <a href="#">Step 5</a> under <b>Create Role</b>; for details about how to change the value of <b>Operation Rights</b>, see step <a href="#">Step 6</a> under <b>Create Role</b>.</p> <p>3. Click <b>OK</b>.</p> |
| Delete a role              | <p>You can delete an unused role.</p> <ol style="list-style-type: none"><li>1. Click  in the <b>Operation</b> column where the required role information is located.</li><li>2. In the <b>Confirm</b> dialog box, click <b>Yes</b>.</li></ol>                                                                                                                                             |

## 2.3.3 Creating Users

This topic describes how to create users. When the default user of the eSight cannot meet the network management requirements, you can create users to ensure security of the eSight and facilitate network management.

### Prerequisite

- You have the operation rights for **Security Management**.
- You learn about the user account policy and password policy.

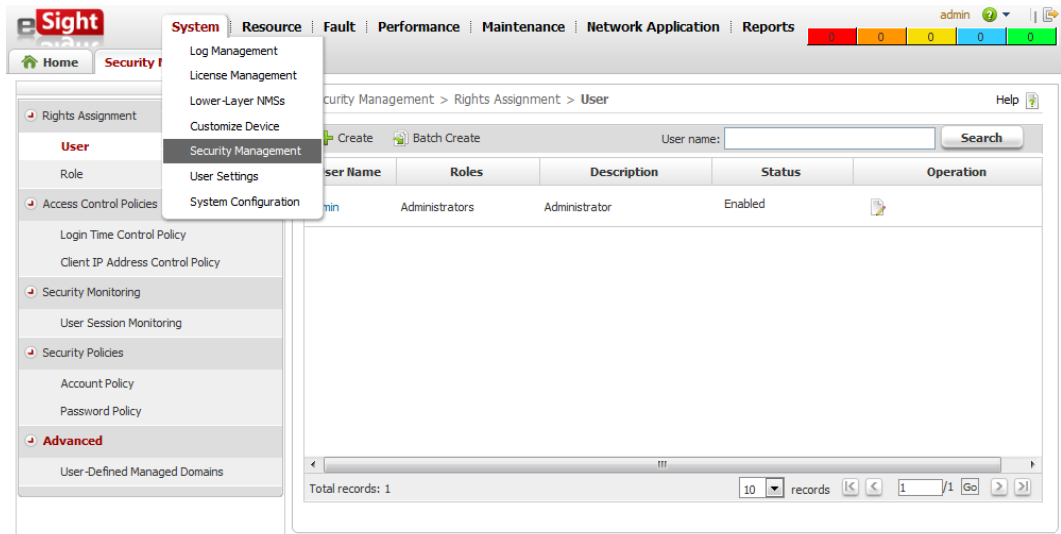
For details about how to set an account policy or a password policy, see [2.2.1 Setting an Account Policy](#) and [2.2.2 Setting a Password Policy](#).

### Context

- Users can be created one by one or in batches. To create users in batches, import a template in .xls format to the eSight.
- A maximum of 1000 users can be created. When the number of users to be created reaches 1000, the eSight stops creating the remaining users.
- You must manually set the user name and password. For the other properties, you can use default values or set them after you create the user account successfully.

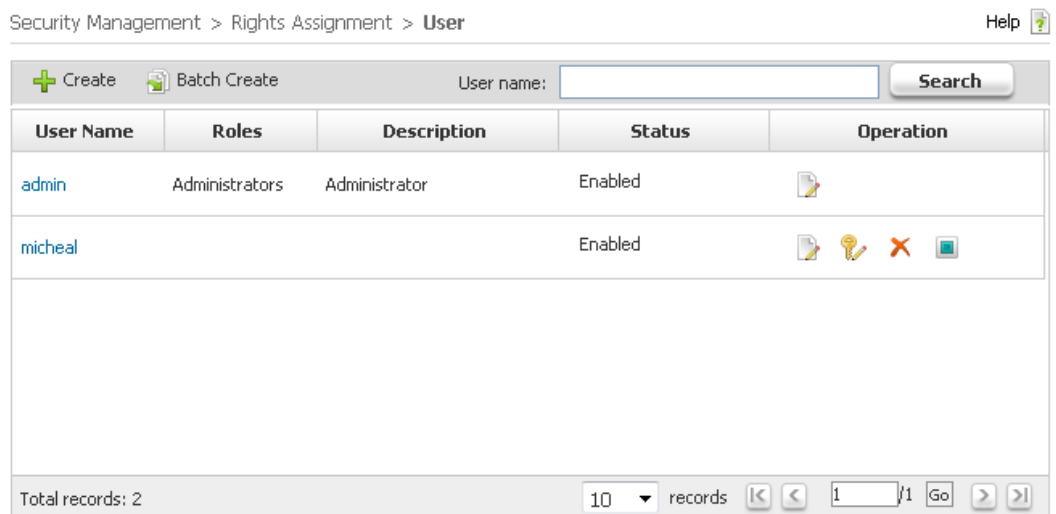
### Procedure

**Step 1** Choose **System > Security Management** from the main menu.

**Figure 2-22** Security management

**Step 2** In the **Security Management** window, choose **Rights Assignment > User**.

**Step 3** On the **User** page, select a method of creating users.

**Figure 2-23** Creating users

- **Create users one by one.**

If only a few users are required, create the users one by one.

1. Click **Create**.
2. On the **Create User** page, set the basic information.
  - a. In the **Basic Info** step, set **User name**.



**Figure 2-24** Setting basic information

Security Management > Rights Assignment > User > **Create User** Help ?

● — ● — ●  
Basic Info      Roles      Access Control Policies

|                        |                                                                         |
|------------------------|-------------------------------------------------------------------------|
| <b>* User name:</b>    | <input style="width: 80%;" type="text" value="user_a"/>                 |
| <b>* Password:</b>     | <a href="#">Set Password</a>                                            |
| <b>Account status:</b> | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| <b>Description:</b>    | <input style="width: 80%;" type="text" value="area_a"/>                 |

- b. Click **Set Password** next to **Password**. In the displayed window, set **Password** and **Confirm password**.

**Figure 2-25** Setting a password

|                            |                                                               |
|----------------------------|---------------------------------------------------------------|
| <b>* Password:</b>         | <input style="width: 80%;" type="password" value="••••••••"/> |
| <b>* Confirm password:</b> | <input style="width: 80%;" type="password" value="••••••••"/> |

**The password must meet the following rules:**

- 1, The password is different from the user name.
- 2, The length ranges from 6 to 32 characters.
- 3, The number of occurrences of a character in a password cannot exceed 3.
- 4, The password contains uppercase and lowercase letters and digits.

- c. Set **Account status** to **Enabled**.
- d. Click **Next**.
3. On the **Create User** page, set a role for the user. The user has the management rights and operation rights of the role.
  - a. In the **Roles** step, select the role.

**Figure 2-26** Selecting the role

Security Management > Rights Assignment > User > **Create User** Help ?

Basic Info Roles Access Control Policies

Select roles:

| <input type="checkbox"/>            | Role Name      | Description                                  |
|-------------------------------------|----------------|----------------------------------------------|
| <input type="checkbox"/>            | Administrators | Administrator role                           |
| <input checked="" type="checkbox"/> | role_a         | own the Security Management rights of area_a |

Total records: 2

**NOTE**

In the **Role Name** column, click the required role name. In the **View Role** dialog box, view the details of the role.

b. Click **Next**.

4. On the **Create User** page, set an access control policy for the user. The user can login the eSight by using a specified IP address within the specified period of time.
  - a. In the **Access Control Policies** step, select a login time control policy and an IP address range.

**Figure 2-27** Setting access control policies

Security Management > Rights Assignment > User > **Create User** Help ?

Basic Info Roles Access Control Policies

Select a time control policy: + Create

|                                  | Policy         | Description                                          | Start and End Dates   | Daily start and end times | Week                                                           |
|----------------------------------|----------------|------------------------------------------------------|-----------------------|---------------------------|----------------------------------------------------------------|
| <input checked="" type="radio"/> | Default Policy | The default policy allows you to log in at any time. | --                    | 00:00~23:59               | Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday |
| <input type="radio"/>            | Time_policy_a  |                                                      | 2012-07-10~2013-07-10 | 09:00~18:30               | Monday, Tuesday, Wednesday, Thursday, Friday, Saturday         |

Total records: 2

Select a range of IP addresses you access: + Create

| <input checked="" type="checkbox"/> | IP Address Range         | Description |
|-------------------------------------|--------------------------|-------------|
| <input checked="" type="checkbox"/> | 12.64.54.25~23.64.54.255 | IP_policy_a |

Total records: 1

Previous Finish Cancel

**NOTE**

- If the required login time control policy does not exist in the **Policy** list, you can click **Create** to create it. For details about how to create a login time control policy, see [2.2.3.1 Setting a Login Time Control Policy](#).
- If the required client IP address control policy does not exist in the **IP Address Range** list, you can click **Create** to create it. For details about how to create a client IP address control policy, see [2.2.3.2 Setting a Client IP Address Control Policy](#).

b. Click **Finish**.

- **Create users in batches.**

If a large number of users are required, create the users in batches to improve operation efficiency.

1. Click **Batch Create**.
2. On the **Batch Create Users** page, click **Template.xls** next to **Download template** to download the template to a local disk.

**Figure 2-28** Creating users in batches

Security Management > Rights Assignment > User > **Batch Create Users** Help 

 The maximum allowable number of users in the system is 1000, you can import 997 users.

Download template: [Template.xls](#)

\* Upload user information:    

**Operation result**

| User Name  | Disable or Not | Description | Role | Time Profile | Terminal Profile | Import Result |
|------------|----------------|-------------|------|--------------|------------------|---------------|
| No record. |                |             |      |              |                  |               |

- Open the template on the local disk, enter the user information, and save the template.

**NOTE**

A user cannot be created if the user information is incorrect.

- On the **Batch Create Users** page, click  next to **Upload user information** to import the template saved on the local disk.

You can click  to remove the selected template and select another one.

- Click  to upload the template.

The eSight automatically creates users based on the user information in the template.

- In the **Operation result** dialog box, confirm the result of creating users in batches, and click **OK**.

The detailed information about the created users is displayed in the operation result list.

**NOTE**

You can view user details in the user list on the **User** page.

----End

## Follow-up Procedure

The following table describes the operations that you can perform on the **User** page after you create a user.

| User Maintenance Operation | Procedure                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View user information      | You can learn about the details of a user.<br>In the <b>User Name</b> column, click the required user name.<br>On the <b>View User</b> page, view the details of the user.                                                                                                                                                                                  |
| Modify user information    | You can modify user information as required.<br><ol style="list-style-type: none"><li>Click  in the <b>Operation</b> column where the required user information is located, and then modify it.</li><li>On the <b>Modify User</b> page, modify the settings of</li></ol> |

| User Maintenance Operation | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <b>Basic Info, Roles, and Access Control Policies.</b><br>3. Click <b>OK</b> .                                                                                                                                                                                                                                                                                                                                                                               |
| Delete a user              | You can delete an unused user.<br><br>1. Click  in the <b>Operation</b> column where the required user information is located.<br>2. In the <b>Confirm</b> dialog box, click <b>Yes</b> .                                                                                                                                                                                   |
| Reset password             | If a user forgets the password when logging to the eSight, the user can use the new password to log in after the password is reset.<br><br>1. Click  in the <b>Operation</b> column where the required user information is located.<br>2. In the displayed window, set <b>New password</b> and <b>Confirm password</b> based on the password rules.<br>3. Click <b>OK</b> . |
| Enable a user              | If an account is not used for a long time and maximum number of days the account is not used continuously is reached, the account is disabled. To use the account again, you can enable the user account.<br><br>Click  in the <b>Operation</b> column where the required user information is located.                                                                    |
| Disable a user             | You can disable a user account when you do not use the user account.<br><br>Click  in the <b>Operation</b> column where the required user information is located.                                                                                                                                                                                                         |

## 2.4 Monitoring the User

You can learn about the information about sessions and operations by monitoring the sessions and operations of the users who are logged in to the eSight. When some unauthorized sessions or operations are detected, you can force the related users to log out, ensuring security of the eSight.

### 2.4.1 Monitoring User Sessions

This topic describes how to monitor user sessions. This function helps you learn about the information about the users who log in to the eSight.

#### Prerequisites

You have the operation rights for **Security Management**.

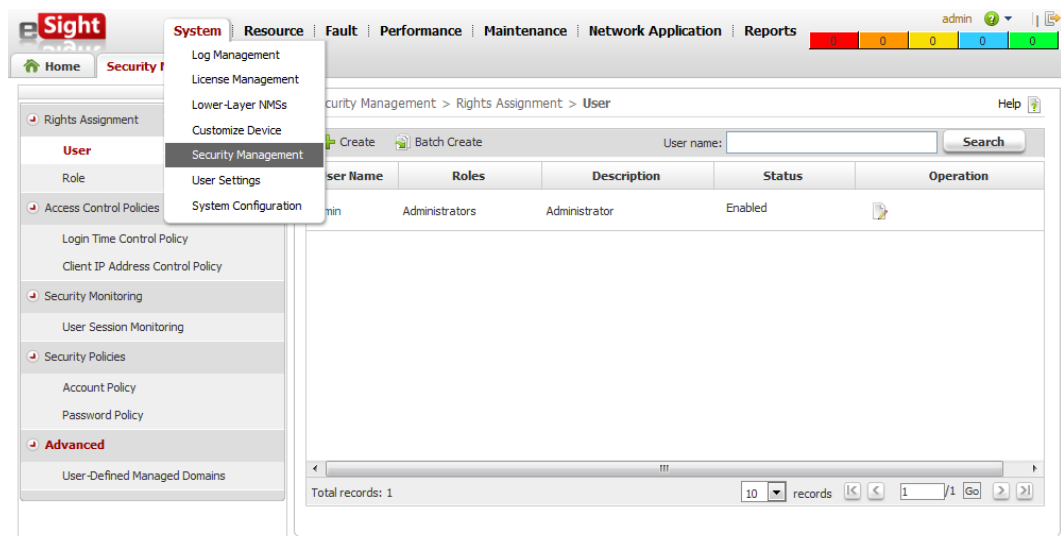
## Context

- A session refers to the connection established between the client and the server. The session starts when a user logs in to the client, and ends when the user logs out of the client.
- Multiple sessions can be created by using one user account.

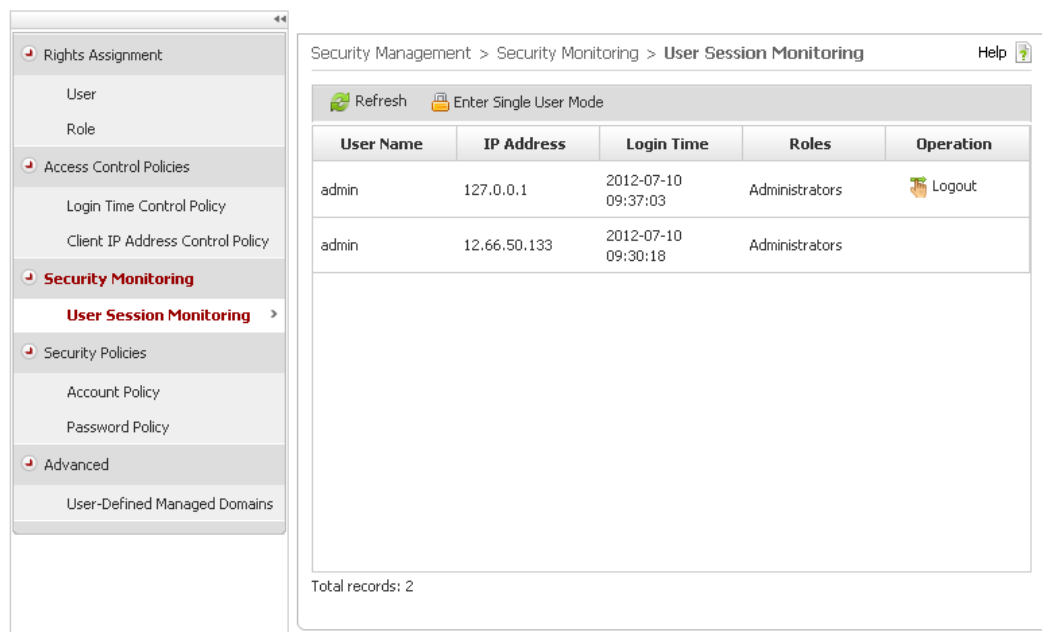
## Procedure

**Step 1** Choose **System > Security Management** from the main menu.

**Figure 2-29** Security Management



**Step 2** In the **Security Management** window, choose **Security Monitoring > User Session Monitoring**.

**Figure 2-30** User session monitoring

**Step 3** On the **User Session Monitoring** page, perform the operations listed in the following table.

| Monitor user sessions   | Operation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View user sessions      | View the session information about online users in the user session list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Update user sessions    | Click <b>Refresh</b> to refresh the user session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Force a user to log out | For details, see <a href="#">2.4.2 Forcing a User to Log Out</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Enter Single User Mode  | <p>When you want to maintain the eSight server, you can choose to make the system enter single user mode.</p> <ol style="list-style-type: none"><li>Click <b>Enter Single User Mode</b>.</li><li>In the <b>Confirm</b> dialog box, click <b>Yes</b>.</li></ol> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>After the system enters single user mode, the eSight only allows the current user to log in to the eSight, and other online users are forcibly logged out.</li><li>You need to make the system exit single user mode immediately you complete maintenance operations. In this way, other users can use the eSight properly.</li></ul> |
| Exit Single User Mode   | <p>You need to exit single user mode after completing maintenance operations.</p> <p>Click <b>Exit Single User Mode</b>.</p> <p><b>NOTE</b></p> <p>After you exit single user mode, other users can log in to the eSight again.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |

----End

## 2.4.2 Forcing a User to Log Out

This topic describes how to force a user to log out. You can force the corresponding users to log out when some dangerous operations or invalid sessions are detected during the monitoring or session.

### Prerequisites

You have the operation rights for **Security Management**.

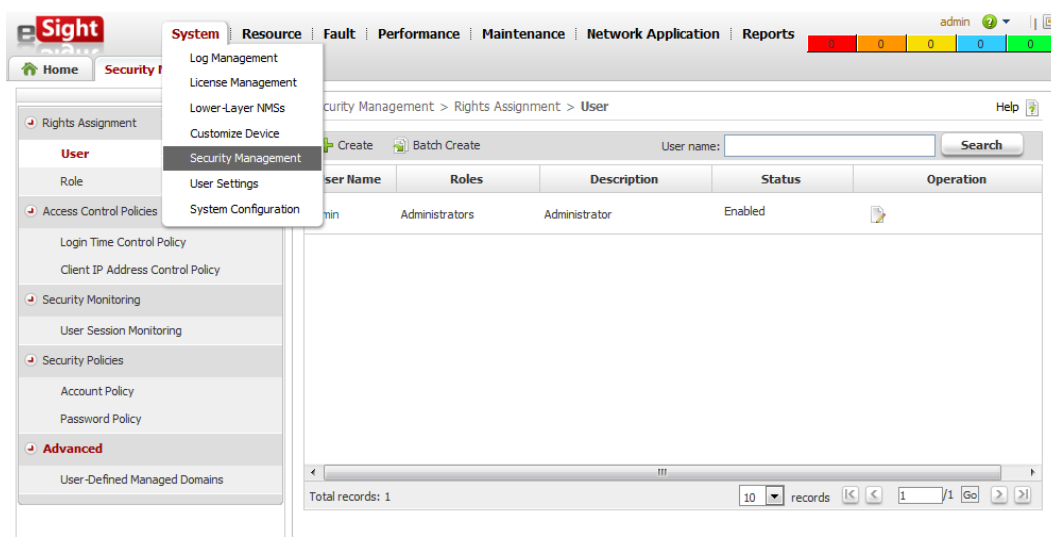
### Context

- This function is applicable only for the user account that generates an illegal session.
- If you log in, you cannot force yourself to log out.

### Procedure

**Step 1** Choose **System > Security Management** from the main menu.

**Figure 2-31** Security management



**Step 2** In the **Security Management** window, choose **Security Monitoring > User Session Monitoring**.

**Step 3** Click  **Logout** in the **Operation** column where the required user information is located.



**Figure 2-32** Forced logging out

Security Management > Security Monitoring > User Session Monitoring Help 

 Refresh  Enter Single User Mode

| User Name | IP Address    | Login Time             | Roles          | Operation                                                                                  |
|-----------|---------------|------------------------|----------------|--------------------------------------------------------------------------------------------|
| micheal   | 12.67.192.154 | 2012-07-10<br>10:05:56 |                |  Logout |
| admin     | 12.66.50.133  | 2012-07-10<br>10:05:04 | Administrators |                                                                                            |

Total records: 2

**Step 4** Click **Yes** in the **Confirm** dialog box.

----End

## 2.5 Example: Typical Security Management Operations

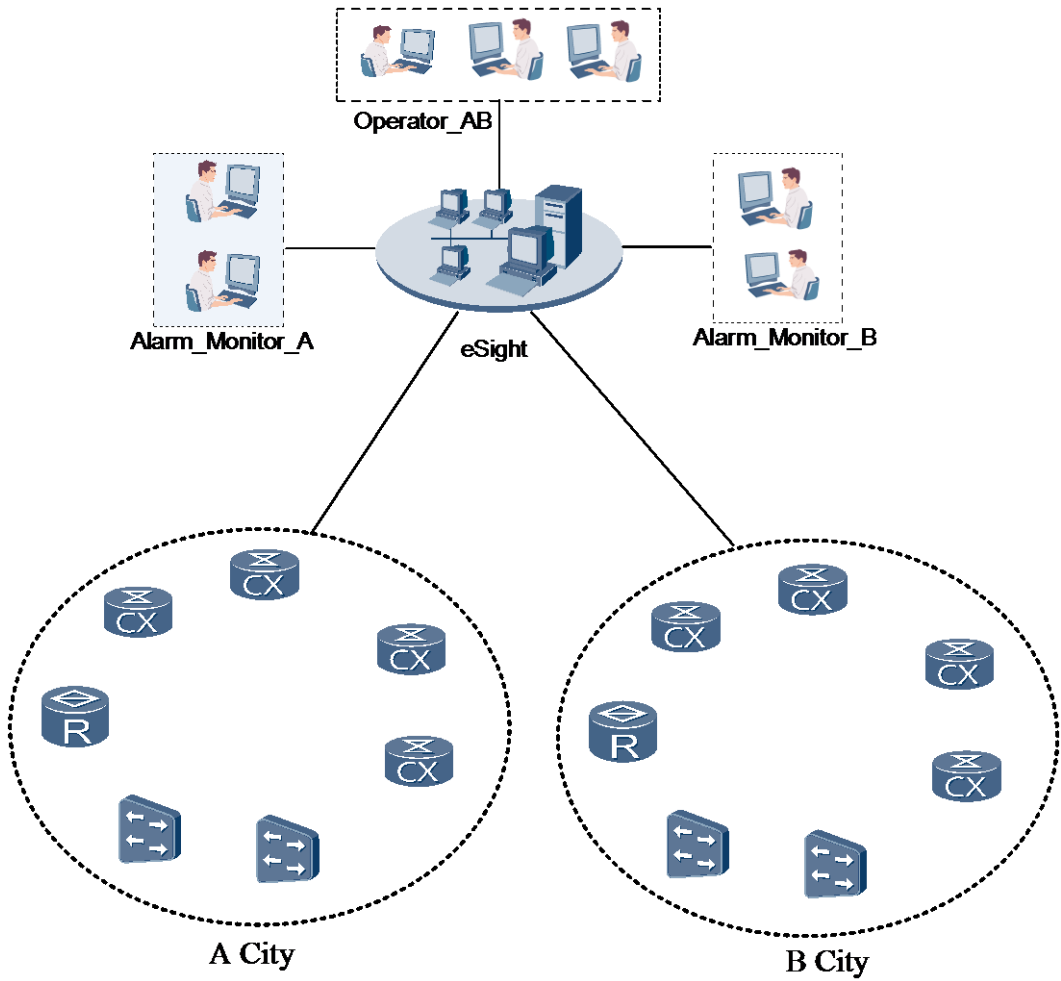
In the eSight, only after you set a role for a user, the user has the operation rights of the role in its managed domains. This topic describes how to create an eSight user and assign rights to the user.

### Application Scenario

The eSight can manage the NEs in an office in a centralized manner. The NEs in the office are allocated to two user-defined managed domain by region, namely, city A and city B, and monitored and maintained by different engineers. To help the engineers to monitor and maintain the NEs by using the eSight, you need to assign accounts and rights for them.

Figure 2-33 shows the network diagram in the current scenario.

Figure 2-33 Rights- and domain-based network diagram



Data Planning

To monitor and maintain NEs in a centralized manner, you can allocate the NEs to two user-defined managed domains, city A and city B.

Based on role responsibilities, the following three roles are planned.

Table 2-2 Role planning

| Role                    | Function                                                                       | Managed Domain           | Operated Rights                                                     |
|-------------------------|--------------------------------------------------------------------------------|--------------------------|---------------------------------------------------------------------|
| Administrators          | Performs operation and maintenance operations on the NEs in city A and city B. | NEs in city A and city B | Has the default operation rights of the eSight super administrator. |
| Alarm monitor of City A | Monitors alarms of the NEs in city A.                                          | NEs in city A            | Browses the masked alarms.<br>Browses historical alarms             |

| Role                    | Function                              | Managed Domain | Operated Rights                                                                  |
|-------------------------|---------------------------------------|----------------|----------------------------------------------------------------------------------|
|                         |                                       |                | Browses the event list                                                           |
| Alarm monitor of City B | Monitors alarms of the NEs in city B. | NEs in city B  | Browses the masked alarms<br>Browses historical alarms<br>Browses the event list |

Based on user responsibilities, the following three users are planned.

**Table 2-3** User planning

| User Name       | Function                                | Role                    |
|-----------------|-----------------------------------------|-------------------------|
| Operator_AB     | Maintains the NEs in city A and city B. | Administrators          |
| Alarm_Monitor_A | Monitors alarms of the NEs in city A.   | Alarm monitor of City A |
| Alarm_Monitor_B | Monitors alarms of the NEs in city B.   | Alarm monitor of City B |

## Configuration Procedure

To create an eSight user and assign rights to the user, perform the following steps:

- Create two user-defined managed domains: city A and city B.
  - Choose **System > Security Management** from the main menu.
  - In the **Security Management** window, choose **Advanced > User-Defined Managed Domains**.
  - On the **User-Defined Managed Domains** page, click **Create**. Then set **Name** to **City A** and click **Add**.
  - In the **Select Managed Objects** dialog box, select all the NEs in city A.
  - Click **OK**. All the NEs in city A are added to the user-defined managed domain for city A.
  - Perform steps 1.a through 1.e to create a user-defined managed domain for city B and add all the NEs in city B to the user-defined managed domain.
- Create alarm monitoring roles for city A and city B respectively, and assign the management rights and operations for the roles.
  - Choose **System > Security Management** from the main menu. In the **Security Management** window, choose **Rights Assignment > Role**.
  - On the **Role** page, click **Create**. In the **Basic Info** step, set **Role name** to **Alarm monitor of City A**, and click **Next**.
  - In the **Select Managed Objects** step, click **Add**. In the **Select Managed Objects** dialog box, select the user-defined managed domain for city A and click **OK**.

- d. Click **Next**.
- e. Click **Add**. In the **Select Operations** dialog box, select operation rights based on [Table 2-2](#), and click **OK**.
- f. Click **Next**.
- g. Click **Finish**. The alarm monitoring role for city A is created successfully.
- h. Perform steps [2.a](#) through [2.g](#) to create the alarm monitoring role for city B.



**NOTE**

The Administrators is the default role of the eSight, and the default managed domain manages all the NEs and has all the operation rights. Therefore, you do not need to create the managed domain for the operator role.

3. Create users **Operator\_AB**, **Alarm\_Monitor\_A**, and **Alarm\_Monitor\_B**, and set the roles for the users.
  - a. Choose **System > Security Management** from the main menu. In the **Security Management** window, choose **Rights Assignment > User**.
  - b. On the **User** page, click **Create**. In the **Basic Info** step, set **User name** to **Operator\_AB** and set **Password** and **Confirm password** of the user. Then click **Next**.
  - c. In the **Roles** step, set the role to **Administrators** and click **Next**.
  - d. (Optional)To ensure security of the eSight, you need to perform the following operations in the **Access Control Policies** step:
    - Set login time for different on-duty persons.
    - Bind the IP addresses allowed for login based on the IP address of the workstation in each area.
  - e. Click **Finish**. The user **Operator\_AB** is successfully created.
  - f. Perform steps [3.a](#) through [3.e](#) to create users **Alarm\_Monitor\_A** and **Alarm\_Monitor\_B** and set their roles as the alarm monitor for city A and the alarm monitor for city B.

When the preceding configuration is complete, you can provide the accounts to related personnel.

---

# 3 Resource Management

---

## About This Chapter

Resource management involves adding resources to the eSight for management.

### [3.1 Overview of Resource Management Operations](#)

This topic describes the resource management operations.

### [3.2 Creating a Subnet](#)

To facilitate management, a large network is divided into several subnets according to a specific rule (by region or device type). The smaller networks are called subnets. NEs can be placed under different subnets based on user-defined logic.

### [3.3 Auto Discovery for NEs](#)

The system automatically searches for NEs in a specified network segment based on the specified SNMP and adds the found NEs. When the NEs in a specified network segment will be added, the NE auto-discovery function helps you to perform the operation in batches and save time.

### [3.4 Creating an NE Manually](#)

If you want a few different types of NEs to access the eSight, you can create these NEs one by one.

### [3.5 Importing NEs Manually in Batches](#)

When the system has a lot of managed objects during deployment or device expansion, you can add NEs in batches by using this function.

### [3.6 Adjusting the Relationships Between NEs and Subnets](#)

This topic describes how to adjust the relationships between NEs and subnets as required when the network structure changes.

### [3.7 Adjusting the Relationships Between Subnets](#)

This topic describes how to adjust the relationships between subnets and subnets as required when the network structure changes.

### [3.8 Physical Resource Management](#)

The physical resource management function provides an entry for uniformly querying and collecting statistics on assets on the live network. This helps provide data to guide maintenance, reconstruction, and capacity expansion on the live network.

### 3.9 Creating an SNMP Template

You can select a created SNMP template without entering parameters on pages such as NE creation page.

### 3.10 Link Management

Link management enables you to query link status, and maintain network links. In addition, links are displayed on topology view. You can learn structure change of the network topology on the live network according to the link topology.

### 3.11 Electronic Labels Management

Electronic labels are used in network design, planning, and maintenance, asset management (including spare part management), order, account management, liquidation, invest tracing, and warranty. eSight supports query and export of an electronic label.

### 3.12 Example: Typical Resource Management Operations

This topic describes an example about how to perform resource management operations. From the example, you will learn about the procedure and basic operations about resource management.

## 3.1 Overview of Resource Management Operations

This topic describes the resource management operations.

### Background

Before performing resource management operations, you need to be familiar with the basic concepts about resource management, such as subnets and NEs. See [1.2.2 Basic Concepts of Resource Management](#). Understanding these concepts helps you avoid errors when performing resource management operations.

### Overview of Resource Management Operations

[Figure 3-1](#) shows the overview of resource management operations. For more details, click the operation in the overview.

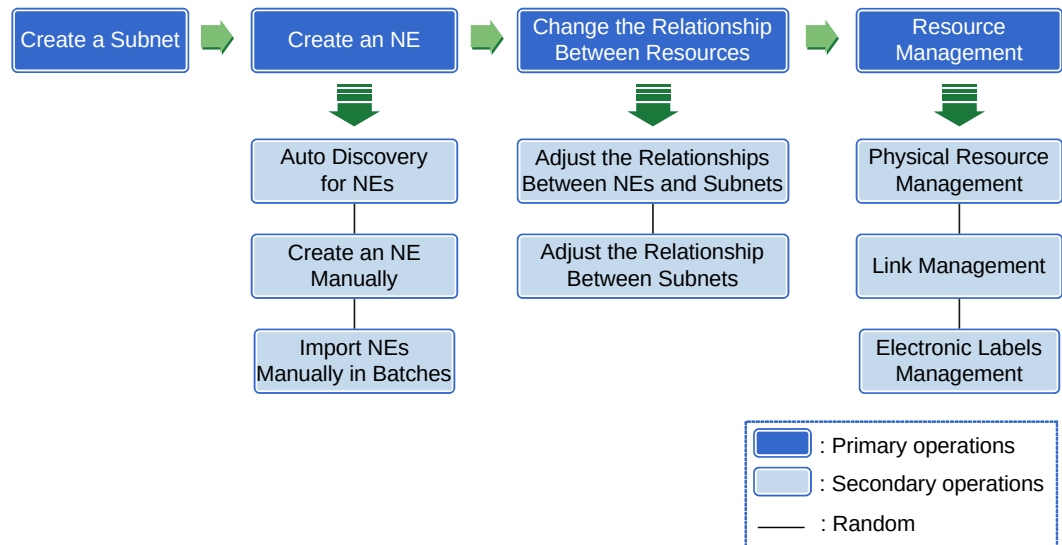
**Figure 3-1** Overview of resource management operations

Table 3-1 describes the resource management operations.

**Table 3-1** Resource management operations

| Operation                                                               | Description                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">3.2 Creating a Subnet</a>                                   | To facilitate management, a large network is divided into several subnets according to a specific rule (by region or device type). The smaller networks are called subnets. NEs can be placed under different subnets based on user-defined logic.                                  |
| <a href="#">3.3 Auto Discovery for NEs</a>                              | The system automatically searches for NEs in a specified network segment based on the specified SNMP and adds the found NEs. When the NEs in a specified network segment will be added, the NE auto-discovery function helps you to perform the operation in batches and save time. |
| <a href="#">3.4 Creating an NE Manually</a>                             | If you want a few different types of NEs to access the eSight, you can create these NEs one by one.                                                                                                                                                                                 |
| <a href="#">3.5 Importing NEs Manually in Batches</a>                   | When the system has a lot of managed objects during deployment or device expansion, you can add NEs in batches by using this function.                                                                                                                                              |
| <a href="#">3.6 Adjusting the Relationships Between NEs and Subnets</a> | This topic describes how to adjust the relationships between NEs and subnets as required when the network structure changes.                                                                                                                                                        |
| <a href="#">3.7 Adjusting the Relationships Between Subnets</a>         | This topic describes how to adjust the relationships between subnets and subnets as required when the network structure changes.                                                                                                                                                    |
| <a href="#">3.8 Physical Resource Management</a>                        | The physical resource management function provides an entry for uniformly querying and collecting statistics on assets on the live network. This helps provide data to guide maintenance, reconstruction, and capacity expansion on the live network.                               |

| Operation                                         | Description                                                                                                                                                                                                                                                 |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">3.10 Link Management</a>              | Link management enables you to query link status, and maintain network links. In addition, links are displayed on topology view. You can learn structure change of the network topology on the live network according to the link topology.                 |
| <a href="#">3.11 Electronic Labels Management</a> | Electronic labels are used in network design, planning, and maintenance, asset management (including spare part management), order, account management, liquidation, invest tracing, and warranty. eSight supports query and export of an electronic label. |

## 3.2 Creating a Subnet

To facilitate management, a large network is divided into several subnets according to a specific rule (by region or device type). The smaller networks are called subnets. NEs can be placed under different subnets based on user-defined logic.

### Prerequisites

You have the operation rights for **Access Resource**.

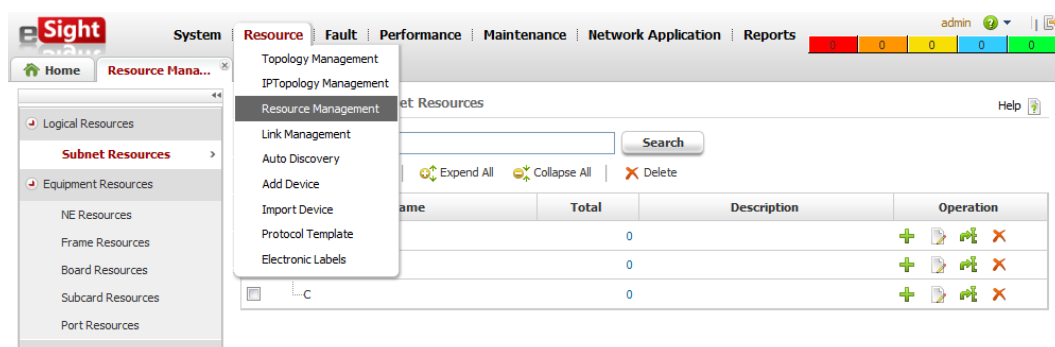
### Context

- You can create subnets under a subnet.
- You can click  to move NEs to a newly created subnet. For details, see [3.6 Adjusting the Relationships Between NEs and Subnets](#).
- A subnet has a maximum of 10 subordinate subnets.
- It is recommended that a subnet contain a maximum of 500 NEs.

### Procedure

**Step 1** Choose **Resource > Resource Management** from the main menu.

**Figure 3-2** Resource Management

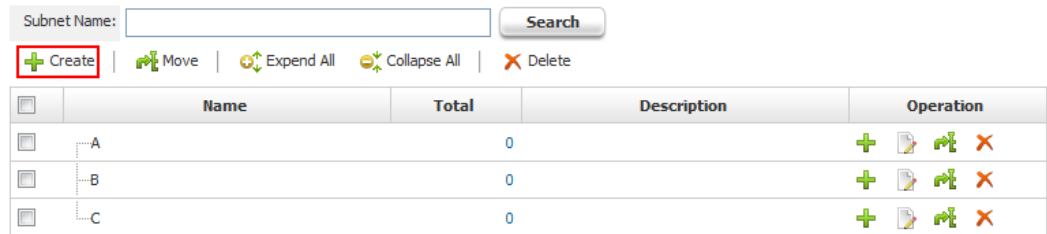




**Step 2** Choose **Logical Resources > Subnet Resources**.

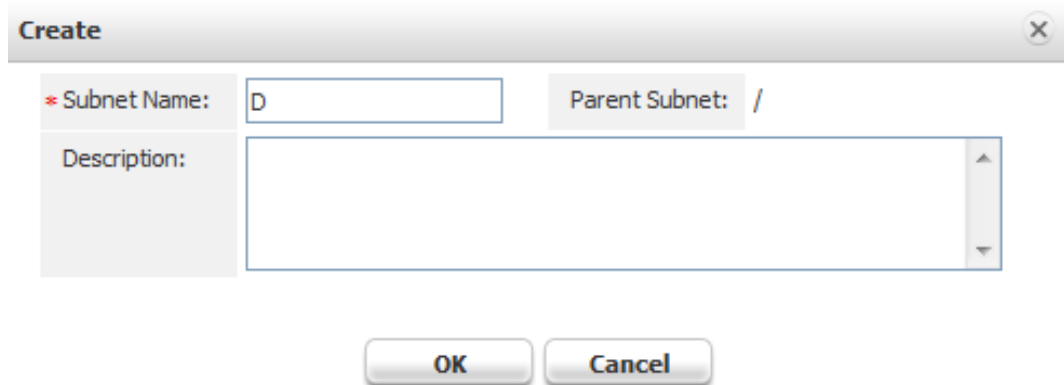
**Step 3** Click **Create** on the **Subnet Resources** page.

**Figure 3-3** Creating a subnet



**Step 4** Set **Subnet Name** and **Description**.

**Figure 3-4** Setting parameters



**Step 5** Click **OK**.



**NOTE**

Click **Apply** to create more subnets of the same type.

- If the subnet is created successfully, the subnet is displayed in the navigation tree and managed object list.
- If the subnet cannot be created, the system prompts the reason for the failure. Click **OK** to set the parameters again.

----End

## Follow-up Procedure

The following table describes the operations that you can perform after you successfully create a subnet.

| Maintaining Subnets       | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modify subnet information | <p>In the eSight, you can modify the attributes of a subnet, such as the subnet name.</p> <ol style="list-style-type: none"><li>1. In the managed object list on the right of the <b>Resource Management</b> window, click  in the <b>Operation</b> column where the target subnet is located.</li><li>2. On the page for modifying subnet information, modify the configuration parameters of the subnet.</li><li>3. Then click <b>OK</b>.</li></ol>                                                                          |
| Delete a subnet           | <p>You can delete the subnets that do not need to be managed by the eSight.</p> <ol style="list-style-type: none"><li>1. In the managed object list on the right of the <b>Resource Management</b> window, delete subnets.<ul style="list-style-type: none"><li>– To delete a subnet, click  in the <b>Operation</b> column where the subnet is located.</li><li>– To delete multiple subnets, select them and click <b>Batch Delete</b>.</li></ul></li><li>2. In the <b>Confirm</b> dialog box, click <b>Yes</b>.</li></ol> |

## 3.3 Auto Discovery for NEs

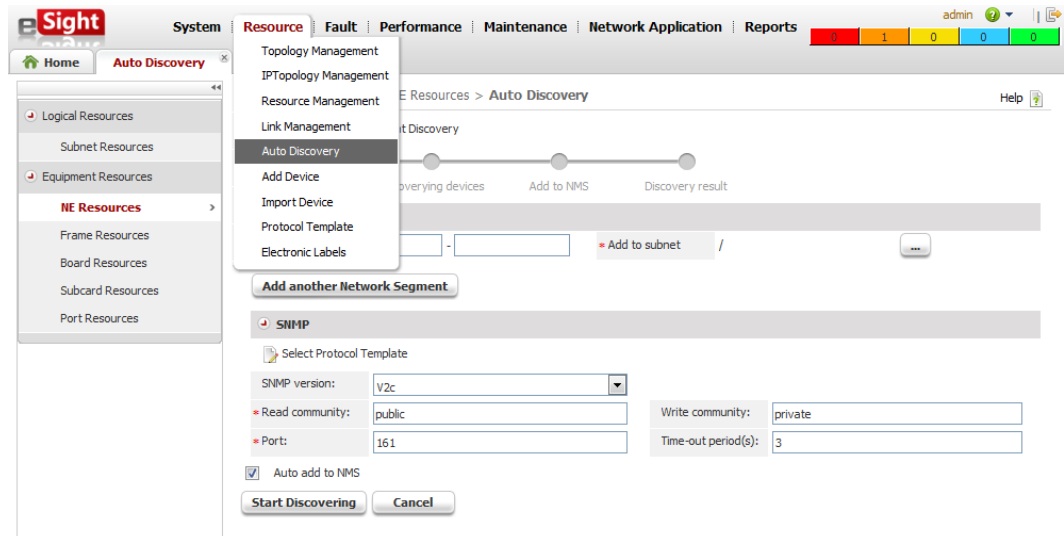
The system automatically searches for NEs in a specified network segment based on the specified SNMP and adds the found NEs. When the NEs in a specified network segment will be added, the NE auto-discovery function helps you to perform the operation in batches and save time.

### Prerequisites

- You have the operation rights for **Access Resource**.
- NEs support the SNMP version specified by the eSight.

### Procedure

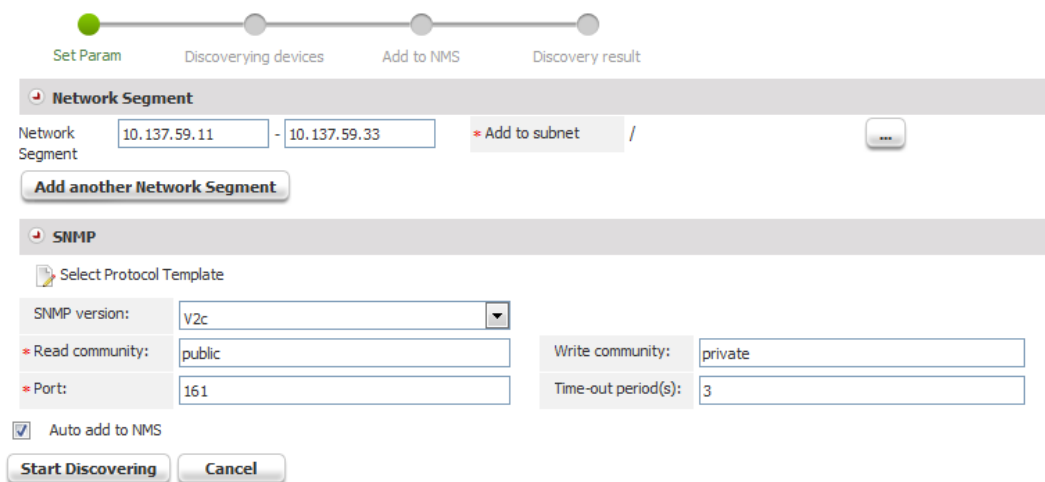
**Step 1** Choose **Resource > Auto Discovery** from the main menu.

**Figure 3-5** Discovering NEs automatically

**Step 2** On the **Network Segment Discovery** page, set network segment discovery parameters and SNMP parameters.

**NOTE**

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. To add an SNMP template, see [3.9 Creating an SNMP Template](#).

**Figure 3-6** Setting automatic discovery parameters

**Step 3 Optional:** Select **Auto add to NMS**.

**NOTE**

- If **Auto add to NMS** is selected, the discovered NEs are automatically added. The [Step 5](#) is skipped.
- If **Auto add to NMS** is not selected, you need to execute the [Step 5](#) to add the discovered NEs.

**Step 4** Click **Start Discovering**.

The discovered NEs are displayed in the list.

**NOTE**

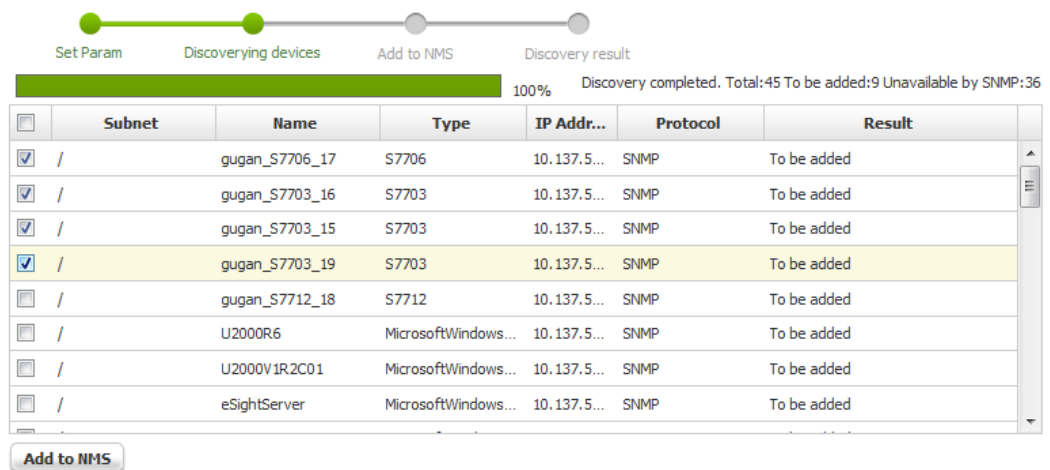
You can click **Stop Discovering** to stop the discover operation.

**Step 5** Select NEs in the list and click **Create**.

If **Auto add to NMS** is selected, this step is skipped.

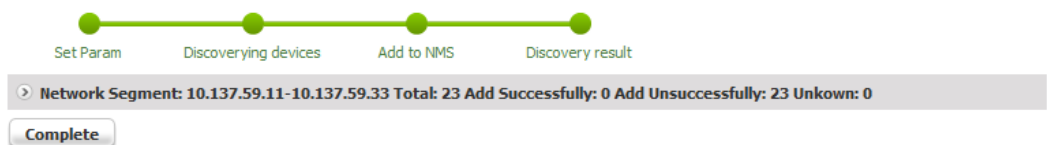
- If the NE is created successfully, the **Result** column is **Add success**.
- If the NE fails to be created, the **Result** column displays **Add fail** and the reason for the failure.

**Figure 3-7** Adding the NEs



**Step 6** Click **Show Discovery Result** to view details about NE addition.

**Figure 3-8** Discovery Result



**Step 7** Click **Complete**.

----End

## 3.4 Creating an NE Manually

If you want a few different types of NEs to access the eSight, you can create these NEs one by one.

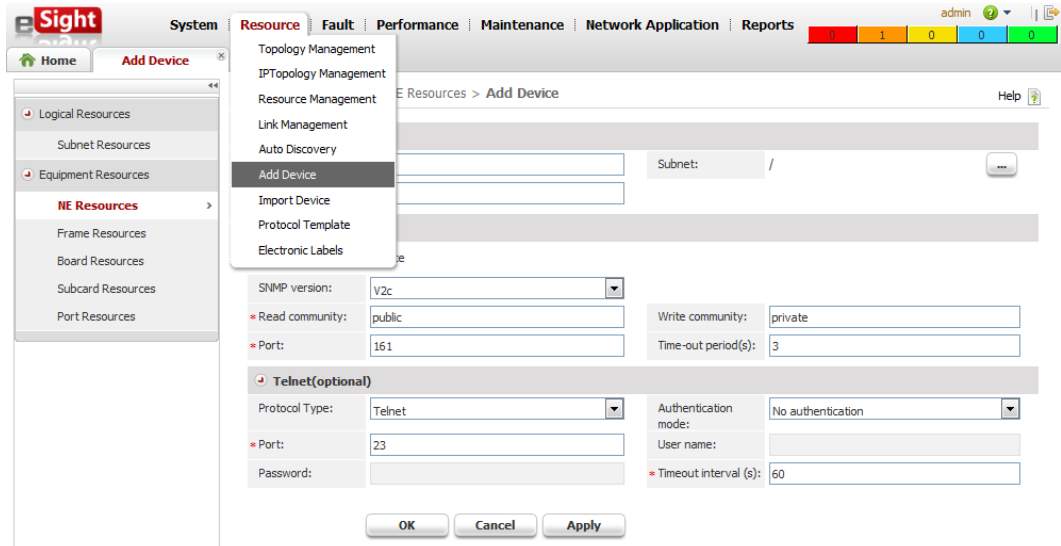
### Prerequisites

You have the operation rights for **Access Resource**.

## Procedure

**Step 1** Choose **Resource > Add Device** from the main menu.

**Figure 3-9** Adding Device



**Step 2** On the **Add Device** page, configure basic information about the NE to be created and SNMP parameters.



### NOTE

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. To add an SNMP template, see [3.9 Creating an SNMP Template](#).

**Figure 3-10** Setting SNMP parameters

**Step 3** Click **OK**.



### NOTE

Click **Apply** to create more NEs.

- If the NE is created successfully, the NE is displayed in the list.
- If the NE cannot be created, the **Error** dialog box is displayed, indicating the reason for the failure. Click **OK** to set the parameters again.

----End

## 3.5 Importing NEs Manually in Batches

When the system has a lot of managed objects during deployment or device expansion, you can add NEs in batches by using this function.

### Prerequisites

You have the operation rights for **Access Resource**.

### Context

Manually importing NEs is to add NEs by importing the .xls template.

Table 3-2 describes every fields in Excel template.

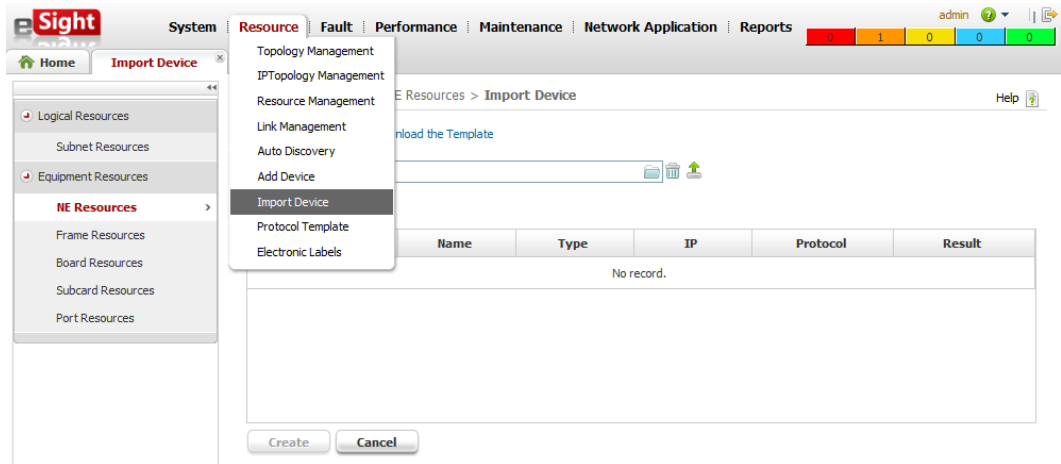
**Table 3-2** Excel template

| Field name       | Description                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------|
| IP Address       | For example, <b>10.123.124.115</b> .                                                                       |
| NE Name          | 1 to 128 characters. The NE name cannot contain the following characters # % & + / ; < = > ? \.            |
| Protocol Type    | Set to <b>SNMP</b> .                                                                                       |
| Protocol Version | The protocol version must be the same as the SNMP protocol version in the device, for example, <b>V1</b> . |
| Port             | This parameter must be the same as the port number of the SNMP protocol, for example, <b>161</b> .         |
| Read Community   | This parameter must be the same as the read community of the SNMP protocol, for example, <b>public</b> .   |
| Write Community  | This parameter must be the same as the write community of the SNMP protocol, for example, <b>private</b> . |

### Procedure

**Step 1** Choose **Resource > Import Device** from the main menu.

Figure 3-11 Importing Device



**Step 2** Click  and download the .xls template to the local computer.

**Step 3** Open the template, fill in NE information, and save the template.

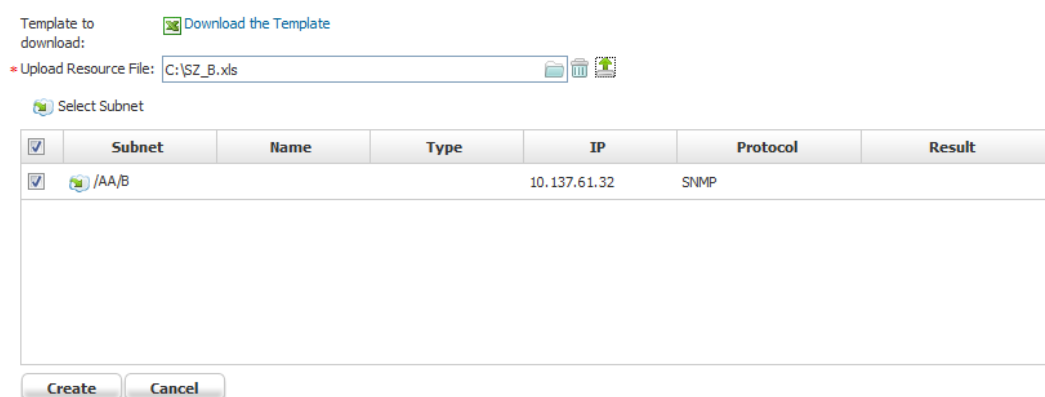
**Step 4** On the **Import Device** page, click  next to **Upload Resource File** and select the saved Excel file.

If you want to import other files, click  to clear the selected files.

**Step 5** Click  to upload a file.

NE information and NE check results are displayed on the right of the page. If is **Result** empty, NE check succeeds.

Figure 3-12 Uploading the file



**Step 6** Select an NE and click **Create**.

The system starts to import the NEs.

- If the NE is created successfully, the **Result** column is **The resource is created successfully**.

- If the NE cannot be created, the reason for the failure is displayed in the **Result** column. You can attempt to resolve the problem and import NEs again based on the failure reason. If the fault persists, contact the technical support personnel.

**Figure 3-13** Result

Template to download: [Download the Template](#)

\* Upload Resource File:   

 100%

Select Subnet

| <input checked="" type="checkbox"/> | Subnet                                                                                  | Name | Type  | IP           | Protocol | Result                                |
|-------------------------------------|-----------------------------------------------------------------------------------------|------|-------|--------------|----------|---------------------------------------|
| <input checked="" type="checkbox"/> |  /AA/B | S93  | S9306 | 10.137.61.32 | SNMP     | The resource is created successfully. |

----End

## 3.6 Adjusting the Relationships Between NEs and Subnets

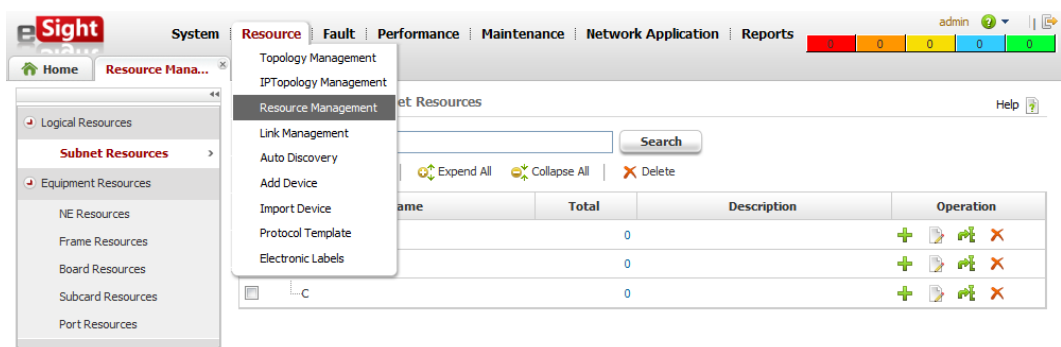
This topic describes how to adjust the relationships between NEs and subnets as required when the network structure changes.

### Prerequisites

You have the operation rights for **Access Resource**.

### Procedure

**Step 1** Choose **Resource > Resource Management** from the main menu.

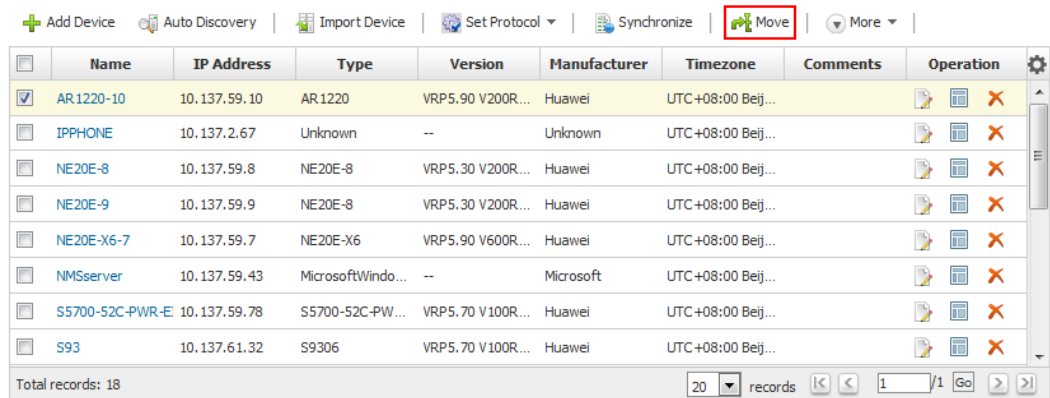
**Figure 3-14** Resource Management

**Step 2** Choose **Equipment Resources > NE Resources**.



**Step 3** Select an NE to be adjusted and click .

**Figure 3-15** Selecting an NE to be adjusted

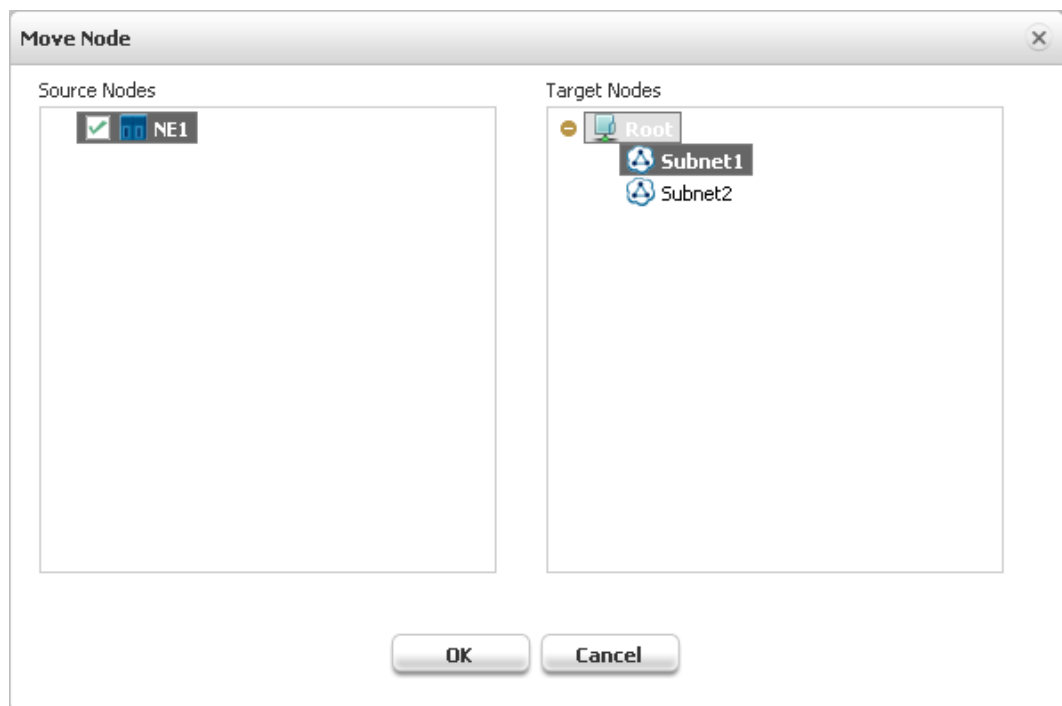


|                                     | Name            | IP Address   | Type              | Version          | Manufacturer | Timezone          | Comments | Operation                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------|--------------|-------------------|------------------|--------------|-------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | AR 1220-10      | 10.137.59.10 | AR 1220           | VRP5.90 V200R... | Huawei       | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | IPPHONE         | 10.137.2.67  | Unknown           | --               | Unknown      | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | NE20E-8         | 10.137.59.8  | NE20E-8           | VRP5.30 V200R... | Huawei       | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | NE20E-9         | 10.137.59.9  | NE20E-8           | VRP5.30 V200R... | Huawei       | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | NE20E-X6-7      | 10.137.59.7  | NE20E-X6          | VRP5.90 V600R... | Huawei       | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | NMSserver       | 10.137.59.43 | MicrosoftWindo... | --               | Microsoft    | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | S5700-52C-PWR-E | 10.137.59.78 | S5700-52C-PW...   | VRP5.70 V100R... | Huawei       | UTC+08:00 Beij... |          |    |
| <input type="checkbox"/>            | S93             | 10.137.61.32 | S9306             | VRP5.70 V100R... | Huawei       | UTC+08:00 Beij... |          |    |

Total records: 18      20 records      1 / 1      Go

**Step 4** In the dialog box that is displayed, select the target subnet to which the NE is moved. Click **OK**.

**Figure 3-16** Adjusting NEs



The operation result is displayed.

**Step 5** Click **OK**.

----End

## 3.7 Adjusting the Relationships Between Subnets

This topic describes how to adjust the relationships between subnets and subnets as required when the network structure changes.

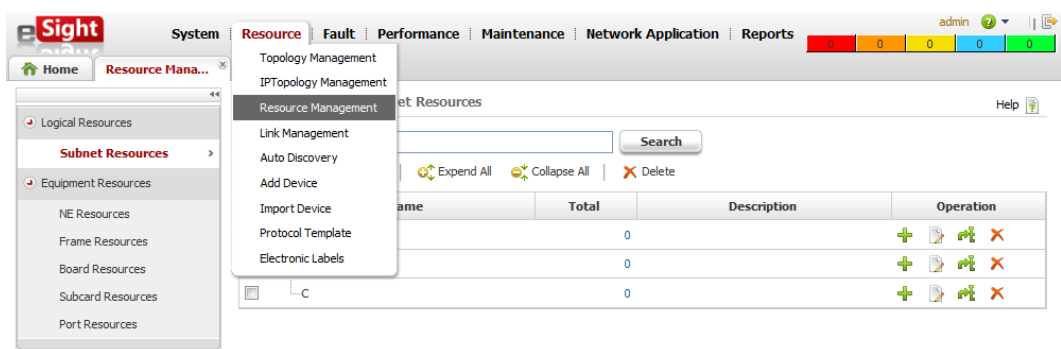
### Prerequisites

You have the operation rights for **Access Resource**.

### Procedure

**Step 1** Choose **Resource > Resource Management** from the main menu.

**Figure 3-17** Resource Management



**Step 2** Choose **Logical Resources > Subnet Resources**.

**Step 3** Select a subnet to be adjusted and click .

**Figure 3-18** Selecting a subnet to be adjusted

|  |  |  |  |                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>                                                            | Name                                                                                | Total                                                                               | Description                                                                         | Operation                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <input checked="" type="checkbox"/>                                                 | A                                                                                   | 0                                                                                   |                                                                                     |      |
| <input type="checkbox"/>                                                            | B                                                                                   | 0                                                                                   |                                                                                     |      |
| <input type="checkbox"/>                                                            | C                                                                                   | 0                                                                                   |                                                                                     |      |
| <input type="checkbox"/>                                                            | AA                                                                                  | 1                                                                                   |                                                                                     |      |
| <input type="checkbox"/>                                                            | B                                                                                   | 1                                                                                   |                                                                                     |      |

**Step 4** Select a target subnet and click **OK**.

----End

## 3.8 Physical Resource Management

The physical resource management function provides an entry for uniformly querying and collecting statistics on assets on the live network. This helps provide data to guide maintenance, reconstruction, and capacity expansion on the live network.

The physical resource management function manages the following objects: devices, subracks, boards, subcards, ports, and servers. [Table 3-3](#) describes operations that can be performed on each type of resources.

**Table 3-3** Supported operations

| Resource Type | GUI Entry                                                                                                                                                                              | Supported Operations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device        | <ol style="list-style-type: none"><li>1. Choose <b>Resource &gt; Resource Management</b> from the main menu.</li><li>2. Choose <b>Equipment Resources &gt; NE Resources</b>.</li></ol> | <p><b>Add Device:</b> If you want a few different types of NEs to access the eSight, create these NEs one by one.</p> <p><b>Import Device:</b> When the system has a lot of managed objects during deployment or device expansion, add NEs in batches by using this function.</p> <p><b>Auto Discovery:</b> When the NEs in a specified network segment will be added, the NE auto-discovery function helps you perform the operation in batches and save time.</p> <p><b>Set SNMP Parameters:</b> sets SNMP parameters of NEs on eSight in batches.</p> <p><b>Set Telnet Parameters:</b> sets Telnet parameters of NEs on eSight.</p> <p><b>Export:</b> exports device information to files.</p> <p><b>Synchronize:</b> synchronizes device data to eSight.</p> <p><b>Move:</b> When the network topology changes, adjust the subnet that the NE belongs to.</p> <p><b>Delete:</b> deletes one or more pieces of data.</p> <p><b>Set Timezone:</b> You can set Timezone of NEs on eSight.</p> <p><b>Modify Remarks:</b> You can click  to modify remarks and maintain</p> |

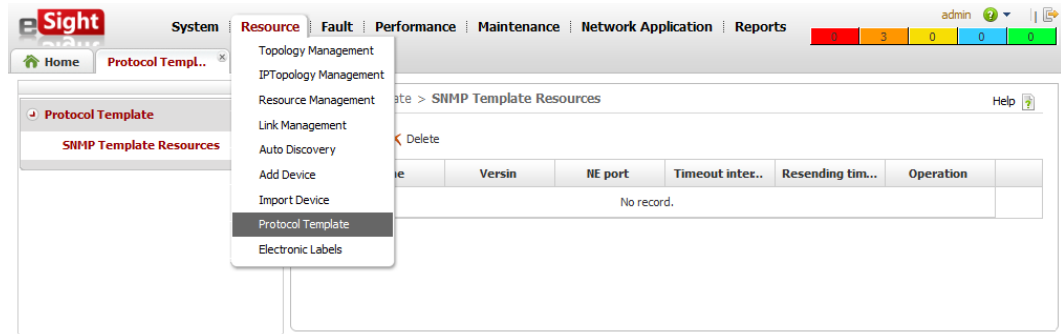
| Resource Type | GUI Entry                                                                                                                               | Supported Operations                                                                                                                                                                                                                                                                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                         | information of device.<br><b>Resources Details:</b> You can  to view device resource details.<br>Display the NE manager:<br>You can click <b>Name</b> of a device to display the NE manager corresponding to the device. |
| Subrack       | 1. Choose <b>Resource &gt; Resource Management</b> from the main menu.<br>2. Choose <b>Equipment Resources &gt; Frame Resources</b> .   | <b>Export:</b> You can export frame information to files.<br><b>Modify Remarks:</b> You can click  to modify frame remarks.                                                                                              |
| Board         | 1. Choose <b>Resource &gt; Resource Management</b> from the main menu.<br>2. Choose <b>Equipment Resources &gt; Board Resources</b> .   | <b>Export:</b> exports board information to files.<br><b>Modify Remarks:</b> You can click  to modify board remarks.                                                                                                     |
| Subcard       | 1. Choose <b>Resource &gt; Resource Management</b> from the main menu.<br>2. Choose <b>Equipment Resources &gt; Subcard Resources</b> . | <b>Export:</b> exports subcard information to files.<br><b>Modify Remarks:</b> You can click  to modify subcard remarks.                                                                                               |
| Port          | 1. Choose <b>Resource &gt; Resource Management</b> from the main menu.<br>2. Choose <b>Equipment Resources &gt; Port Resources</b> .    | <b>Export:</b> exports port information to files.<br><b>Modify Remarks:</b> You can click  to modify port remarks.                                                                                                     |

## 3.9 Creating an SNMP Template

You can select a created SNMP template without entering parameters on pages such as NE creation page.

### Procedure

**Step 1** from the main menu Choose **Resource > Protocol Template**.

**Figure 3-19 Protocol Template**

**Step 2** Click **Create**.

**Step 3** Set parameters on the **Add SNMP Template Resources** page.

**Figure 3-20 Adding SNMP Template Resources**

|                         |         |
|-------------------------|---------|
| * Template name:        | snmp1   |
| SNMP version:           | V2c     |
| * Read community:       | public  |
| Write community:        | private |
| * NE port:              | 161     |
| * Timeout interval (s): | 3       |
| * Resending times:      | 3       |

**Step 4** Click **OK**.

----End

## Follow-up Procedure

You can perform the following operations on the **Add SNMP Template Resources** page.

| Maintaining the SNMP Template | Procedure                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Viewing an SNMP template      | Click  .                                            |
| Deleting an SNMP template     | Click an SNMP template and click <b>Delete</b> .                                                                                       |
| Copying an SNMP template      | Click the SNMP template to be copied and click  . |

## 3.10 Link Management

Link management enables you to query link status, and maintain network links. In addition, links are displayed on topology view. You can learn structure change of the network topology on the live network according to the link topology.

### Prerequisites

The Telnet parameters on eSight and the NE are set.

### Context

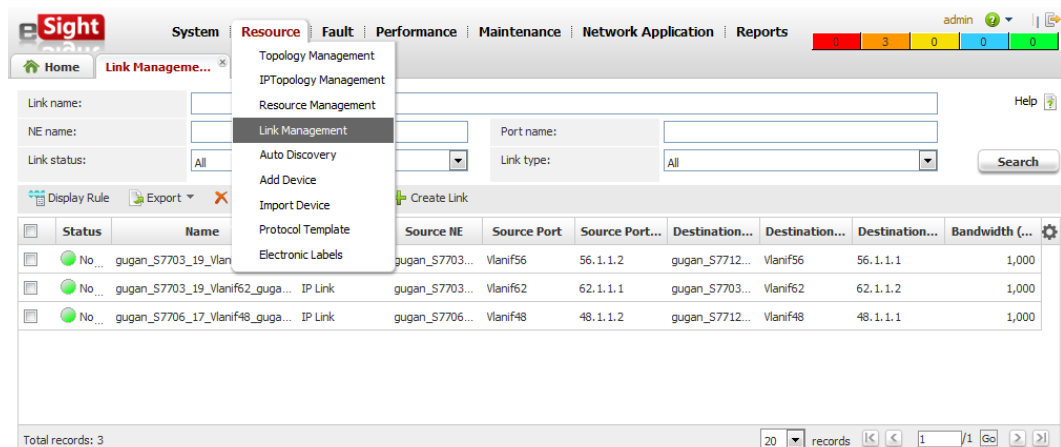
When an NE is created on eSight, eSight automatically discovers the link between the NE and other NEs and adds the NE to the link topology.

Links on the live network are changing all the time. You must perform the **Discover Link** operation before performing link management on eSight to enable eSight to discover new links on the live network, ensuring data consistency of eSight and the live network.

### Procedure

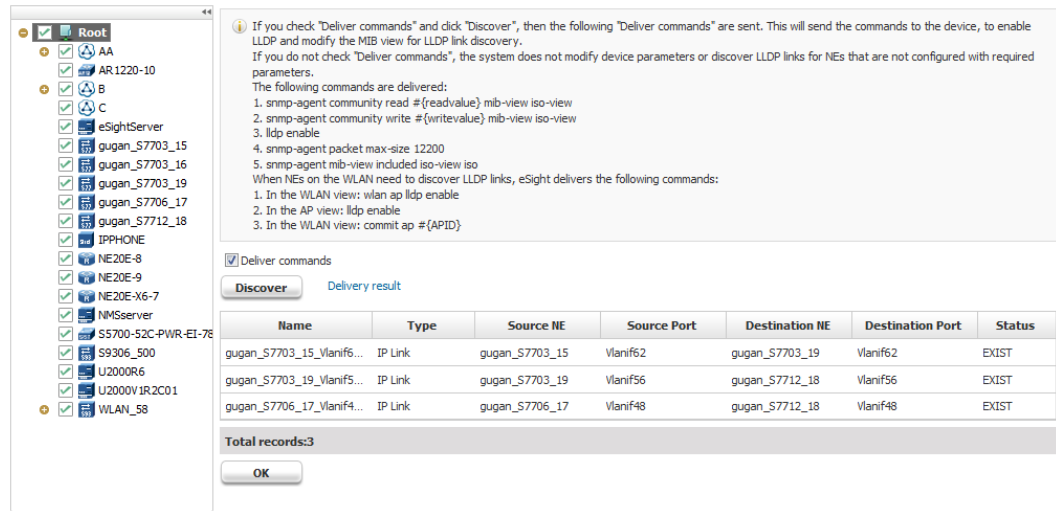
**Step 1** Choose **Resource > Link Management** from the main menu.

Figure 3-21 Link Management



**Step 2 Optional:** Set filter parameters at the top of the pane and click **Search**.

**Step 3** Click **Discover Link**. On the left side of the window, select the NEs at the ends of a link to be discovered, select **Deliver commands**, and click **Discover**. The link discovered by eSight is displayed on the right of the window. Click **OK**.

**Figure 3-22** Discovering Links automatically**Table 3-4** Commands for discovering the LLDP link

| Commands                                                   | Description                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmp-agent community read #{readvalue} mib-view iso-view   | Add the read right of the #{readvalue} community in the MIB and ISO views.                                                                                                                                                                                                                                                                  |
| snmp-agent community write #{writevalue} mib-view iso-view | Add the write right of the #{writevalue} community in the MIB and ISO views.                                                                                                                                                                                                                                                                |
| lldp enable                                                | Enabling the LLDP function of an interface means enabling LLDP packet exchange with the neighboring node. The local interface can not only receive state information on the neighboring node but also delivers local state information to the neighboring node. In this way, the data required by eSight for topology discover is obtained. |
| snmp-agent packet max-size 12200                           | The biggest SNMP packet that the Agent can receive or send are 12200 bytes.                                                                                                                                                                                                                                                                 |
| snmp-agent mib-view included iso-view iso                  | Add an ISO object into a view.                                                                                                                                                                                                                                                                                                              |

**NOTE**

The preceding commands are used only for LLDP link discovery and NEs' other functions are not affected.

For the LLDP link:

- If the commands listed in Table 3-4 are not set on an NE, set Telnet parameters on eSight and the NE, and then select **Deliver commands**. After the LLDP link is discovered, you can click **Delivery result** to view the command delivery and execution result.
- If the commands listed in Table 3-4 are set on the NE, do not select **Deliver commands** so that the LLDP link will be automatically discovered on eSight.

For the Side by Side link, do not select **Deliver commands** so that the Side by Side link will be automatically discovered on eSight.

**Step 4 Optional:** Create a link.

1. Click **Create Link** to create a link.
2. Set **Link name**, **Link type**, **Source NE**, **Source Port**, **Destination NE**, and **Destination Port**, and click **OK**.



**NOTE**

You can also create a link in the Topology Management.

**Step 5** Export the link information in eSight to the client and save the information as a file in Word, Excel, PDF, or PowerPoint format.

- Choose **Export > Export Selected**. In the window that is displayed, click **Save**.
- Choose **Export > Export All**. In the window that is displayed, click **Save**.

----End

## Follow-up Procedure

You can perform operations listed in the following table after adding links.

| Maintaining Links             | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change the link display rules | <p>Change the link display rules.</p> <ol style="list-style-type: none"><li>1. In the <b>Link Management</b> window, click <b>Display Rule</b> to set the display rule for a link.<ul style="list-style-type: none"><li>– In <b>Naming Rule</b>, set the display fields of a link name.</li><li>– In <b>Tip Rule</b>, set the display fields of link tips.</li></ul></li></ol> <p><b>NOTE</b><br/>Tips rules are displayed in the topology management window. After moving the cursor to a link, you can see the tips of the link after a while.</p> |
| Delete a link                 | <p>Delete a link.</p> <ol style="list-style-type: none"><li>1. In the <b>Link Management</b> window, select a link to be deleted and click <b>Delete</b>.</li><li>2. In the displayed dialog box, click <b>Yes</b>.</li></ol> <p><b>NOTE</b></p>                                                                                                                                                                                                                                                                                                     |



| Maintaining Links | Operation Method                                                                                                                |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                   | The deleted link is a link of eSight. To re-upload the link data to eSight, you can perform the <b>Discover Link</b> operation. |

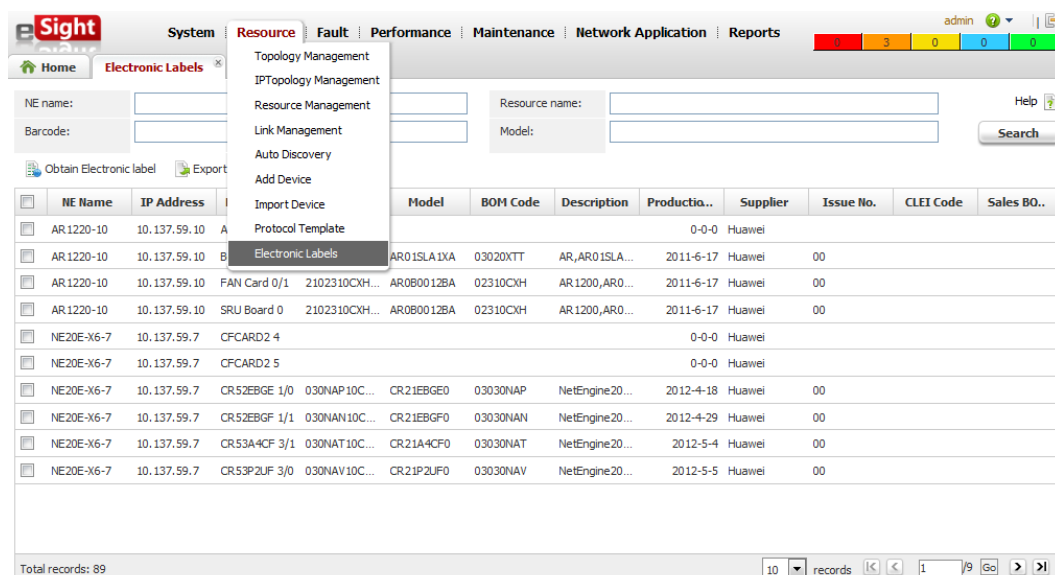
## 3.11 Electronic Labels Management

Electronic labels are used in network design, planning, and maintenance, asset management (including spare part management), order, account management, liquidation, invest tracing, and warranty. eSight supports query and export of an electronic label.

### Procedure

**Step 1** Choose **Resource > Electronic Label** from the main menu.

Figure 3-23 Electronic Label



**Step 2** Click **Obtain Electronic label** and select one or more NEs. Then click **Obtain** to view the electronic labels of the physical resources.



#### NOTE

Obtaining network-wide electronic labels takes a long time. Perform this operation during off-peak hours.

**Figure 3-24** Obtaining Electronic label

| <input type="checkbox"/> | NE Name             | IP Address   | NE Type          |
|--------------------------|---------------------|--------------|------------------|
| <input type="checkbox"/> | NE20E-9             | 10.137.59.9  | NE20E-8          |
| <input type="checkbox"/> | NE20E-X6-7          | 10.137.59.7  | NE20E-X6         |
| <input type="checkbox"/> | AR1220-10           | 10.137.59.10 | AR1220           |
| <input type="checkbox"/> | WLAN_58             | 10.137.59.58 | SPU              |
| <input type="checkbox"/> | S5700-52C-PWR-EI-78 | 10.137.59.78 | S5700-52C-PWR-EI |
| <input type="checkbox"/> | S93                 | 10.137.61.32 | S9306            |
| <input type="checkbox"/> | S9306_500           | 10.137.59.5  | S9306            |
| <input type="checkbox"/> | gugan_S7703_19      | 10.137.59.19 | S7703            |
| <input type="checkbox"/> | gugan_S7703_16      | 10.137.59.16 | S7703            |
| <input type="checkbox"/> | NE20E-8             | 10.137.59.8  | NE20E-8          |

Total records: 13    10 records    1/2    Go    > >|

Select All   Obtain   Cancel

**Step 3** Export the electronic labels.

- Choose **Export > Export Selected**. In the window that is displayed, click **Save**.
- Choose **Export > Export All**. In the window that is displayed, click **Save**.

----End

## 3.12 Example: Typical Resource Management Operations

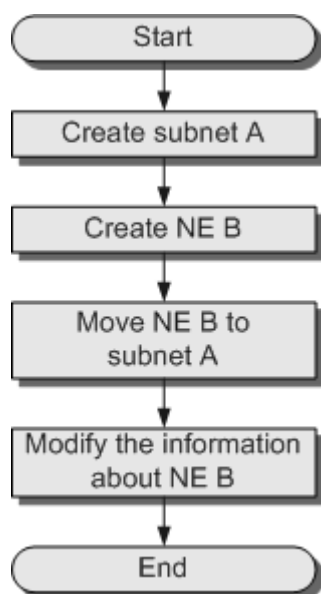
This topic describes an example about how to perform resource management operations. From the example, you will learn about the procedure and basic operations about resource management.

### Context

To meet the increase in service usage, company X purchases new devices. The administrator needs to add the devices to the physical view of the eSight and manage the devices in the eSight.

Figure 3-25 shows the procedure.

Figure 3-25 Procedure



## Procedure

### Step 1 Create a subnet A.

1. Choose **Resource > Resource Management** from the main menu.
2. In the navigation tree of the **Resource Management** window, select **Root**. On the managed object page on the right, click **Create**.
3. On the **Select Object Type** page, choose **Subnets and Solutions > Subnet**.
4. On the **Configure Parameters** page, set the name and description of subnet A.
5. Then click **OK**.

### Step 2 Create NE B.

1. In the navigation tree of the **Resource Management** window, select **Root**. On the managed object page on the right, click **Create**.
2. On the **Select Object Type** page, choose **Physical Devices > Snmp Network Element**.
3. On the **Configure Parameters** page, set the basic information and SNMP protocol parameters for NE B.
4. Then click **OK**.

### Step 3 Move NE B to subnet A.

1. In the **Resource Management** window, click .
2. In the **Source Nodes** area in the **Move Node** dialog box, select NE B. In the **Target Nodes** area, select subnet A.
3. Then click **OK**.

### Step 4 Modify the information about NE B.

1. In the **Resource Management** window, select subnet A.

2. On the managed object page on the right, click  in the **Operation** column of NE B.
3. Modify the name of NE B.
4. Then click **OK**.

----End

---

# 4 Topology Management

---

## About This Chapter

Topology management involves creating and managing the topology of the entire network. The physical view shows the networking and running status of devices. The NEs are displayed in certain colors in the physical view, and their status is also displayed. This information helps you monitor the entire network in real time.

### 4.1 Overview of Topology Management Operations

This topic describes the topology management operations.

### 4.2 Physical Topology Management

### 4.3 IP Topology Management

IP topology views are generated based on the analysis and computing of networks managed by eSight. IP topology views display the division of routing devices and subnets, and links between Layer 2 devices.

## 4.1 Overview of Topology Management Operations

This topic describes the topology management operations.

### Background

Before performing topology management operations, you need to be familiar with the basic concepts about topology management. For details, see [1.2.3 Basic Concepts of Topology Management](#). Understanding these concepts helps you avoid errors when performing topology management operations.

### Overview of topology management operations

[Figure 4-1](#) shows the overview of topology management operations. For more details, click the operation in the overview.

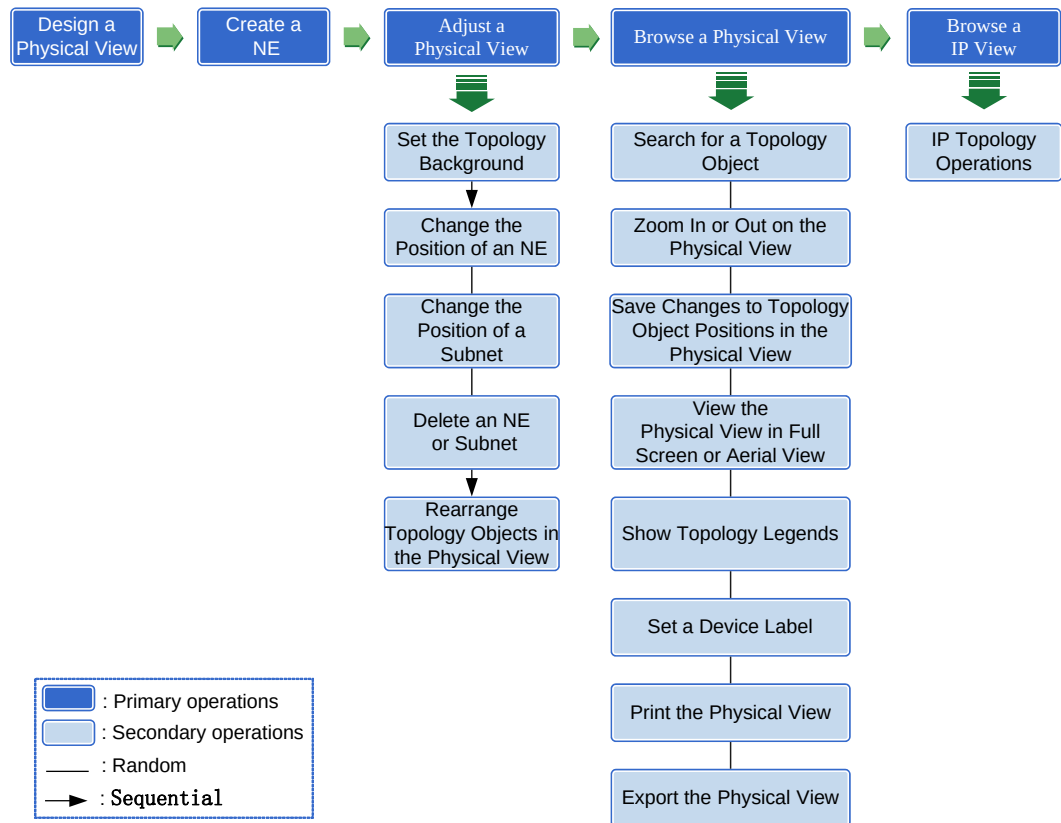
**Figure 4-1** Overview of topology management operations

Table 4-1 describes the topology management operations.

**Table 4-1** Topology management operations

| Operation                                                 | Description                                                                                                                                                                                                          |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">4.2.1 Designing a Physical View</a>           | Before deploying NEs in a physical view, you need to design the physical view. The physical view should clearly reflect the actual communication network structure to facilitate routine maintenance and operations. |
| <a href="#">4.2.2.2 Changing the Position of an NE</a>    | When the positions of NEs change, you need to adjust the corresponding positions in the physical view to update the relationships between NEs and other topology objects.                                            |
| <a href="#">4.2.2.3 Changing the Position of a subnet</a> | When the positions of subnets change, you need to adjust the corresponding positions in the physical view to update the relationships between the subnets and other topology objects.                                |
| <a href="#">4.2.2.4 Deleting an NE or Subnet</a>          | You can delete an NE or subnet that does not need to be managed by the eSight.                                                                                                                                       |
| <a href="#">4.2.2.1 Setting the Topology Background</a>   | This topic describes how to set the topology background based on the layout of topology objects.                                                                                                                     |
| <a href="#">4.2.2.5 Rearranging Topology Objects in a</a> | This topic describes how to rearrange topology objects in a physical view if required.                                                                                                                               |

| Operation                                                                                | Description                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Physical View</a>                                                            |                                                                                                                                                                                             |
| <a href="#">4.2.3.1 Searching for a Topology Object</a>                                  | You can use the search function to quickly locate an object, such as an NE, a link or a subnet.                                                                                             |
| <a href="#">4.2.3.2 Zooming In or Out on a Physical View</a>                             | This topic describes how to zoom in or zoom out on a physical view, restore a physical view to its initial state, and make a physical view display in a proper size or in full screen mode. |
| <a href="#">4.2.3.3 Saving Changes to Topology Object Positions in the Physical View</a> | If the position of a topology object in the physical view is changed, you can save the position as required.                                                                                |
| <a href="#">4.2.3.4 Viewing the Physical View in Full Screen or Aerial View</a>          | This topic describes how to view a physical view in full screen or in aerial view.                                                                                                          |
| <a href="#">4.2.3.5 Showing Topology Legends</a>                                         | This topic describes how to show topology legends in the physical view. Topology legends define the meanings of topology object colors or status.                                           |
| <a href="#">4.2.3.6 Setting a Device Label</a>                                           | This topic describes how to set a device label. The device label information includes the name and IP address of a device.                                                                  |
| <a href="#">4.2.3.7 Printing the Physical View</a>                                       | You can print the physical view.                                                                                                                                                            |
| <a href="#">4.2.3.8 Exporting the Physical View</a>                                      | You can export the physical view to a local PC.                                                                                                                                             |
| <a href="#">4.3.2 IP Topology Operations</a>                                             | Describes how to perform operations on the IP topology to monitor devices and links.                                                                                                        |

## 4.2 Physical Topology Management

### 4.2.1 Designing a Physical View

Before deploying NEs in a physical view, you need to design the physical view. The physical view should clearly reflect the actual communication network structure to facilitate routine maintenance and operations.

The eSight provides the following suggestions for designing the physical view to meet various management requirements:

- By the area where NEs are located
- By NE type
- By NE IP address
- By NE owner

## 4.2.2 Adjusting a Physical View

After designing a physical view, you can adjust it as required. Adjusting a physical view involves adjusting topology objects and setting the topology background.

### 4.2.2.1 Setting the Topology Background

This topic describes how to set the topology background based on the layout of topology objects.

#### Prerequisites

You have the operation rights for **Modify Topology**.

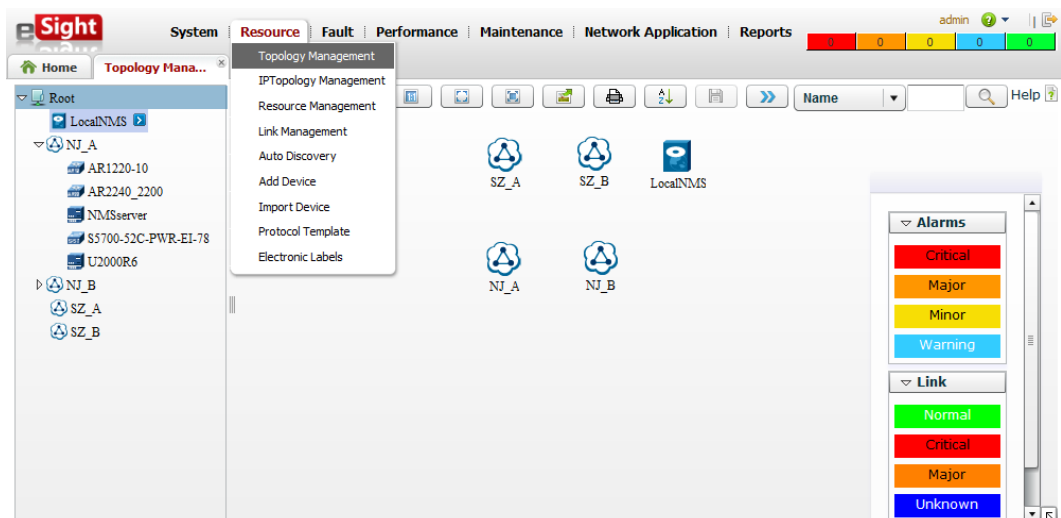
#### Context

The eSight supports the following formats of background image files: .jpg, .jpeg, .gif, and .png.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

Figure 4-2 Topology Management



**Step 2** On the toolbar of the **Topology Management** window, click .

**Step 3** Import an image file.

1. In the **Set Background** dialog box, select **Show background image**.

2. Click . The required image file is imported.

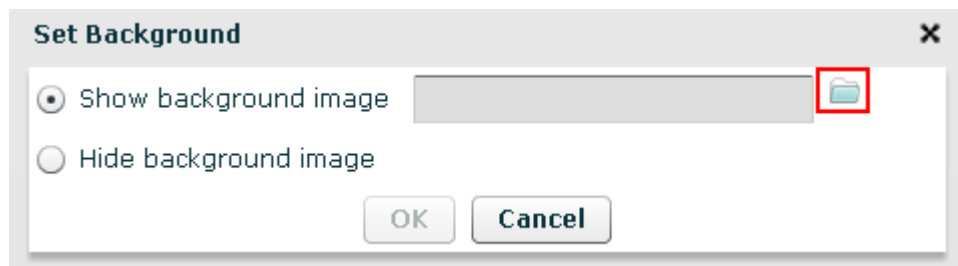


#### NOTE

If you do not want the background image to be displayed in the physical view, select **Hide background image**.



**Figure 4-3** Importing an image



**Step 4** Click **OK**.

The image is displayed as the topology background.

----**End**

### 4.2.2.2 Changing the Position of an NE

When the positions of NEs change, you need to adjust the corresponding positions in the physical view to update the relationships between NEs and other topology objects.

#### Prerequisites

You have the operation rights for **Modify Topology**.

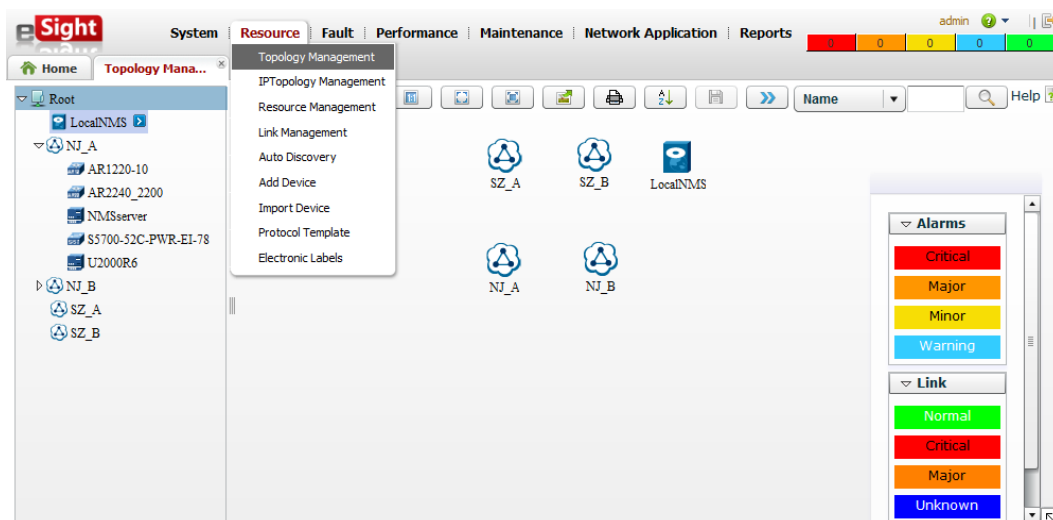
#### Context

You can adjust the positions of NEs in the physical view on your local computer but cannot save the changes if you do not have permission **Modify Topology**.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

Figure 4-4 Topology Management



**Step 2** In the **Topology management** window, adjust the position of an NE. You can adjust the position of an NE by using either of the following two methods:

- Adjust the position of an NE
  - Move a single NE: In the physical view, click the NE, and drag it to a specified position.
  - Move multiple NEs: In the physical view, select multiple NEs while holding down **Ctrl**, and drag them to a specified position.
- Adjust the relationship between an NE and a subnet
  1. In the navigation tree or physical view, select an NE.  
You can press **Ctrl** to select more NEs from the physical view.
  2. On the topology toolbar, click .
  3. In the topology navigation tree or physical view, select the target subnet. In the physical view, double-click the target subnet to open it, and click .

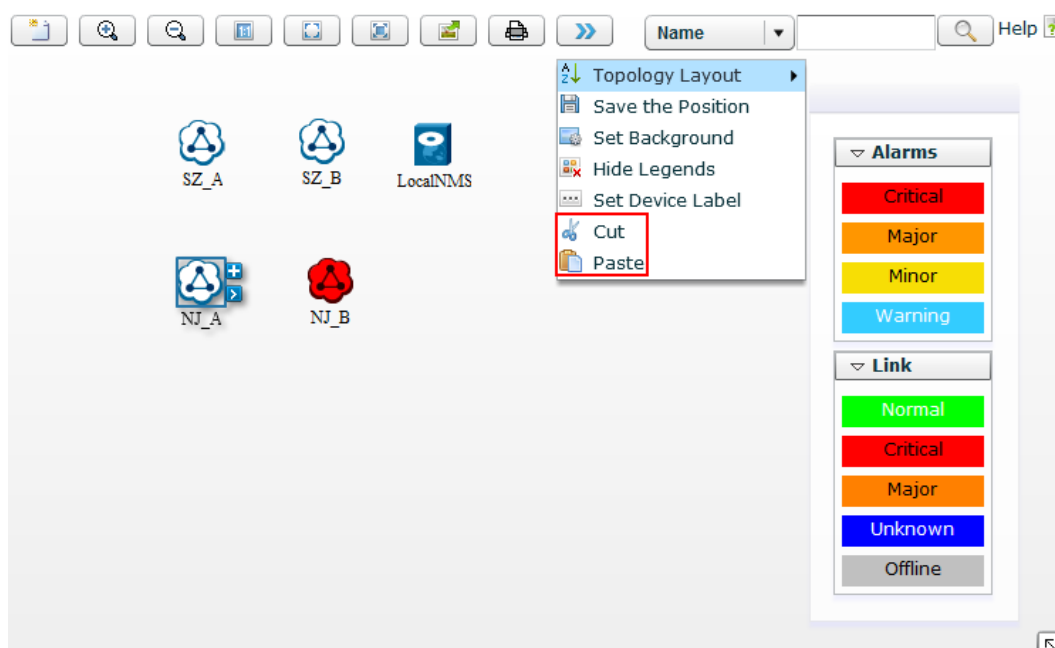
 **NOTE**

- If the object subnet has subnodes, you can select any subnodes at the level under the object subnet in the topology navigator and click .
- If the NE to be adjusted is already located under the target subnet,  is unavailable.

When you click :

- If the paste operation is successful, the selected NE is displayed under the target subnet.
- If the paste operation fails, the  icon is unavailable.

**Figure 4-5** Adjust the relationship between an NE and a subnet



**Step 3** On the toolbar, click  to save the setting.

----End

### 4.2.2.3 Changing the Position of a subnet

When the positions of subnets change, you need to adjust the corresponding positions in the physical view to update the relationships between the subnets and other topology objects.

#### Prerequisites

You have the operation rights for **Modify Topology**.

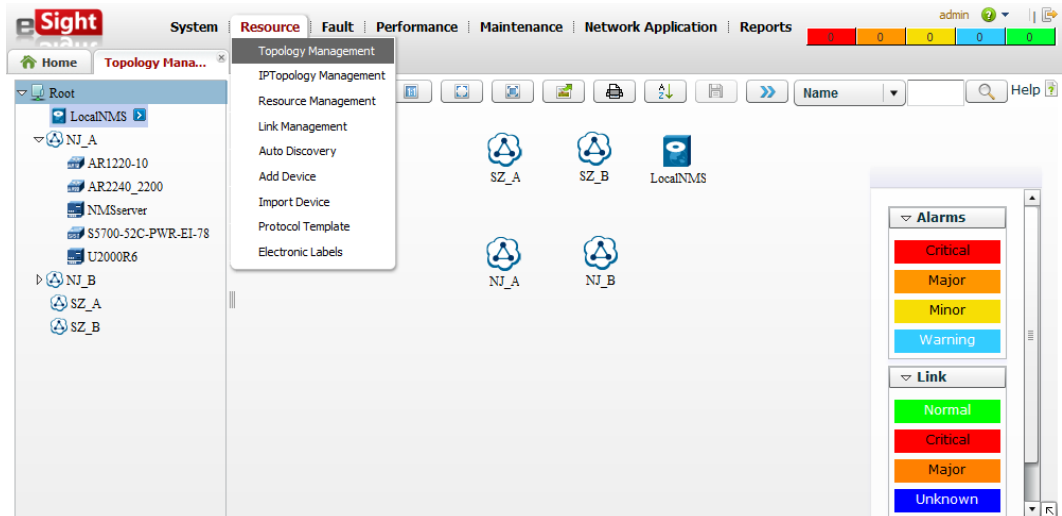
#### Context

You can adjust the positions of subnets in the physical view on your local computer and cannot save the changes if you do not have permission **Modify Topology**.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

**Figure 4-6** Topology Management



**Step 2** In the **Topology Management** window, adjust the position of a subnet. You can adjust the position of a subnet by using either of the following two methods:

- Adjust the position of a subnet
  - To move a subnet, click the subnet and drag it to a specified position.
  - To move subnets, press **Ctrl** while selecting the subnets and drag them to a specified position.
- Adjust the relationship between subnets
  1. In the navigation tree or physical view, select a subnet.  
You can press **Ctrl** to select more subnets from the physical view.
  2. On the topology toolbar, click .
  3. In the topology navigation tree, select the target subnet. In the physical view, double-click the target subnet to open it, and click .

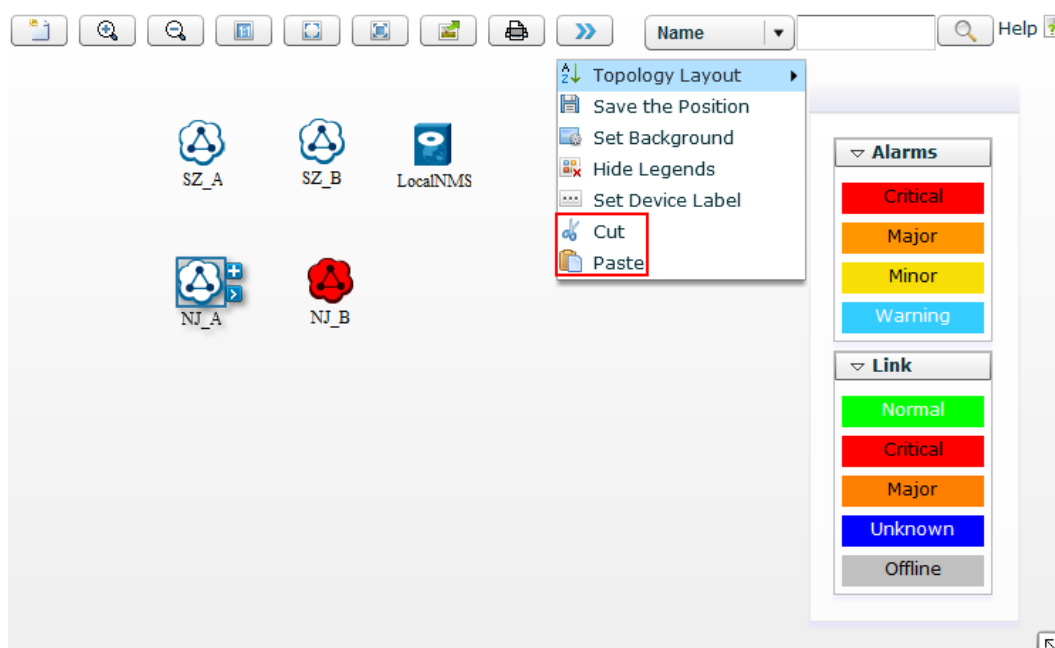
 **NOTE**

- If the object subnet has subnodes, you can select any subnodes at the level under the object subnet in the topology navigator and click .
- If the subnet to be adjusted is already located under the target subnet,  is unavailable.

When you click :

- If the paste operation is successful, the selected subnet is displayed under the target subnet.
- If the paste operation fails, the  icon is unavailable.

**Figure 4-7** Adjust the relationship between subnets



**Step 3** On the toolbar, click  to save the setting.

----End

#### 4.2.2.4 Deleting an NE or Subnet

You can delete an NE or subnet that does not need to be managed by the eSight.

##### Prerequisites

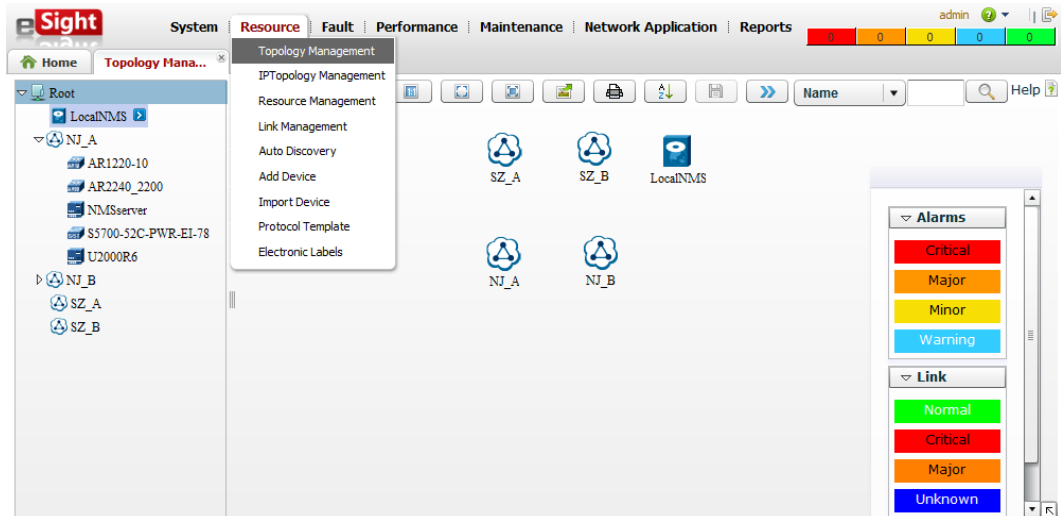
You have permission **Modify Topology** and **Access Resource**.

##### Context

You cannot delete a subnet or NE that hosts NEs.

##### Procedure

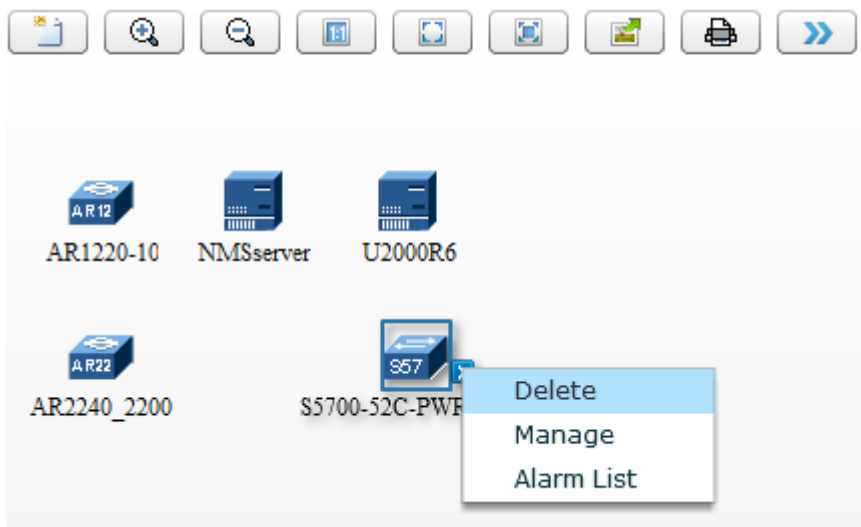
**Step 1** Choose **Resource > Topology Management** from the main menu

**Figure 4-8** Topology Management

**Step 2** In the **Topology Management** window, select a subnet or NE.

You can also select a subnet or NE from the physical view.

**Step 3** Click  in the lower right corner of the subnet or NE, and select **Delete**.

**Figure 4-9** Delete an NE or Subnet

----End

#### 4.2.2.5 Rearranging Topology Objects in a Physical View

This topic describes how to rearrange topology objects in a physical view if required.

## Prerequisites

You have the operation rights for **Modify Topology**.

## Context

- You can arrange topology objects only on your local computer but cannot save the changes if you have no permission **Modify Topology**.
- If you select some topology objects, only the selected topology objects are arranged.
- If you do not select any topology objects, all topology objects are arranged.
- The eSight provides the following layouts:
  - Round: layout in the form of a loop
  - Symmetry: symmetric layout
  - From Top to Bottom: tree layout from top to bottom
  - From Bottom to Top: tree layout from bottom to top
  - From Left to Right: tree layout from left to right
  - From Right to Left: tree layout from right to left



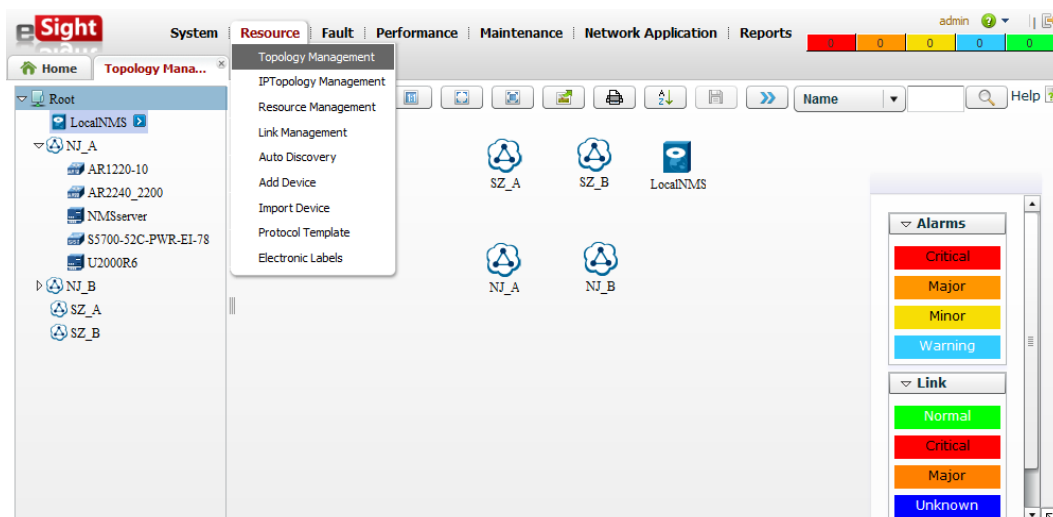
### CAUTION

The default arrangement modes allow you to sort NE icons, but they sometimes damage the existing arrangement mode. Therefore, use the default arrangement modes with caution.

## Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

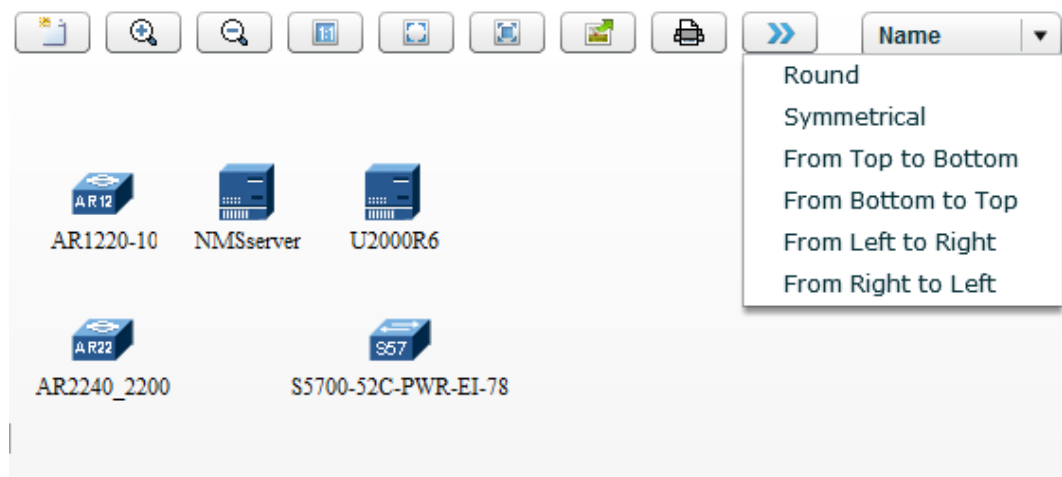
**Figure 4-10** Topology Management



**Step 2** In the **Topology Management** window, select topology objects, and click  to select a layout mode.

The topology objects in the physical view are arranged in the selected layout.

**Figure 4-11** Selecting a layout mode



**Step 3** Click  to save the new positions.

----End

## 4.2.3 Browsing a Physical View

This topic describes the methods of browsing a physical view.

### 4.2.3.1 Searching for a Topology Object

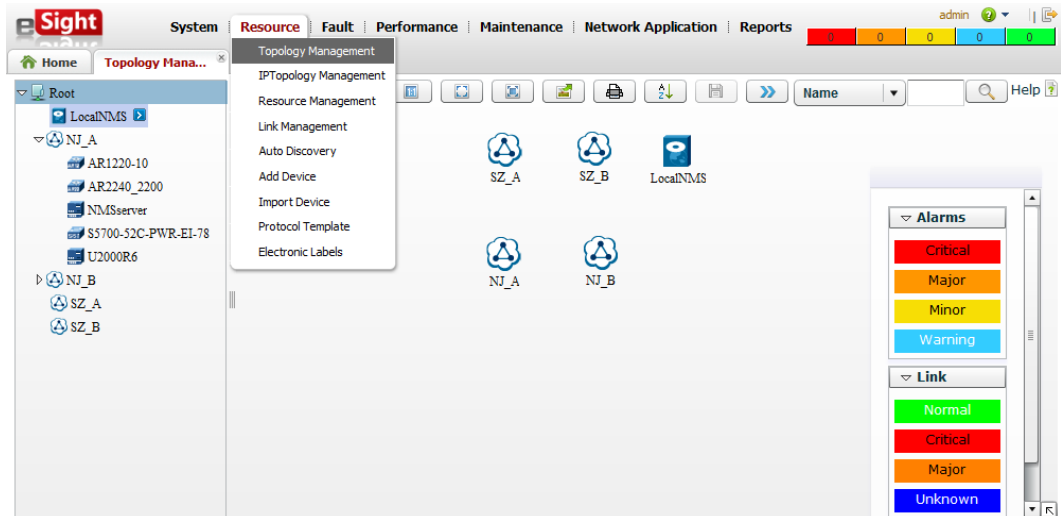
You can use the search function to quickly locate an object, such as an NE, a link or a subnet.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.



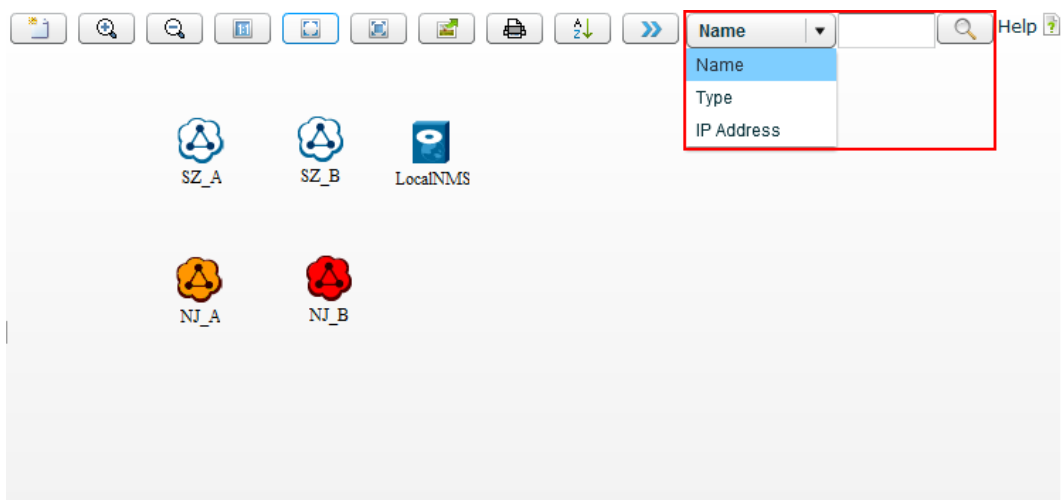
Figure 4-12 Topology Management



**Step 2** Set search criteria in the text box next to  on the toolbar.

1. Select a field from the drop-down list.
2. Enter the value of the selected field.

Figure 4-13 Setting the search criteria



**Step 3** Click .

The eSight searches for topology objects based on the specified search criteria and displays the found topology objects in the **Search Result** dialog box.

**Step 4** In the **Search Result** dialog box, click the name of the required topology object. The topology object is quickly located in the physical view and navigation tree.

----End

### 4.2.3.2 Zooming In or Out on a Physical View

This topic describes how to zoom in or zoom out on a physical view, restore a physical view to its initial state, and make a physical view display in a proper size or in full screen mode.

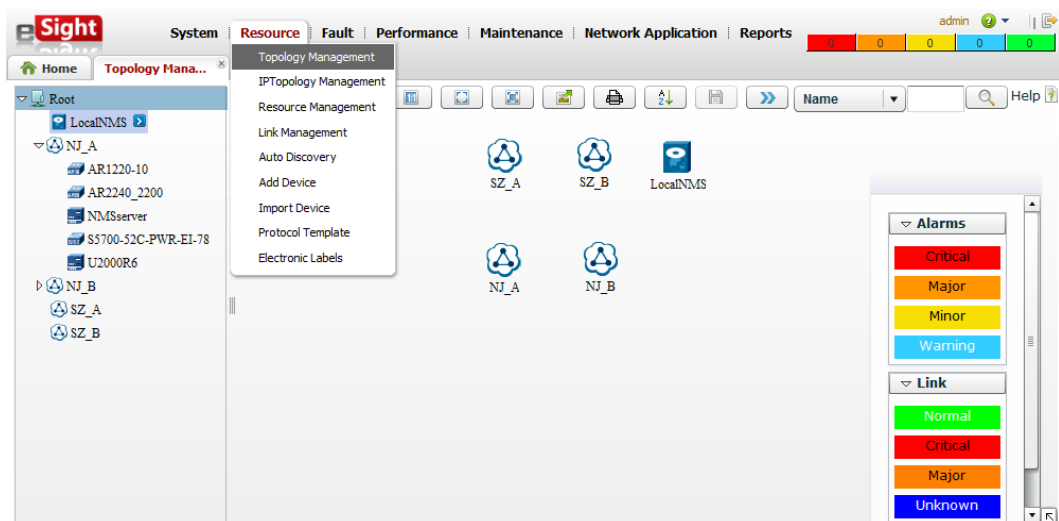
#### Prerequisites

You have the operation rights for **Modify Topology**.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

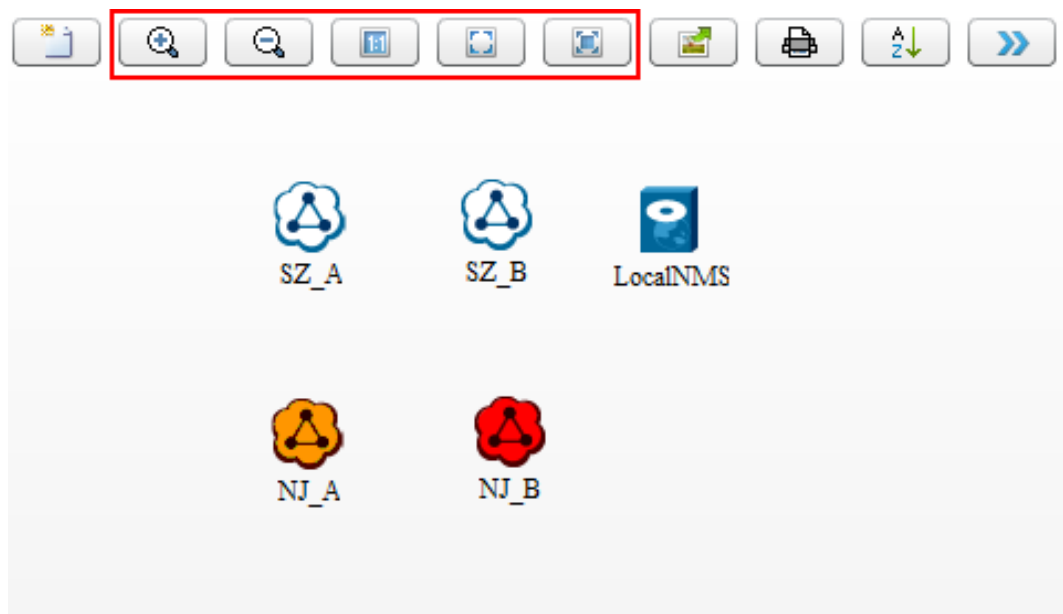
**Figure 4-14** Topology Management



**Step 2** In the **Topology Management** window, adjust the size of the physical view in the following ways:

- Click  to zoom in on the physical view.
- Click  to zoom out on the physical view.
- Click  to reset the physical view.
- Click  to display the physical view in a proper size.
- Click  to display the physical view in full screen mode.
- Adjust the size of the physical view by using the aerial view. For details, see [4.2.3.4 Viewing the Physical View in Full Screen or Aerial View](#).
  - In the aerial view, rotate the mouse wheel forward to zoom in on the physical view.
  - In the aerial view, rotate the mouse wheel backward to zoom out on the physical view.

**Figure 4-15** Zooming the physical view in and out



----End

### 4.2.3.3 Saving Changes to Topology Object Positions in the Physical View

If the position of a topology object in the physical view is changed, you can save the position as required.

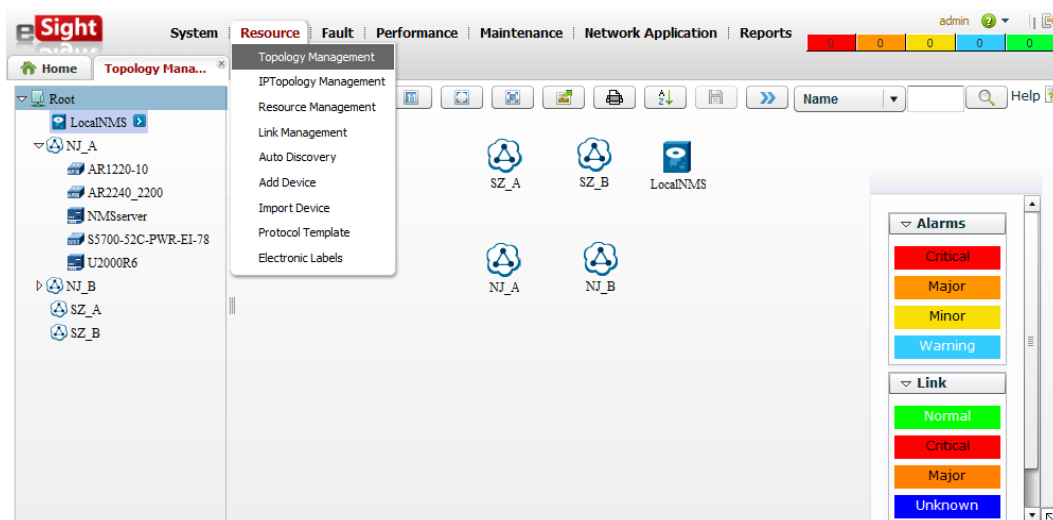
#### Prerequisites

You have the operation rights for **Modify Topology**.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

Figure 4-16 Topology Management



**Step 2** In the **Topology Management** window, adjust the position of a topology object.

**Step 3** Click  to save the physical view.

----End

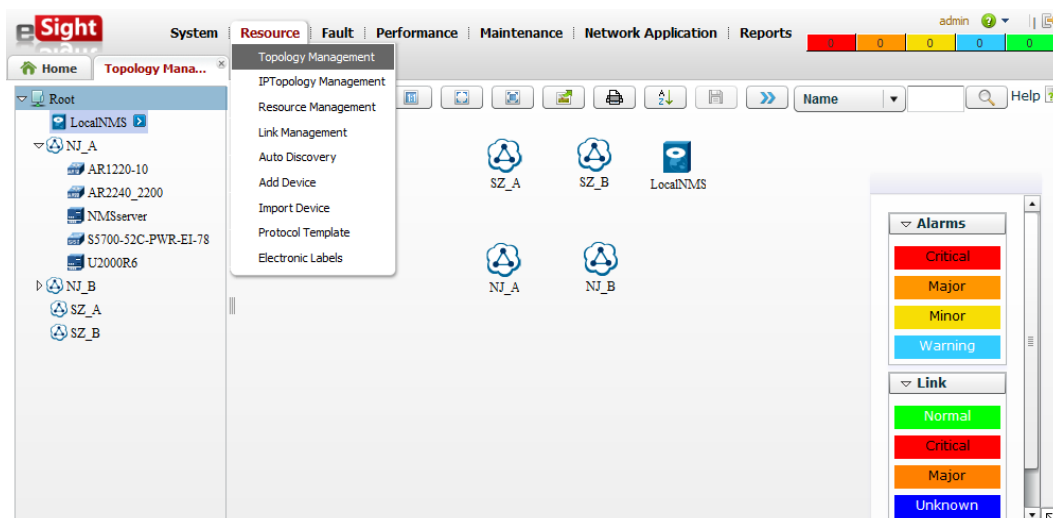
#### 4.2.3.4 Viewing the Physical View in Full Screen or Aerial View

This topic describes how to view a physical view in full screen or in aerial view.

#### Procedure

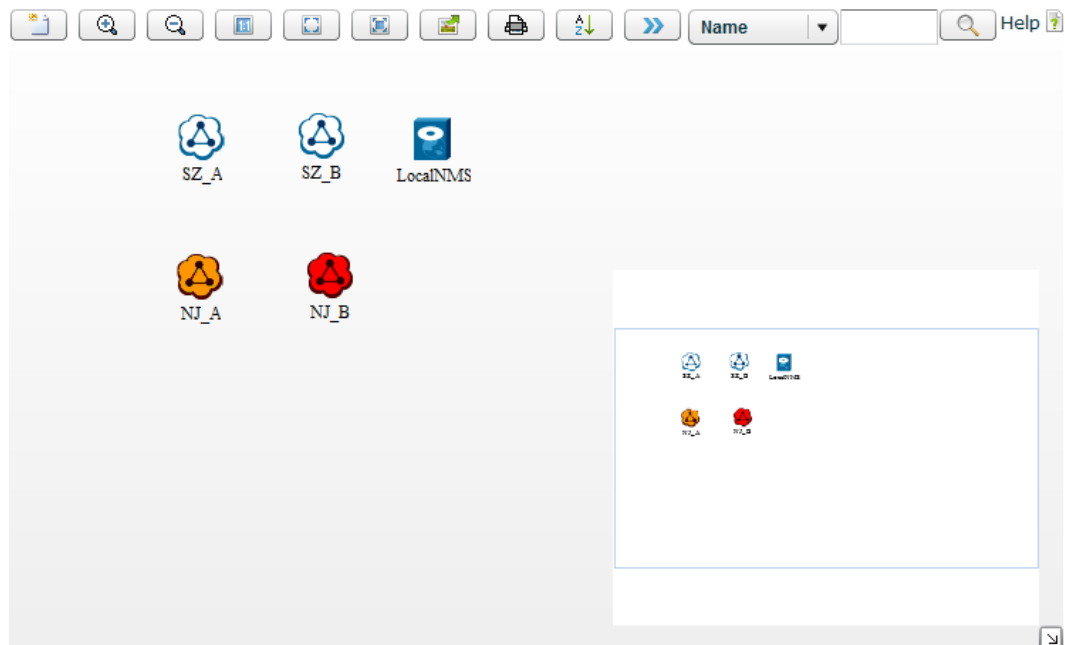
**Step 1** Choose **Resource > Topology Management** from the main menu.

Figure 4-17 Topology Management



**Step 2** In the **Topology Management** window, click  at the right lower corner of the physical view.

**Figure 4-18** Aerial view of the physical view



**Step 3 Optional:** In the aerial view, drag the rectangle to change the display area.

**Step 4 Optional:** Adjust the size of the physical view by using the aerial view.

- In the aerial view, rotate the mouse wheel forward to zoom in on the physical view.
- In the aerial view, rotate the mouse wheel backward to zoom out on the physical view.

**Step 5** Click  to close the aerial view.

**Step 6** Click  to display the physical view in full screen.

 **NOTE**

- You can press **Esc** to exit the full screen mode.
- If you click , the size of the topology object icons may change, but the topology object positions and shapes do not change.
- You cannot perform the following operations on a full screen physical view:
  - Creating virtual NEs
  - Creating virtual links
  - Searching topology objects
  - Setting the topology background

----End

### 4.2.3.5 Showing Topology Legends

This topic describes how to show topology legends in the physical view. Topology legends define the meanings of topology object colors or status.

#### Prerequisites

You have the operation rights for **Modify Topology**.

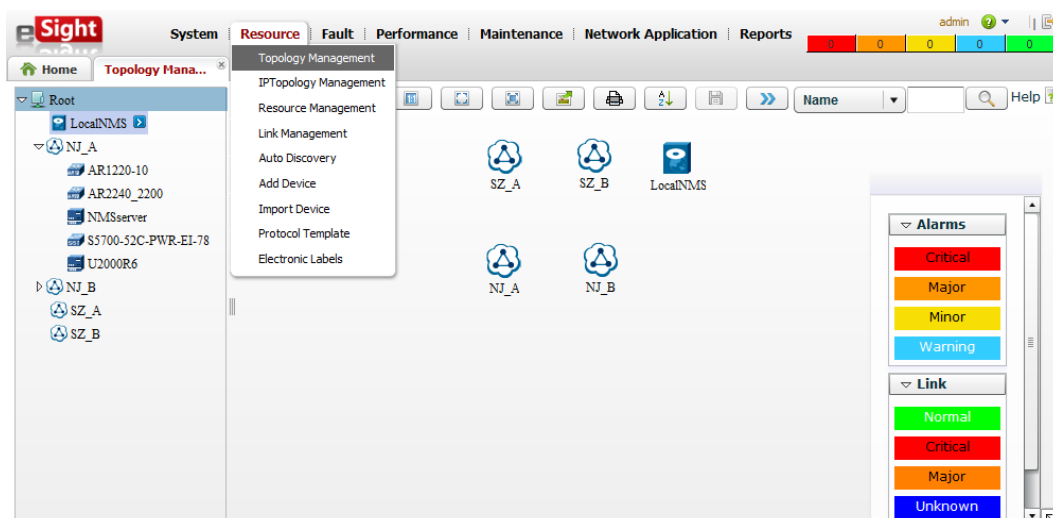
#### Context

The computer resolution is 1024 x 768.

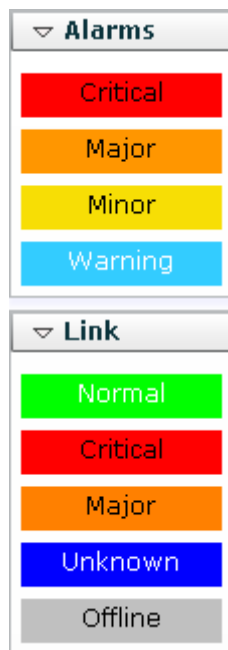
#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

**Figure 4-19** Topology Management



**Step 2** On the toolbar of the **Topology Management** window, choose  > **Show Legends**.  
Topology legends are shown in the following figure.



 **NOTE**

To close the topology legends, choose  > **Hide Legends** again.

----End

### 4.2.3.6 Setting a Device Label

This topic describes how to set a device label. The device label information includes the name and IP address of a device.

#### Prerequisites

You have the operation rights for **Modify Topology**.

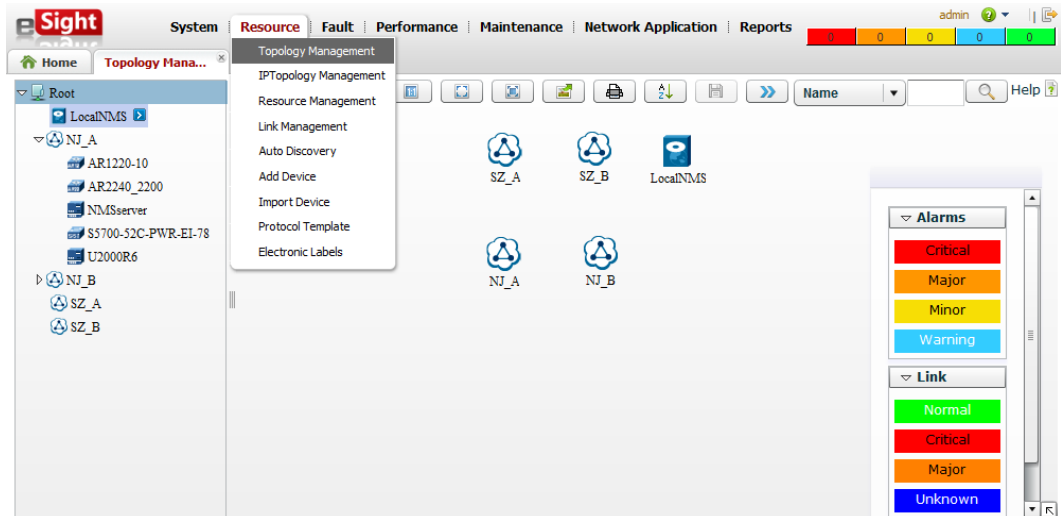
#### Context

- The computer resolution is 1024 x 768.
- If you do not select any of the device name, IP address, and system name, the device name is displayed by default.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

**Figure 4-20** Topology Management



**Step 2** On the toolbar of the **Topology Management** window, choose  > **Set Device Label**.

**Step 3** In the **Set Device Label** dialog box, select the device name, IP address, or system name.

**Figure 4-21** Set Device Label



**Step 4** Click **OK**.

The selected device information is displayed under the device icon.

----End

### 4.2.3.7 Printing the Physical View

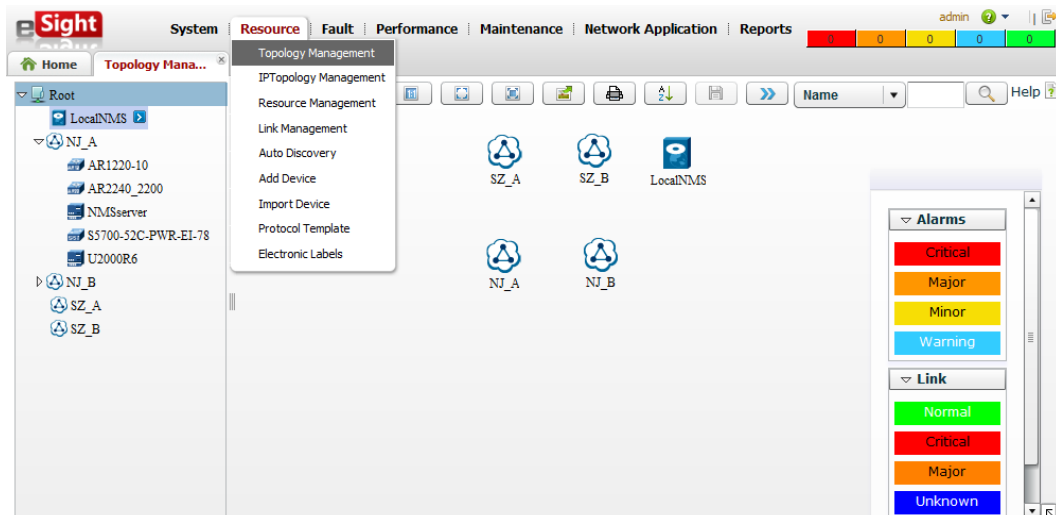
You can print the physical view.



## Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

**Figure 4-22** Topology Management



**Step 2** On the toolbar of the **Topology Management** window, click .

**Step 3** Set the print parameters.

**Step 4** Click **Print**.

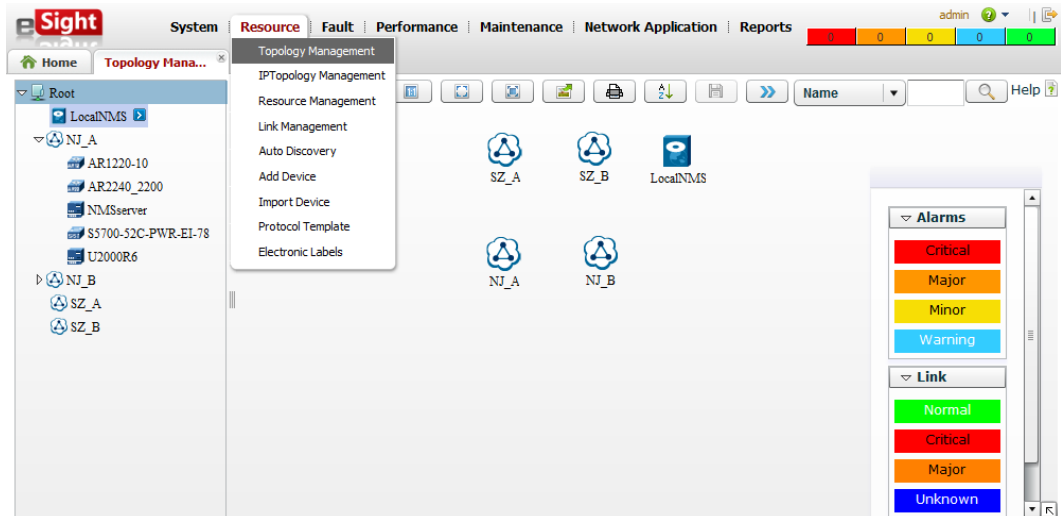
----End

### 4.2.3.8 Exporting the Physical View

You can export the physical view to a local PC.

## Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

**Figure 4-23** Topology Management

**Step 2** On the toolbar of the **Topology Management** window, click .

**Step 3** Select a path to save the file, and the file format.

**Step 4** Click **Save**.

----End

## 4.2.4 Example: Typical Topology Management Operations

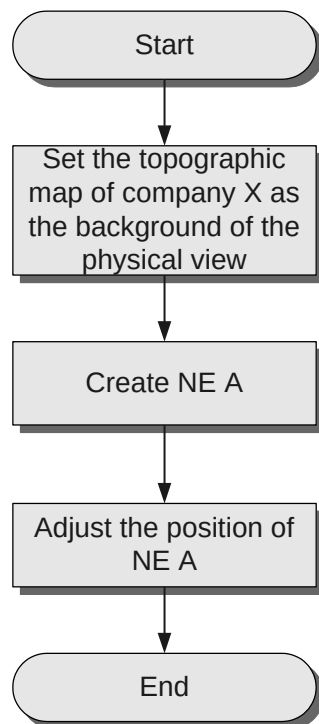
This topic describes an example about how to perform topology management operations. With this example, you can learn about the procedure for creating a topology view.

### Context

Due to the increase in service usage, company X purchases new devices. The administrator needs to add the devices to the topology view of the eSight for management.

[Figure 4-24](#) shows the procedure for creating a topology view.

**Figure 4-24** Procedure



## Procedure

**Step 1** Set the topographic map of company X as the background of the topology view

1. Choose **Resource** > **Topology Management** from the main menu.
2. On the toolbar of the **Topology Management** window, click .
3. In the **Set Background** dialog box, select **Show background image**, and click .
4. Select the topographic map file of company X and click **Open**.
5. Click **OK**.

**Step 2** Create NE A.

1. Choose **Resource** > **Add Device** from the main menu.
2. On the **Add Device** page, configure basic information about the NE to be created and SNMP parameters.
3. Click **OK**.

**Step 3** Adjust the position of NE A.

1. In the topology view, click NE A and drag it to a specified position.
2. On the toolbar, click  to save the setting.

----End

## 4.3 IP Topology Management

IP topology views are generated based on the analysis and computing of networks managed by eSight. IP topology views display the division of routing devices and subnets, and links between Layer 2 devices.

For details about operations for common buttons on the IP topology toolbar, see [4.2.2 Adjusting a Physical View](#) and [4.2.3 Browsing a Physical View](#).

### 4.3.1 IP Topology Management Functions

An IP topology consists of the Layer 2 and Layer 3 topology views. The Layer 2 topology view displays all devices on subnets and physical connections between these devices based on Layer 2 links. The Layer 3 topology view displays connections between routing devices and subnets based on IP links. During routine maintenance, you can view the Layer 2 and Layer 3 topology views to obtain the real-time information about routing devices, Link Layer Discovery Protocol (LLDP) links, IP links, and subnets.

[Table 4-2](#) lists IP topology management functions.

**Table 4-2** IP topology management functions

| Function               |                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP topology monitoring | Device alarm, subnet alarm, and link alarm   | <ul style="list-style-type: none"><li>• Device alarm: The color of a device icon indicates the highest severity of alarms generated on the device.</li><li>• Link alarm: The color of a link indicates the highest severity for alarms generated on the link. The severity depends on the highest severity of alarms generated on both ends of the link.</li><li>• Subnet alarm: The color of a subnet indicates the highest severity for alarms generated on the subnet.</li></ul> <b>NOTE</b><br>Topology views display icons that indicate the real-time highest severity of alarms that occur on devices, links, and subnets. |
|                        | Link status                                  | <ul style="list-style-type: none"><li>• The Layer 2 topology view displays the real-time status of LLDP links.</li><li>• The Layer 3 topology view displays the real-time status of IP links.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                        | Detailed information about links and devices | When you move the cursor to the icon of a device or link icon, the detailed information about the device or link is displayed in a pop-up window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                        | Viewing active alarms on the entire network  | In the IP topology view, right-click the blank area, and choose <b>Current Alarms</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                        | Viewing active alarms on a device            | In the IP topology view, right-click a device, and choose <b>Alarm List</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IP                     | Automatic                                    | eSight recognizes routing devices based on the routing function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Function            |                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| topology management | recognition of Layer 2 and Layer 3 devices | <p>If a device supports the routing and forwarding functions and has two or more interfaces (including physical interfaces and logical interfaces) to which IP addresses are assigned, eSight recognizes the device as a Layer 3 device; otherwise, eSight recognizes the device as a Layer 2 device.</p> <p><b>NOTE</b><br/>When a device is added to eSight, it will be displayed in the IP topology.</p>                                                                                                                                                                                                                                                                                                                                                                         |
|                     | Blank subnet display and hiding            | <p>A blank subnet refers to a subnet where no device is deployed. eSight can display and hide blank subnets as required.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                     | IP change management                       | <ul style="list-style-type: none"><li>• <b>IP Change Notification:</b> eSight monitors device IP address changes in real time. When a device IP address is changed, eSight notifies users of the change with an icon.</li><li>• <b>Remove IP Change Notifications:</b> If an IP change notification requires no further attention, you can remove it.</li><li>• <b>IP Changes:</b> When an IP change notification is displayed, you can view the IP change details in the IP change list.</li><li>• <b>IP Change Summary:</b> IP change summary lists detailed information about all IP changes on the entire network.</li><li>• <b>Remove All IP Change Notifications:</b> If all the current IP change notifications require no further attention, you can remove them.</li></ul> |

## 4.3.2 IP Topology Operations

This topic describes how to perform operations on the IP topology to monitor devices and links.

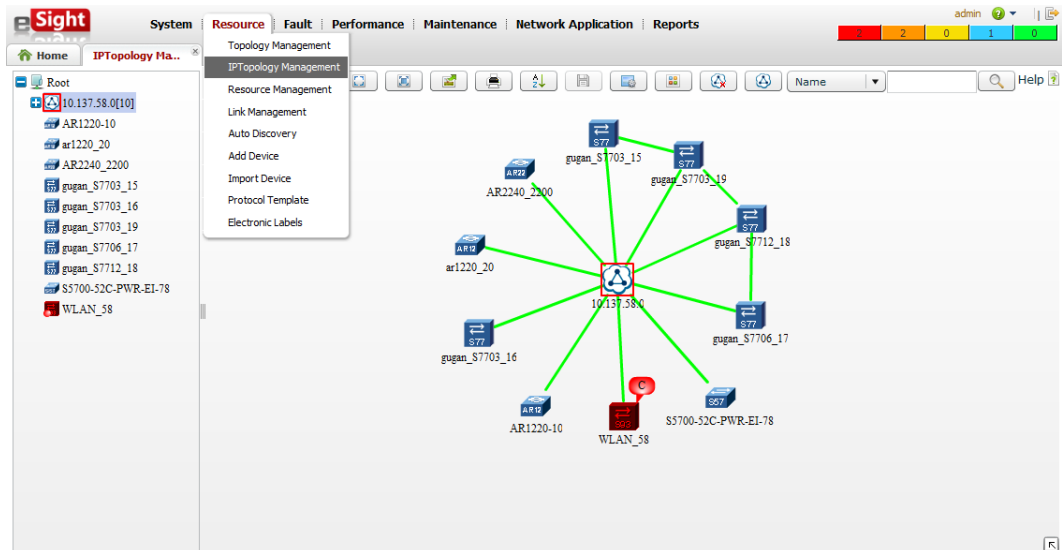
### Prerequisites

- Devices have been added to eSight.
- To remove IP change notifications, you must have the "operator" or a superior right.

### Procedure

- Check the Layer 3 topology view.
1. Choose **Resource > IP Topology Management**.

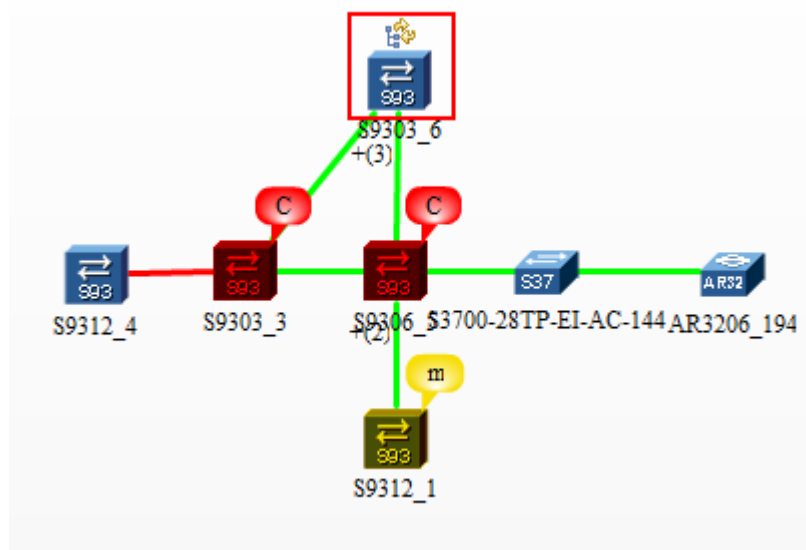
Figure 4-25 IP Topology Management



The Layer 3 topology view is displayed on the right.

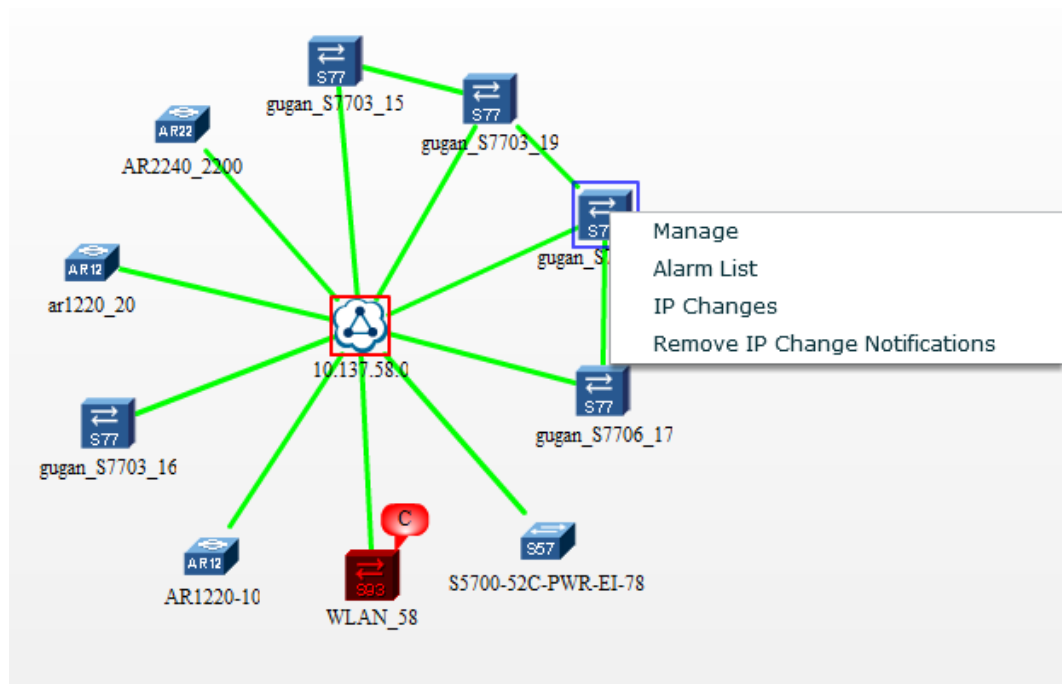
2. **Optional:** On the Layer 3 topology view, click  to sort subnets and devices in the current topology view. The Layer 3 topology view displays connections between Layer 3 devices and connections between Layer 3 devices and subnets.
3. **Optional:** On the Layer 3 topology view, click  to display blank subnets or click  to hide blank subnets.
  - Check the Layer 2 topology view.
    1. Choose **Resource > IP Topology Management**.
    2. You can check the Layer 2 topology view in either of the following ways:
      - On the Layer 3 topology view, double-click a subnet icon .
      - On the Layer 3 topology view, click a subnet icon  and click  to expand the Layer 2 topology view.
  - Manage IP changes.
    1. View IP change notifications: On the IP topology management page, if  is displayed on a device, the device IP address is changed.

**Figure 4-26** IP change notifications



2. View the device IP change list: On the IP topology management page, right-click a device with an IP change notification, and choose **IP Changes**.

### Figure 4-27 IP Changes



 **NOTE**

To view IP changes on the entire network, right-click the blank area on the IP topology management page, and choose **IP Change Summary**.

- Remove IP change notifications: On the IP topology management page, right-click a device with an IP change notification, and choose **Remove IP Change Notifications**.

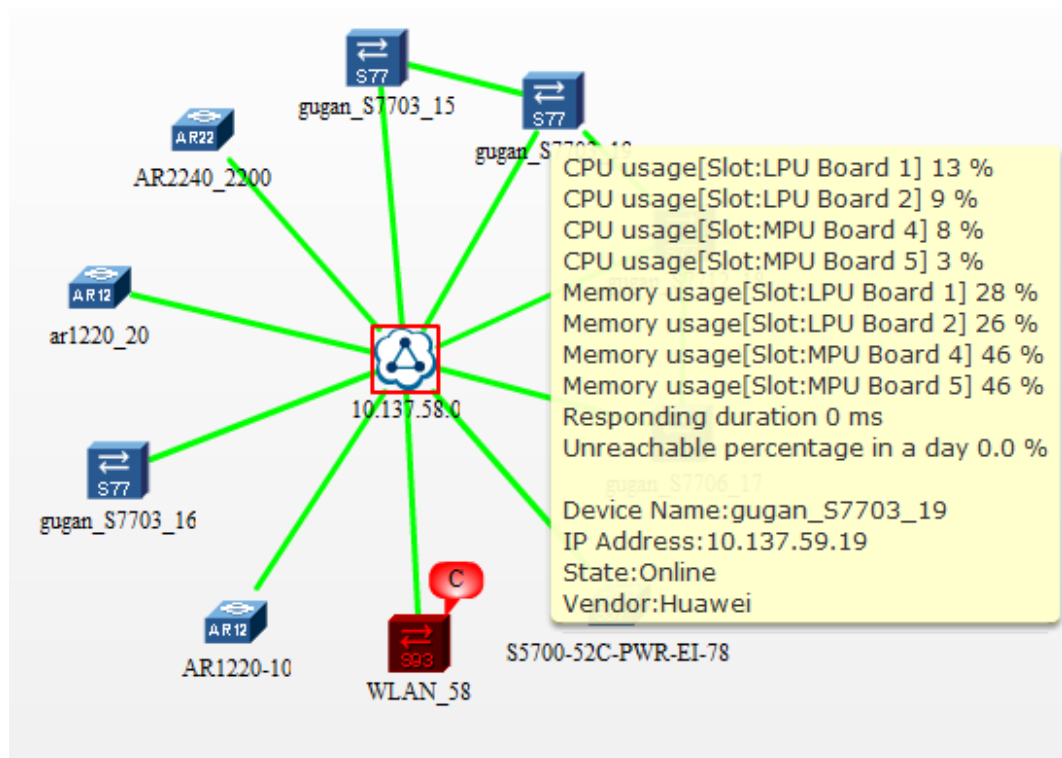


#### NOTE

To remove IP change notifications from the entire network, right-click the blank area on the IP topology management page, and choose **Remove All IP Change Notifications**.

- View device and link details.
  1. Choose **Resource > IP Topology Management**.
  2. Move the pointer to a device or link icon. The device or link information is displayed in the topology view.

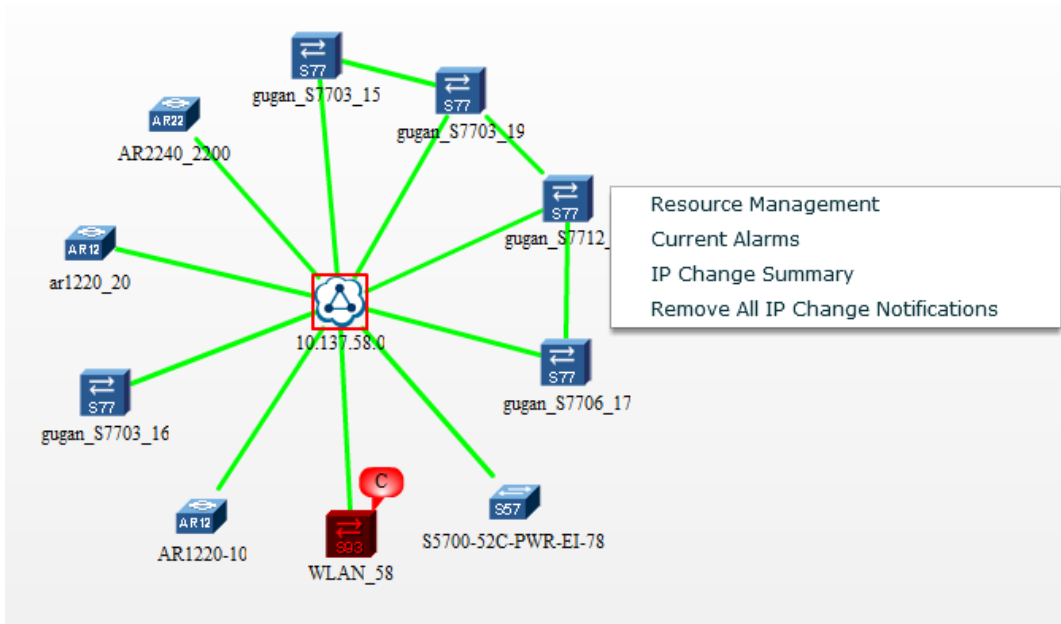
**Figure 4-28** Device information



- View alarms.
  - View alarms on a device: In the IP topology view, right-click a device, and choose **Alarm List**.
  - View alarms on the entire network: In the IP topology view, right-click the blank area, and choose **Current Alarms**.



Figure 4-29 Current Alarms



----End

### 4.3.3 Example: Typical Operations for IP Topology Management

This topic uses an example to describe the process of managing the IP topology.

#### Prerequisites

- Devices have been added to eSight.

#### Scenario

Company A added some devices to meet the service expansion requirement and deployed the devices on the same network segment (10.137.51.0). The following describes how to add the devices to the IP topology and view them in the topology view.

#### Operation Process

| Step                             | Description                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Recognize devices automatically. | When devices are added to eSight, the IP topology recognizes devices automatically and allocate them to proper subnets. |
| Check the Layer 3 topology view. | Check the Layer 3 topology view in the IP topology.                                                                     |
| Check the Layer 2 topology view. | Check the Layer 2 topology view in the IP topology.                                                                     |

## Procedure

**Step 1** Recognize devices automatically.

**Step 2** Check the Layer 3 topology view.

1. Choose **Resource > IP Topology Management**.
2. Find the newly created subnet 10.137.51.0 in the topology view.

**Step 3** Check the Layer 2 topology view: In the Layer 3 topology view, double-click subnet 10.137.51.0 to access the Layer 2 topology view.

----**End**

# 5 Fault Management

## About This Chapter

The eSight provides the functions of monitoring alarms, querying alarms or events, and setting remote alarm notification to help you detect, identify, and troubleshoot the network or device faults rapidly.

### 5.1 Overview of Fault Management Operations

This topic describes the fault management operations.

### 5.2 Setting Remote Alarm Notifications

You can set the rule for remote alarm notification, including notification condition, time, and mode. After setting the rule for remote alarm notification, the alarms meeting the rule are sent to the maintenance personnel, helping the remote maintenance personnel to get notified in a timely manner and take proper measures.

### 5.3 Setting a Fault Monitoring Rule

The eSight allows you to set fault monitoring rules, such as the alarm mask rule, alarm sound, and user-defined criteria.

### 5.4 Monitoring Alarms

The eSight provides physical view, alarm board, and alarm bar chart to help you monitor alarms, learn about alarm status, and take proper measures.

### 5.5 Alarm Analysis

By querying and analyzing historical alarms and events and masked alarms, you can learn about the alarm trend of an NE to determine whether to upgrade the NE.

### 5.6 Example: Typical Fault Management Operations

This topic describes an example about how to perform fault management operations. From the example, you will learn about the procedure and basic operations about fault management.

## 5.1 Overview of Fault Management Operations

This topic describes the fault management operations.

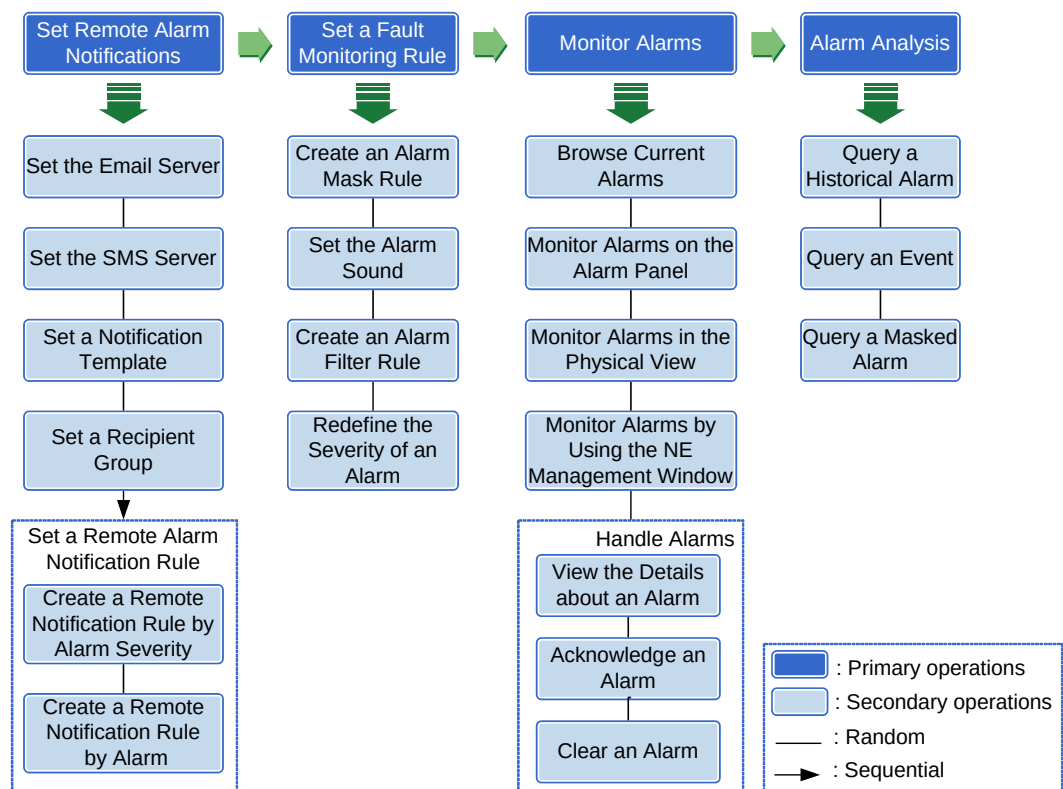
## Context

Before performing fault management operations, you must be familiar with the basic concepts about fault management, such as alarm severity, alarm status. For details, see [1.2.4 Basic Concepts of Fault Management](#). Understanding these concepts will help you avoid errors when performing fault management operations.

## Overview of Fault Management Operations

[Figure 5-1](#) shows the overview of fault management operations. For more details, click the operation in the overview.

**Figure 5-1** Overview of fault management operations



[Table 5-1](#) describes the fault management operations.

**Table 5-1** Fault operations

| Operation                                      | Description                                                                                                                                     |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">5.2.2 Setting the Email Server</a> | When an alarm is reported, you can set the parameters of the email server that sends remote notification to users by email.                     |
| <a href="#">5.2.3 Setting the SMS Server</a>   | When an alarm is reported, you can set the parameters of the short message service (SMS) server that sends remote notification to users by SMS. |
| <a href="#">5.2.4 Setting a Notification</a>   | You can customize a remote notification template for                                                                                            |

| Operation                                                                     | Description                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Template</a>                                                      | alarms or events. The eSight sends the alarms or events meeting the remote notification rules to users by email or SMS based on the template.                                                                                                                                                                 |
| <a href="#">5.2.5 Setting a Recipient Group</a>                               | When you set the remote alarm notification, you need to set the recipient group to be notified.                                                                                                                                                                                                               |
| <a href="#">5.2.6.1 Creating a Remote Notification Rule by Alarm Severity</a> | You can create a remote notification rule by alarm severity when you concern specified alarm severities.                                                                                                                                                                                                      |
| <a href="#">5.2.6.2 Creating a Remote Notification Rule by Alarm</a>          | You can create a remote notification rule by alarm when you learn about the alarm source of an alarm or event and the alarm or event information.                                                                                                                                                             |
| <a href="#">5.3.1 Creating an Alarm Mask Rule</a>                             | This topic describes how to create an alarm mask rule. For the alarms that are reported to the eSight and do not require attention, you can create a mask rule to mask them. The masked alarms are not displayed in the current alarm list. This helps you find the desired alarms in the current alarm list. |
| <a href="#">5.3.2 Setting the Alarm Sound</a>                                 | You can specify alarm sounds for different alarm severities. When an alarm is generated, the sound box in the host produces a sound.                                                                                                                                                                          |
| <a href="#">5.3.3 Creating an Alarm Filter Rule</a>                           | If the default alarm filter rules cannot meet user requirements, you can create an alarm filter as required.                                                                                                                                                                                                  |
| <a href="#">5.3.4 Redefining the Severity of an Alarm</a>                     | Redefining the severity of an alarm helps you to draw more or less attention to the alarm.                                                                                                                                                                                                                    |
| <a href="#">5.4.1 Browsing Current Alarms</a>                                 | You can set the filter criteria in the current alarm list to view the alarms to be concerned and handled.                                                                                                                                                                                                     |
| <a href="#">5.4.2 Monitoring Alarms on the Alarm Panel</a>                    | You can view the alarm panel to learn about the number of different severities of alarms or learn about the alarm status from the alarm panel or alarm sound.                                                                                                                                                 |
| <a href="#">5.4.3 Monitoring Alarms in the Physical View</a>                  | The physical view allows you to monitor the alarms of NEs real time.                                                                                                                                                                                                                                          |
| <a href="#">5.4.4 Monitoring Alarms by Using the NE Management Window</a>     | This topic describes how to view the alarm information about the NEs managed by the eSight under resource management. The alarm information reflects the running status of an NE, which helps discover and resolve the fault as soon as possible.                                                             |
| <a href="#">5.4.5.2 Viewing the Details about an Alarm</a>                    | You can view the details about current alarms, historical alarms, and masked alarms in the eSight. Alarm details include the alarm name, advice, and location information.                                                                                                                                    |
| <a href="#">5.4.5.3 Acknowledging an Alarm</a>                                | This topic describes how to acknowledge an alarm. Acknowledging an alarm is to indicate that the alarm has been handled and can be ignored.                                                                                                                                                                   |
| <a href="#">5.4.5.4 Clearing an Alarm</a>                                     | If an alarm cannot be cleared automatically or does not                                                                                                                                                                                                                                                       |

| Operation                                         | Description                                                                                            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------|
|                                                   | exist on an NE, you need to manually clear the alarm. If the alarm is cleared, the fault is rectified. |
| <a href="#">5.5.1 Querying a Historical Alarm</a> | You can quickly find the desired historical alarms based on specified search criteria.                 |
| <a href="#">5.5.2 Querying an Event</a>           | You can query events to learn about the information sent from a device to the eSight.                  |
| <a href="#">5.5.3 Querying a Masked Alarm</a>     | This topic describes how to quickly query the desired masked alarms.                                   |

## 5.2 Setting Remote Alarm Notifications

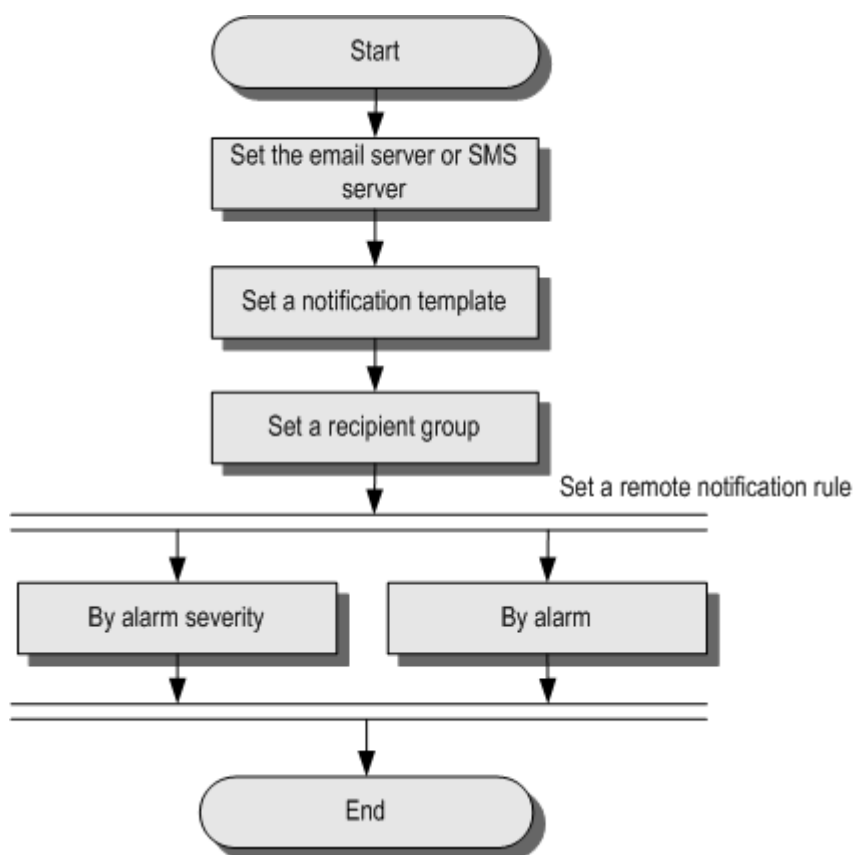
You can set the rule for remote alarm notification, including notification condition, time, and mode. After setting the rule for remote alarm notification, the alarms meeting the rule are sent to the maintenance personnel, helping the remote maintenance personnel to get notified in a timely manner and take proper measures.

### 5.2.1 Procedure for Setting Remote Notification

This topic describes the procedure for setting remote notification. If an alarm is detected in the eSight, you can send alarm information that meeting the remote notification rules to the maintenance personnel, so that the maintenance personnel who are not on site can learn about the alarm on the server and take appropriate measures.

## Flow Chart of Setting Remote Notification

Figure 5-2 Procedure for setting remote notification



## Procedure Description

Table 5-2 Procedure description

| Step | Operation                                                  | Description                                                                                                                                                                                        |
|------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Set the email server or short message service (SMS) server | You can set the parameters of the email server or SMS server. The eSight can send the alarms or events meeting the remote notification rules to users by email or SMS.                             |
| 2    | Set a notification template                                | You can customize a remote notification template for alarms or events. The eSight sends the alarms or events meeting the remote notification rules to users by email or SMS based on the template. |
| 3    | Set a recipient group                                      | You can set the user name, mobile phone number, and email address of the user to be notified. The eSight sends alarms or events meeting the remote notification rules to the user by email or SMS. |
| 4    | Set a remote notification                                  | You can add notification rules by <b>By Alarm Severity</b>                                                                                                                                         |

| Step | Operation | Description                                                                                                        |
|------|-----------|--------------------------------------------------------------------------------------------------------------------|
|      | rule      | and <b>By Alarm</b> . The alarms meeting notification rules are sent to the maintenance personnel by email or SMS. |

## 5.2.2 Setting the Email Server

When an alarm is reported, you can set the parameters of the email server that sends remote notification to users by email.

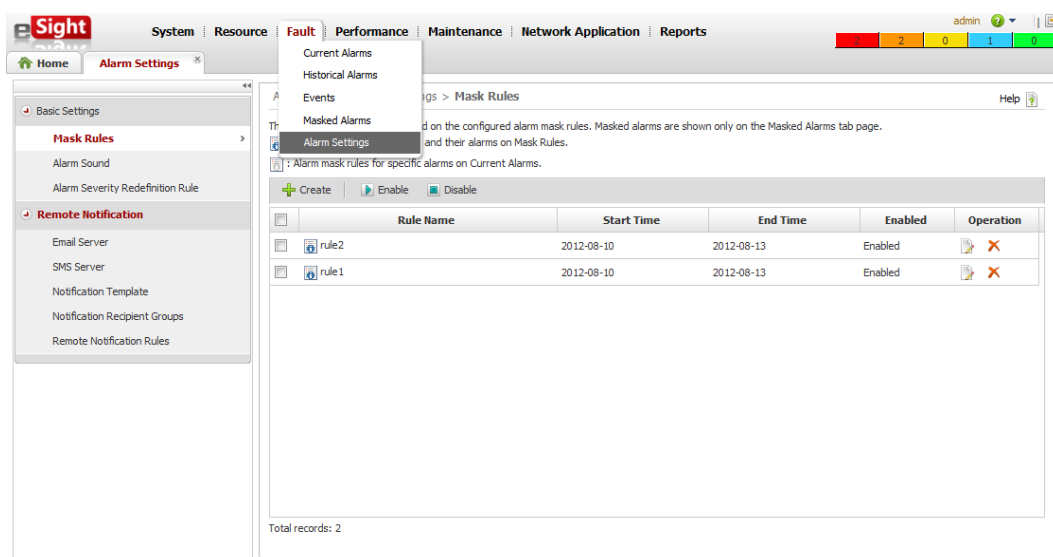
### Prerequisites

- You have the operation rights for **Alarm Settings** and **System Configuration**.
- The email server IP address and sender address are obtained.

### Procedure

**Step 1** Choose **Fault > Alarm Settings** from the main menu.

Figure 5-3 Alarm settings



**Step 2** In the **Alarm Settings** window, choose **Remote Notification > Email Server**.

**Step 3** On the **Email Server Settings** page, set the email server, sender address and server port.

- SMTP server:** the IP address of the email server.
- Sender address:** the email address of the sender.
- Server port:** the port on the email server used to connect to the eSight.



#### NOTE

The default SMTP port number is 25 and the default SSL port number is 465. Ensure that the server port is correct for successful email transmission.



- **Require authentication:** Determines whether the current user has permissions to send emails. If the email server requires authentication, you need to select **Require authentication** and set the user name and password of the email server.
- **Require SSL:** Determines the protocol used to connect to the email server.
  - Select the check box: The SSL protocol is used.
  - Deselect the check box: The SMTP protocol is used.

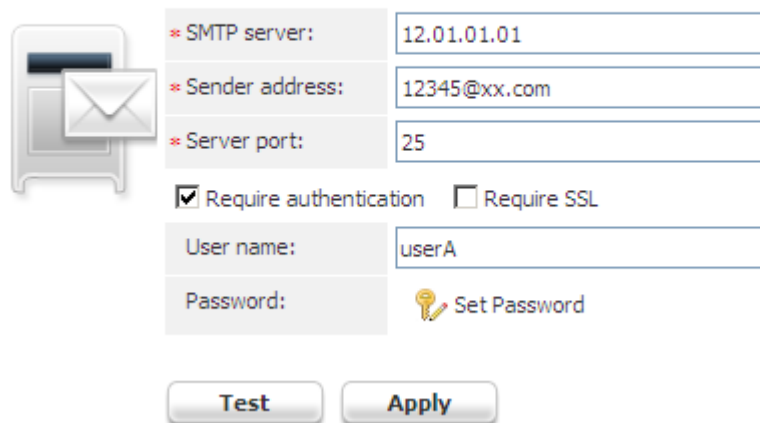


## CAUTION

If the SSL protocol is used to connect to email server, an SSL certificate must be installed. For details on how to install the SSL certificate, see [16.9 How Do I Install an SSL Certificate for the Email Server?](#).

**Figure 5-4** Setting the email server

Alarm Settings > Remote Alarm Notification > **Email Server Settings**



The form is titled 'Email Server Settings' and is preceded by an icon of an envelope and a document. It contains the following fields and controls:

- \* SMTP server:** Text box containing '12.01.01.01'.
- \* Sender address:** Text box containing '12345@xx.com'.
- \* Server port:** Text box containing '25'.
- ☒ **Require authentication** and ☐ **Require SSL** (checkboxes).
- User name:** Text box containing 'userA'.
- Password:** Text box with a key icon and the text 'Set Password'.
- Test** and **Apply** buttons at the bottom.

**Step 4** Click **Apply**.



### NOTE

- Click **Test** to check the connection to the Email server. The system displays a message showing the connection status. When you test the server connection, if the entered parameter is incorrect, the response will be slow and it might take some time.
- In the emailRecipient.xml file in eSight server installation directory\AppBase\etc\oms.core, you can change the email address for receiving test success emails.

----End

## 5.2.3 Setting the SMS Server

When an alarm is reported, you can set the parameters of the short message service (SMS) server that sends remote notification to users by SMS.

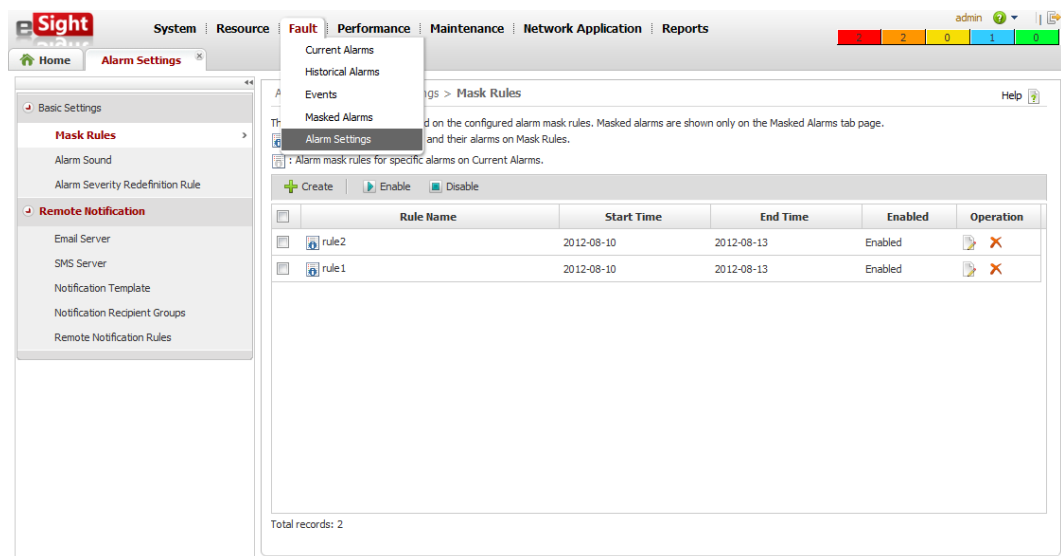
## Prerequisites

- You have the operation rights for **Alarm Settings**.
- The host name, port, code protocol, and calling number of the SMS server are obtained.

## Procedure

**Step 1** Choose **Fault > Alarm Settings** from the main menu.

Figure 5-5 Alarm settings



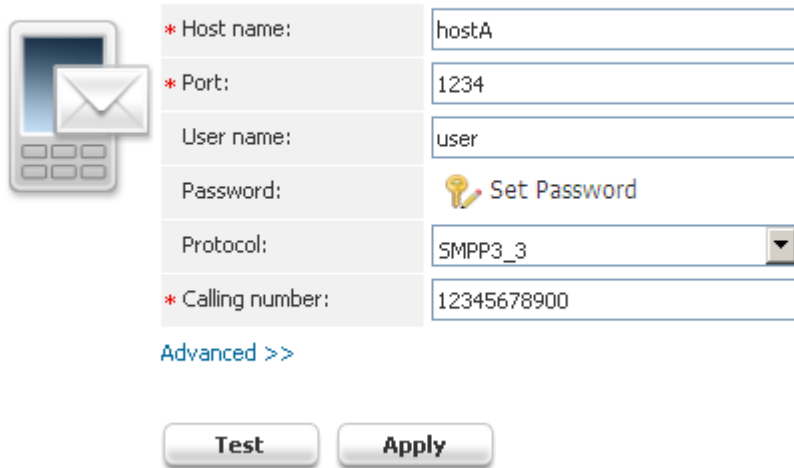
**Step 2** In the **Alarm Settings** window, choose **Remote Notification > SMS Server**.

**Step 3** In the **SMS Server Settings** window, set the host name, port number, and calling number.

- **Host name:** the host name or IP address of the short message center.
- **Port:** the port number of the short message center. You can set it as required.
- **Calling number:** calling number for sending a short message.

**Figure 5-6** Setting the SMS server

Alarm Settings > Remote Notification > **SMS Server Settings**



The form contains the following fields and controls:

- \* Host name:** Text input field with value "hostA".
- \* Port:** Text input field with value "1234".
- User name:** Text input field with value "user".
- Password:** Text input field with a "Set Password" button (key icon) next to it.
- Protocol:** Dropdown menu with "SMPP3\_3" selected.
- \* Calling number:** Text input field with value "12345678900".
- Advanced >>** Link below the fields.
- Test** and **Apply** buttons at the bottom.

 **NOTE**

If you want to send long messages and status reply, click **Advanced** to set related parameters.

The maximum length supported for a short message varies according to the protocol you select.

**Table 5-3** Short message length supported by each protocol

| Encoding Protocol | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMPP3_3/SMPP3_4   | <ul style="list-style-type: none"><li>Supports long short messages.</li></ul> <p>The recipient can receive the entire message, no matter how many characters are contained a short message sent by the sender.</p> <ul style="list-style-type: none"><li>Do not support long short messages.</li></ul> <p>A short message contains a maximum of <b>70</b> characters. If a message contains more than <b>70</b> characters, the system splits the message and sends several short messages to the recipient.</p> |
| CMPP2_x/CMPP3_x   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SGIP              | <ul style="list-style-type: none"><li>Supports long short messages.</li></ul> <p>The recipient can receive the entire message, no matter how many characters are contained a short message sent by the sender.</p> <ul style="list-style-type: none"><li>Do not support long short messages.</li></ul> <p>A short message contains a maximum of <b>80</b> characters. If a message contains more than <b>80</b> characters, the system splits the message and sends several short messages to the recipient.</p> |

**Step 4** Click **Apply**.**NOTE**

- Click **Test** to check the connection to the SMS server. The system displays a message showing the connection status. When you test the server connection, if the entered parameter is incorrect, the response will be slow and it might take some time.
- In the smRecipient.xml file in eSight server installation directory\AppBase\etc\oms.fm, you can change the mobile number for receiving test success SMS messages.

----End

## 5.2.4 Setting a Notification Template

You can customize a remote notification template for alarms or events. The eSight sends the alarms or events meeting the remote notification rules to users by email or SMS based on the template.

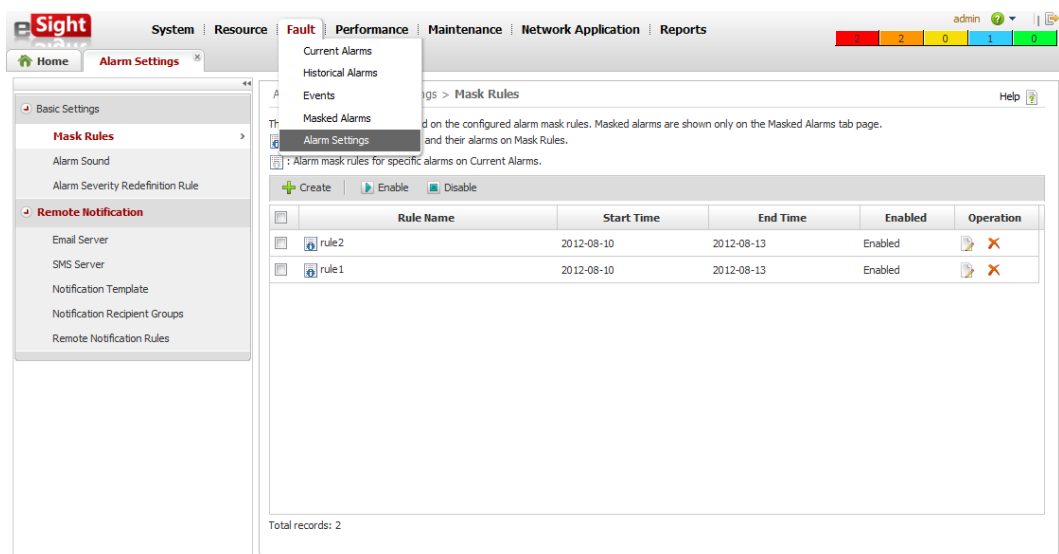
### Prerequisites

You have the operation rights for **Alarm Settings**.

### Procedure

**Step 1** Choose **Fault > Alarm Settings** from the main menu.

**Figure 5-7** Alarm settings

**Step 2** In the **Alarm Settings** window, choose **Remote Notification > Notification Template**.**Step 3** In the **Notification Template Settings** page, set the alarm or event notification template.

- Set the alarm notification template:  
On the **Alarm Template** tab page, select the alarm field to be added under the **Available Alarm Fields**. Click  to add the field to the **Selected Alarm Fields** list.

In the **Selected Alarm Fields** list, click  or  to adjust the location of the field.

- Set the event notification template:

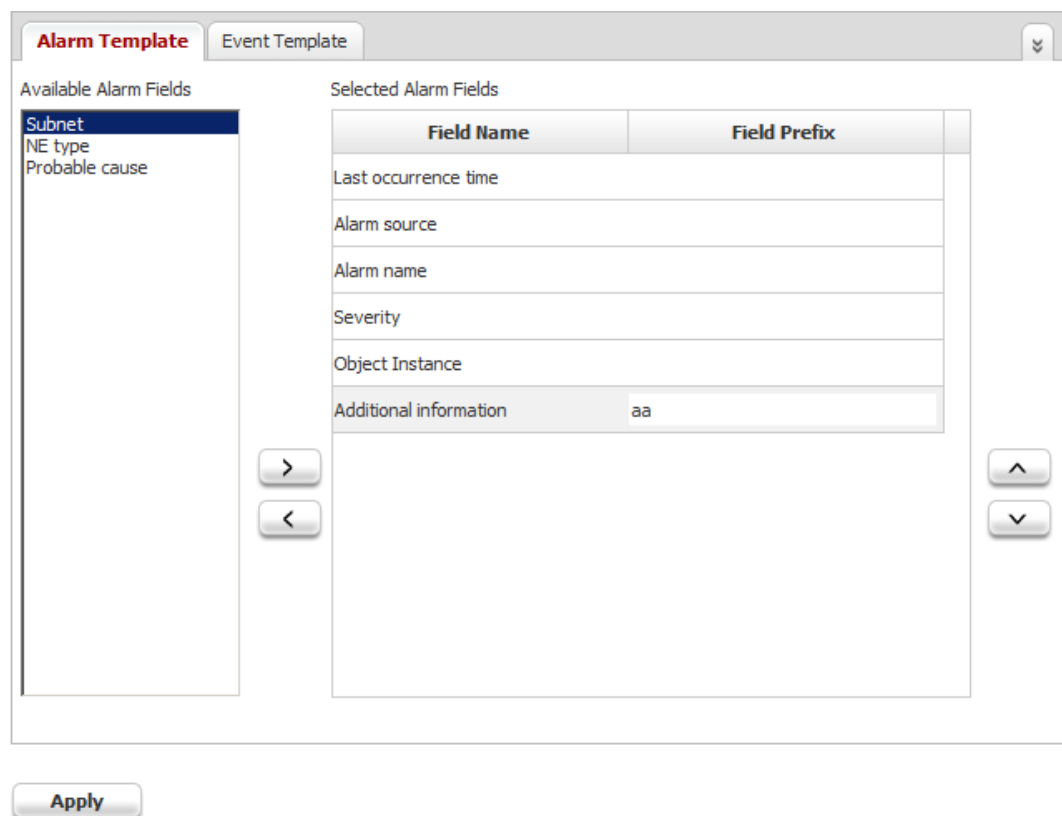
On the **Event Template** tab page, select the event field to be added under **Available**

**Event Fields**. Click  to add the field under **Selected Event Fields**.

In the **Selected Event Fields** list, click  or  to adjust the location of the field.

In the **Selected Alarm Fields** or **Selected Event Fields** area, set the prefix of **Field Name**. When an alarm or event is sent to users by SMS, the specified prefix is automatically added before the notification information field.

**Figure 5-8** Setting the template of alarm or event notification



| Field Name             | Field Prefix |
|------------------------|--------------|
| Last occurrence time   |              |
| Alarm source           |              |
| Alarm name             |              |
| Severity               |              |
| Object Instance        |              |
| Additional information | aa           |

**Step 4** Click **Apply**.

----End

## 5.2.5 Setting a Recipient Group

When you set the remote alarm notification, you need to set the recipient group to be notified.

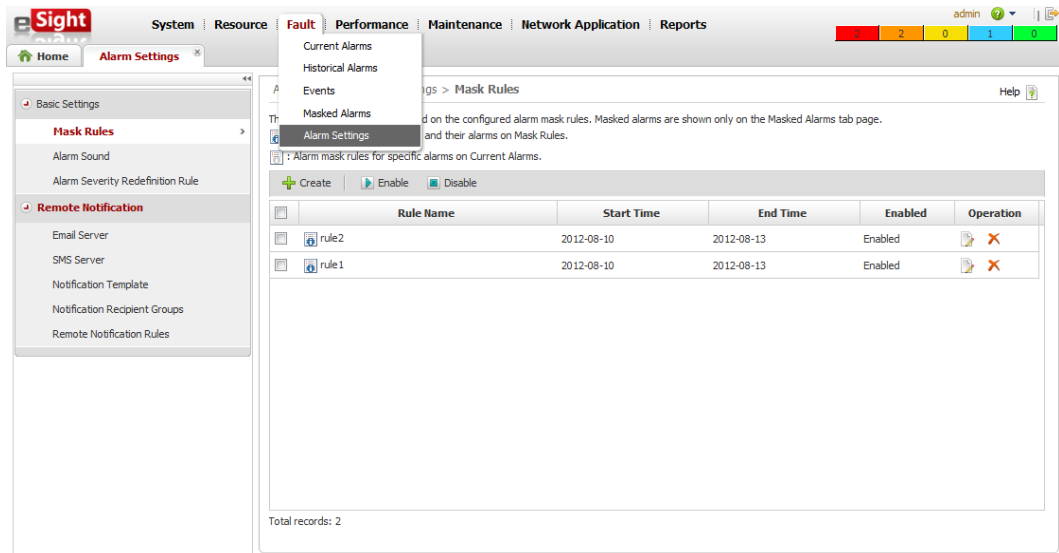
## Prerequisites

You have the operation rights for **Alarm Settings**.

## Procedure

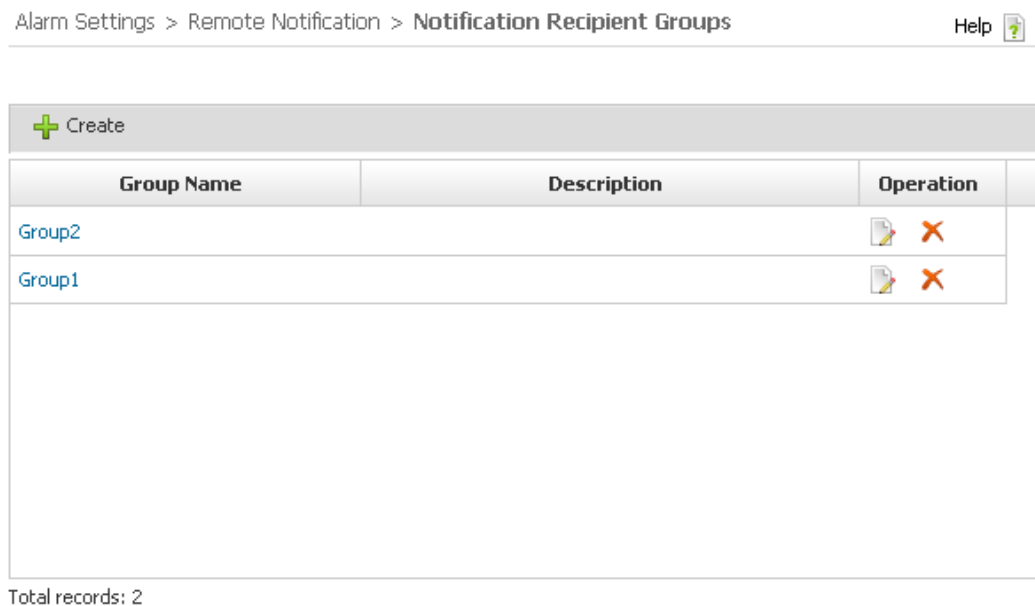
**Step 1** Choose **Fault > Alarm Settings** from the main menu.

**Figure 5-9** Alarm settings



**Step 2** In the **Alarm Settings** window, choose **Remote Notification > Notification Recipient Groups**.

**Figure 5-10** Notification recipient groups



**Step 3** In the **Notification Recipient Groups** page, you can perform the following operations.

| Setting Recipient Groups         | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a recipient group         | <ol style="list-style-type: none"><li>1. Click <b>Create</b>.</li><li>2. On the <b>Create Recipient Group</b> page, set the name and description of the recipient group, and add users to the recipient group.<br/>Add users to the recipient group:<ol style="list-style-type: none"><li>a. On the <b>Create Recipient Group</b> page, click <b>Create</b>.</li><li>b. In the <b>Create Recipient</b> dialog box, set the user name, mobile phone number, and email address.</li><li>c. Click <b>OK</b>.</li></ol><br/>On the <b>Create Recipient Group</b> page, click  or  in the <b>Operation</b> column where the required user information is located to modify or delete the user information.</li><li>3. On the <b>Create Recipient Group</b> page, click <b>Save</b>.</li></ol> |
| View recipient Group             | <ol style="list-style-type: none"><li>1. Click <b>Group Name</b> of the required recipient group.</li><li>2. On the <b>View User Group</b> page, view the recipient group information and user information.</li></ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Edit a recipient group and users | <ol style="list-style-type: none"><li>1. Click  in the <b>Operation</b> column where the required recipient group information is located.</li><li>2. On the <b>Modify User Group</b> page, modify the name, description, and user information about the recipient group.<br/>Modifying user information involves adding, deleting, and modifying user information.</li></ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Delete a recipient group         | <ol style="list-style-type: none"><li>1. Click  in the <b>Operation</b> column where the required recipient group information is located.</li><li>2. In the <b>Confirm</b> dialog box, click <b>Yes</b>.</li></ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

----End

## 5.2.6 Setting a Remote Alarm Notification Rule

This topic describes how to set a remote alarm notification rule. Based on the specified notification rule, the eSight sends related alarms to the maintenance personnel by email or SMS.

**By Alarm Severity** and **By Alarm** are the two methods of adding a notification rule.

- **By Alarm Severity:** When the alarm of a specified severity is generated or cleared, the eSight sends a remote notification to a specified user group.
- **By Alarm:** When the alarm of a specified NE is generated or cleared, the eSight sends a remote notification to a specified user group.

### 5.2.6.1 Creating a Remote Notification Rule by Alarm Severity

You can create a remote notification rule by alarm severity when you concern specified alarm severities.

#### Prerequisites

You have the operation rights for **Alarm Settings**.

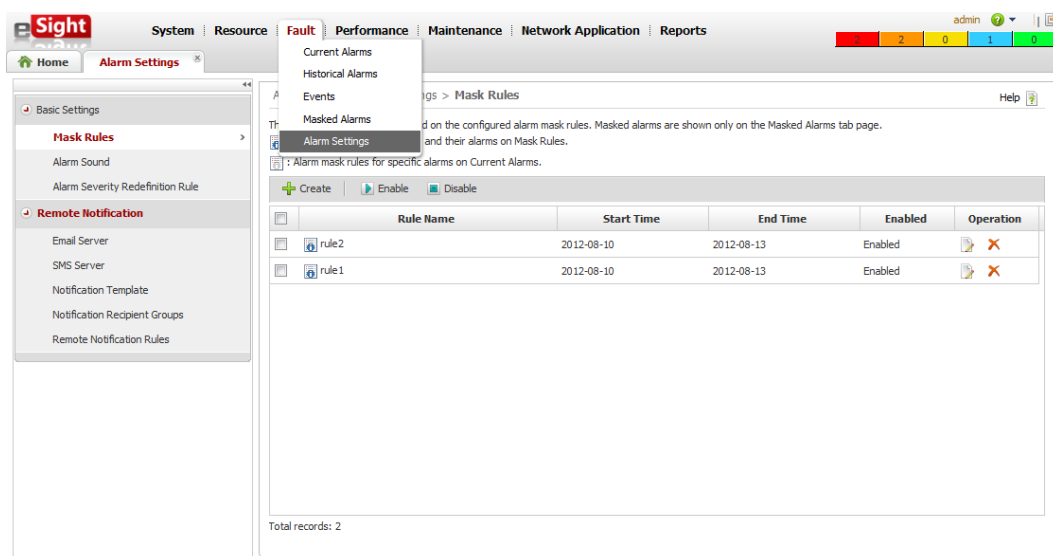
#### Context

A remote notification rule is enabled by default once it is created.

#### Procedure

**Step 1** Choose **Fault > Alarm Settings** from the main menu.

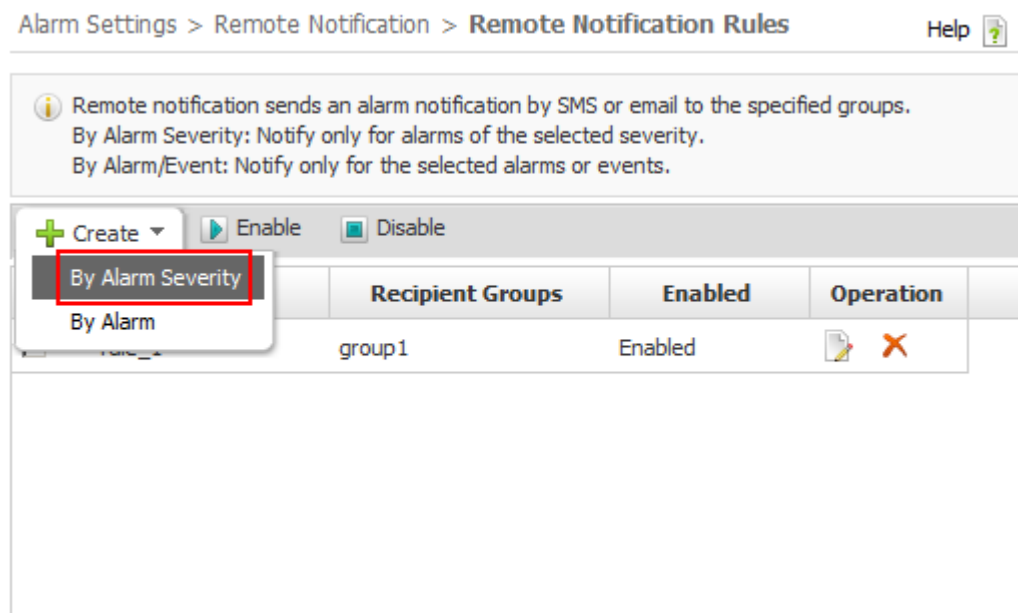
**Figure 5-11** Alarm settings



**Step 2** In the **Alarm Settings** window, choose **Remote Notification > Remote Notification Rules**.

**Step 3** In the **Remote Notification Rules** page, choose **Create > By Alarm Severity**.



**Figure 5-12** Creating remote notification rules by alarm severity

**Step 4** In the **Create By Alarm Severity** page, set **Rule name**, **Severity**, and **Notification recipient groups**.

 **NOTE**

- You can click  to set multiple recipient groups.
- In the **Notification recipient groups** drop-down list, you can select or add a user group. For details, see [5.2.5 Setting a Recipient Group](#).

**Step 5** Click **Save**.

----End

## Follow-up Procedure

In the **Remote Notification Rules** page, you can perform the following operations.

| Setting Notification Rules | Operation Method                                                                                                                                                                                                                                          |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable notification rules  | Enable a disabled remote notification rule.<br>Select one or more notification rules and click <b>Enable</b> to enable the notification rules.                                                                                                            |
| Disable notification rules | Disable a remote notification rule that is not used currently.<br>Select one or more notification rules and click <b>Disable</b> to disable the notification rules.                                                                                       |
| Modify notification rules  | Modify a remote notification rule to meet management requirements.<br>1. Click  in the <b>Operation</b> column where the required remote notification rule is located. |

| Setting Notification Rules | Operation Method                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | 2. On the <b>By Alarm Severities</b> or <b>By Alarm</b> page, modify the remote notification rule information.                                                                                                                                                                                                                                                       |
| Delete notification rules  | Delete an unused remote notification rule to ensure sufficient memory and proper running of tasks on the server.<br><br>1. Click  in the <b>Operation</b> column where the required remote notification rule is located.<br>2. In the <b>Confirm</b> dialog box, click <b>Yes</b> . |

### 5.2.6.2 Creating a Remote Notification Rule by Alarm

You can create a remote notification rule by alarm when you learn about the alarm source of an alarm or event and the alarm or event information.

#### Prerequisites

You have the operation rights for **Alarm Settings**.

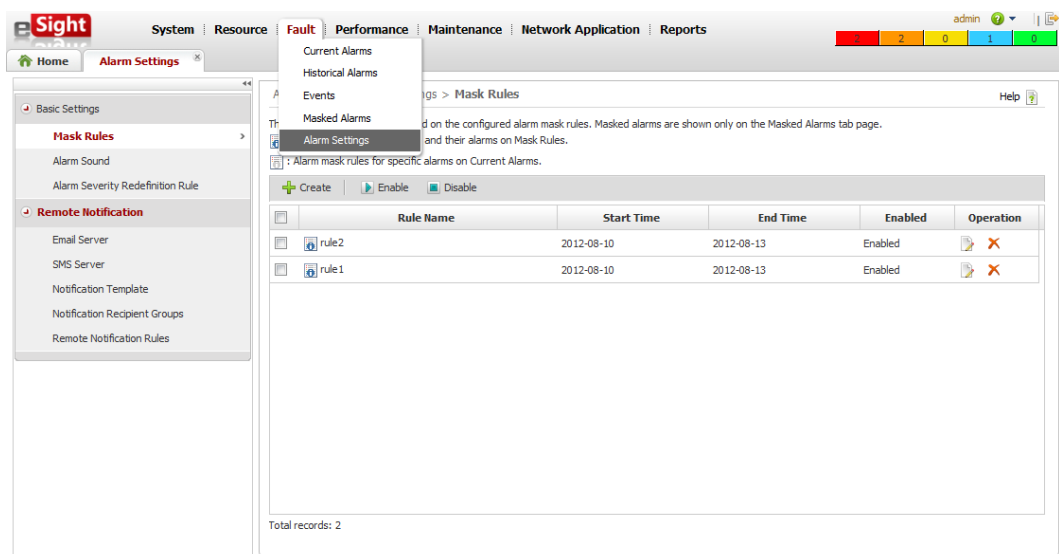
#### Context

A remote notification rule is enabled by default once it is created.

#### Procedure

**Step 1** Choose **Fault > Alarm Settings** from the main menu.

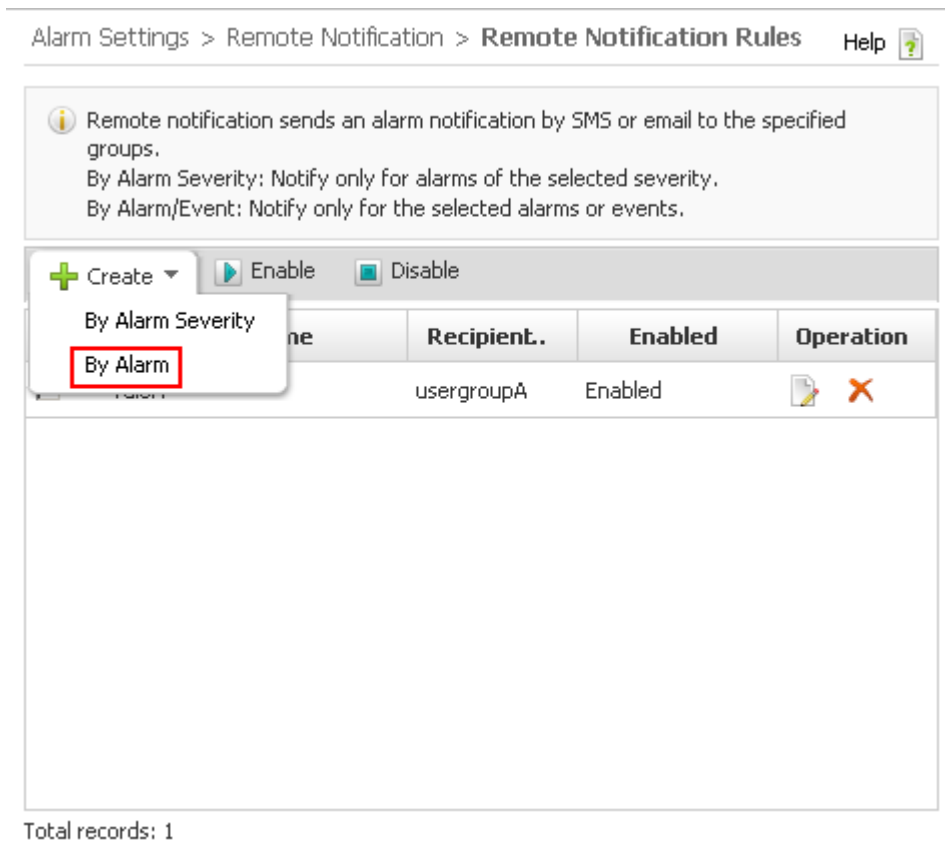
**Figure 5-13** Alarm settings



**Step 2** In the **Alarm Settings** window, choose **Remote Notification > Remote Notification Rules**.

**Step 3** On the **Remote Notification Rules** page, choose **Create > By Alarm**.

**Figure 5-14** Creating remote notification rules by alarm



**Step 4** Select an alarm source.

- Under **Alarm Sources** step on the **Create by Alarm** page, set **Rule name** and click **Add Alarm Sources**.

**Figure 5-15** Adding alarm sources

Alarm Settings > Remote Notification > Remote Notification Rules > **Create by Alarm** Help ?

Alarm Sources      Alarms/Events      Recipient Groups

Rule name:

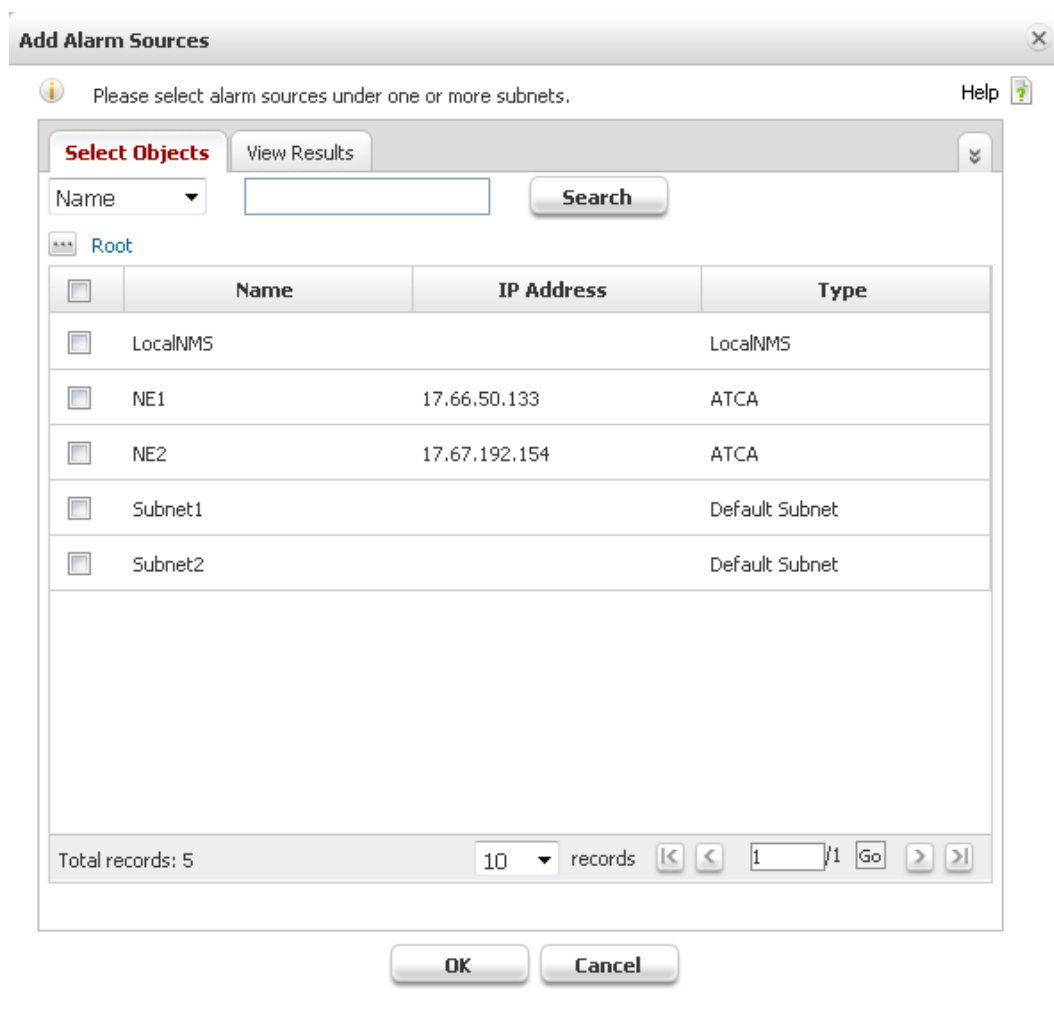
+ Add Alarm Sources ✕ Delete

Next Cancel

2. Under **Select Objects** in the **Add Alarm Sources** dialog box, select alarm sources.

 **TIP**

- Click a subnet name to open the list of devices or subnets.
- Click a node in the navigation tree, for example, **ROOT**. The related page is displayed.
- Set the keyword of **Name**, **IP Address**, or **Type** to search for the NEs or subnets that meet the search criteria.

**Figure 5-16** Selecting objects

3. On the **View Results** tab page, view the selected alarm sources.

 **NOTE**

- On the **View Results** tab page, you can click  in the **Operation** column to deselect the required alarm sources.
- You can click **Clear All** on the **View Results** tab page to clear the alarm sources on the **View Results** tab page.

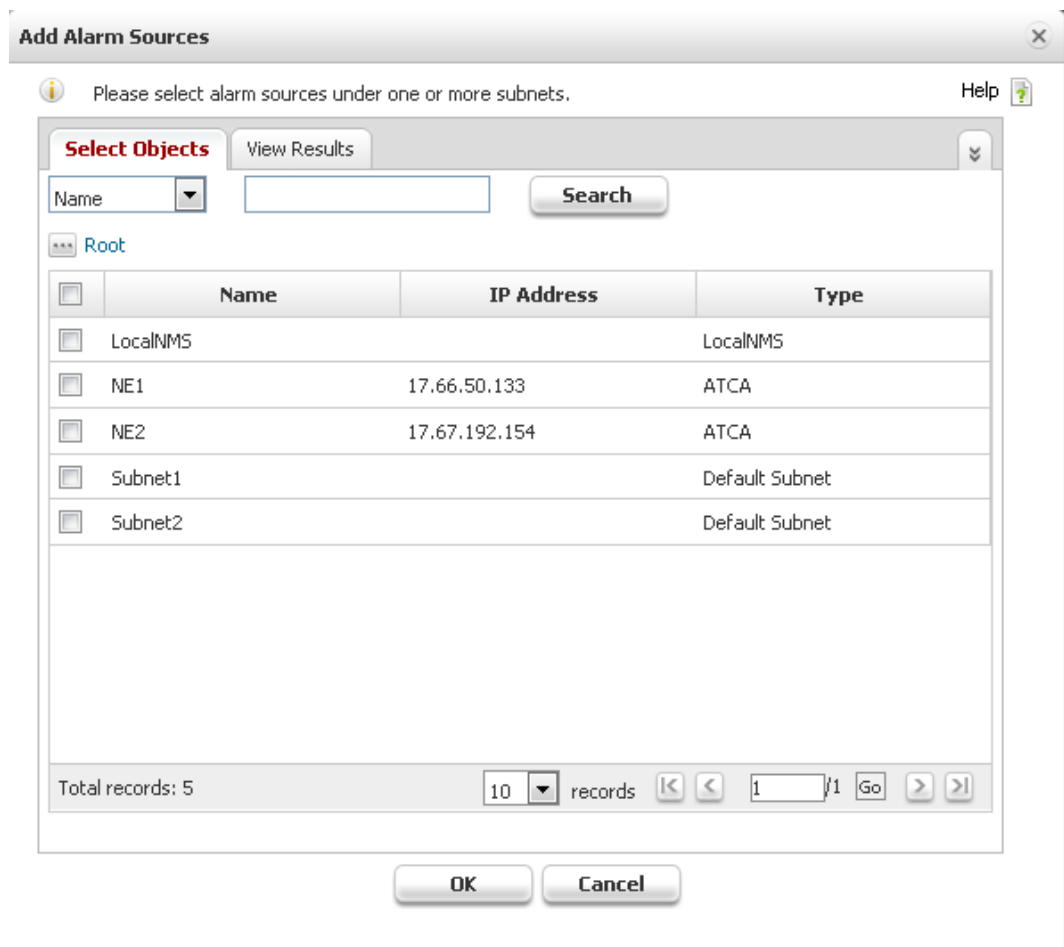
4. Click **OK**.
5. Click **Next**.

**Step 5** Select an alarm or event.

**NOTE**

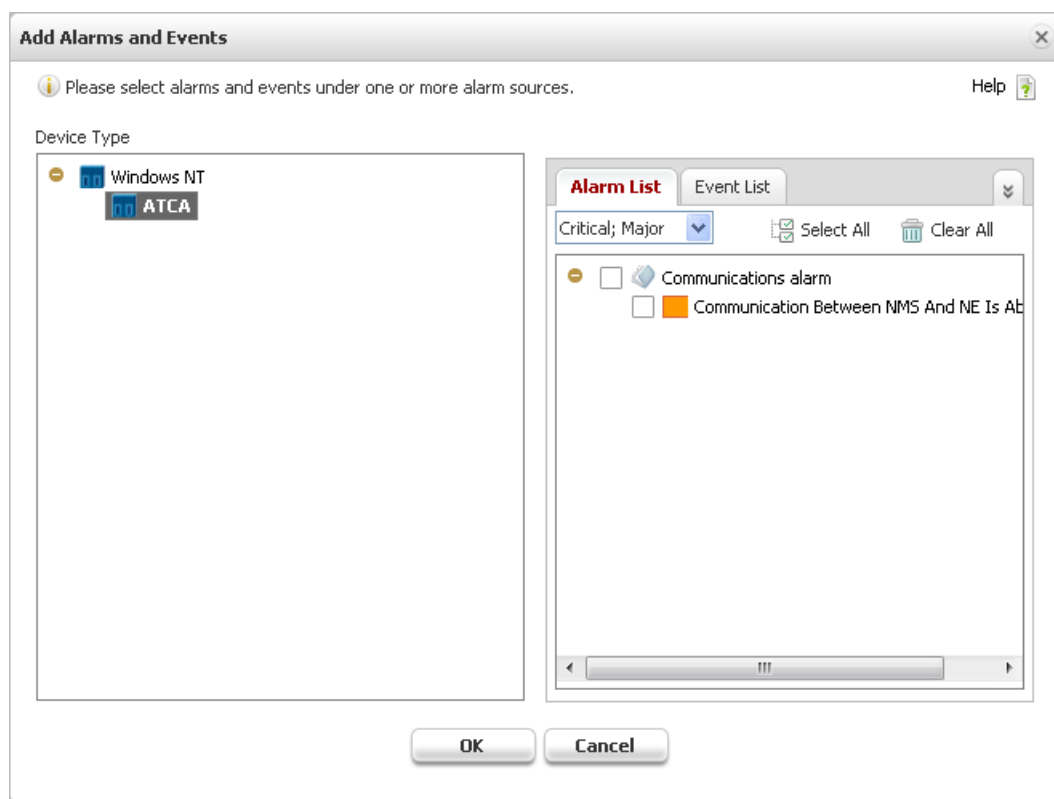
- If you select a subnet under the **Alarm Sources** step, you can select an alarm or event under the **Alarms/Events** step for all NEs in the subnet.
- If you select an NE under the **Alarm Sources** step, you can select an alarm or event under the **Alarms/Events** step for only the selected NE.
- If you select only a resource of an NE under the **Alarm Sources** step, you can select an alarm or event under the **Alarms/Events** step for the selected resource and the NE.

1. Under **Alarms/Events** step on the **Create by Alarm** page, click **Add Alarms and Events**.

**Figure 5-17** Adding alarms and events

2. Under **Device Type** in the **Add Alarms and Events** dialog box, select a device type.
  - After you select a device type, the alarms or events under the device type are displayed on the right pane.
  - A red asterisk (\*) is displayed in the upper right corner of the selected device type, which indicates that you selected the alarms or events under the device type.

**Figure 5-18** Selecting device type



3. Under **Alarm List** or **Event List** in the **Add Alarms and Events** dialog box, select an alarm or event.
  - Click **Select All** or **Clear All** to select or clear all the alarm sources under **Alarm List** or **Event List**.
  - Select the alarms or events under multiple device types as required. The alarms or events that you selected will not be displayed in the list.
  - In the **Alarm List** area, set an alarm severity and select the required alarms of the specified alarm severity.
  - In the **Event List** area, select the required events.
4. Click **OK**.
5. Click **Next**.

**Step 6** Select a recipient group.

In the **Recipient Groups** step on the **Create by Alarm** page, set a recipient group and set whether to send a remote notification once an alarm is cleared.

**Figure 5-19** Selecting recipient Groups

Alarm Settings > Remote Notification > Remote Notification Rules > **Create by Alarm** Help 

● ——— ● ——— ●  
Alarm Sources Alarms/Events Recipient Groups

Rule name:

☐ Notify of alarm clearance

\* Notification recipient groups: + Add

 A

Group:

Group1

Group2

Create Recipient Group

Previous Finish Cancel

**Step 7** Click **Finish**.

----End

## 5.3 Setting a Fault Monitoring Rule

The eSight allows you to set fault monitoring rules, such as the alarm mask rule, alarm sound, and user-defined criteria.

### 5.3.1 Creating an Alarm Mask Rule

This topic describes how to create an alarm mask rule. For the alarms that are reported to the eSight and do not require attention, you can create a mask rule to mask them. The masked alarms are not displayed in the current alarm list. This helps you find the desired alarms in the current alarm list.

#### Prerequisites

You have the operation rights for **Alarm Settings**.

#### Context

The values of **Time** can be **Anytime** and **Only during following periods**.

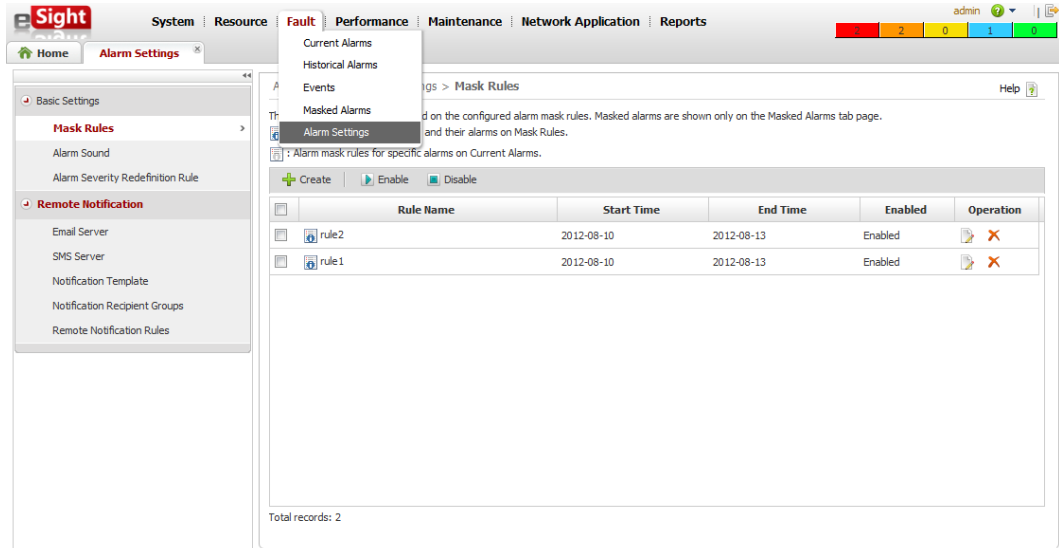
- **Anytime**: indicates that a mask rule is available at any time on the specified **Date**.
- **Only during following periods**: indicates that a mask rule is available within daily periods of time on the specified **Date**. Note that a maximum of five periods of time is allowed in a day.



## Procedure

**Step 1** Choose **Fault > Alarm Settings** from the main menu.

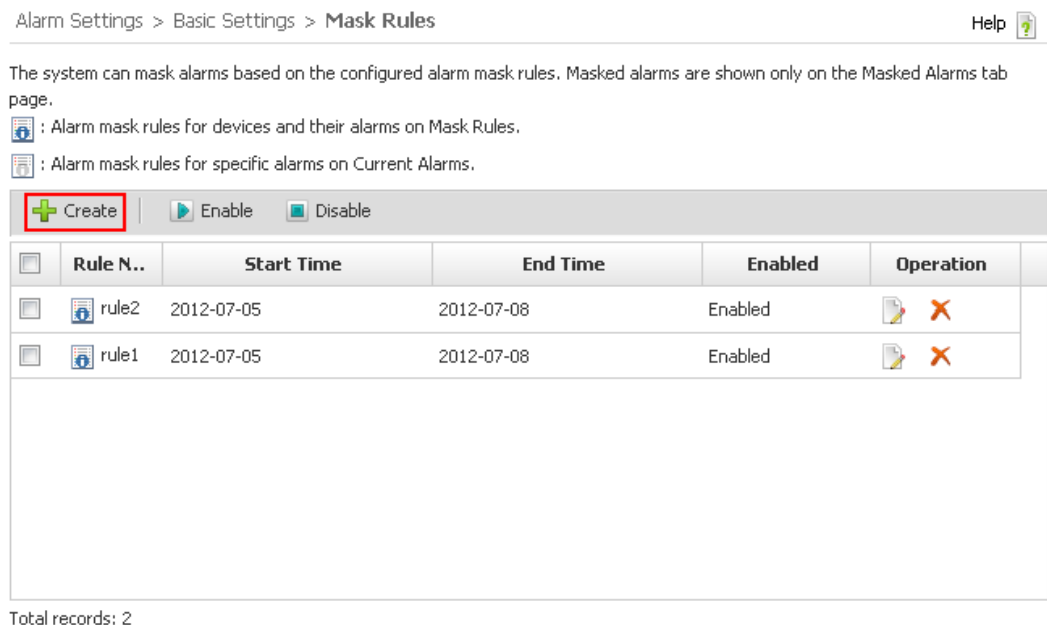
**Figure 5-20** Alarm settings



**Step 2** In the **Alarm Settings** window, choose **Basic Settings > Mask Rules**.

**Step 3** On the **Mask Rules** page, click **Create**.

**Figure 5-21** Creating an alarm mask rule



**Step 4** Set the basic information.

1. Under **Basic Information** step on the **Create an Alarm Mask Rule** page, set **Rule name**, **Date**, and **Time**.

**Figure 5-22** Setting the basic information

Alarm Settings > Basic Settings > Mask Rules > **Create an Alarm Mask Rule**

---

Basic Information      Alarm Sources      Alarms

Rule name:

---

\* Date:   to  

Time: ☒ Anytime    ☐ Only during following periods

2. Click **Next**.

**Step 5** Select an alarm source.

1. Under **Alarm Sources** step on the **Create an Alarm Mask Rule** page, click **Add Alarm Sources**.

**Figure 5-23** Adding alarm sources

Alarm Settings > Basic Settings > Mask Rules > **Create an Alarm Mask Rule** Help ?

Basic Information Alarm Sources Alarms

Rule name: ruleA

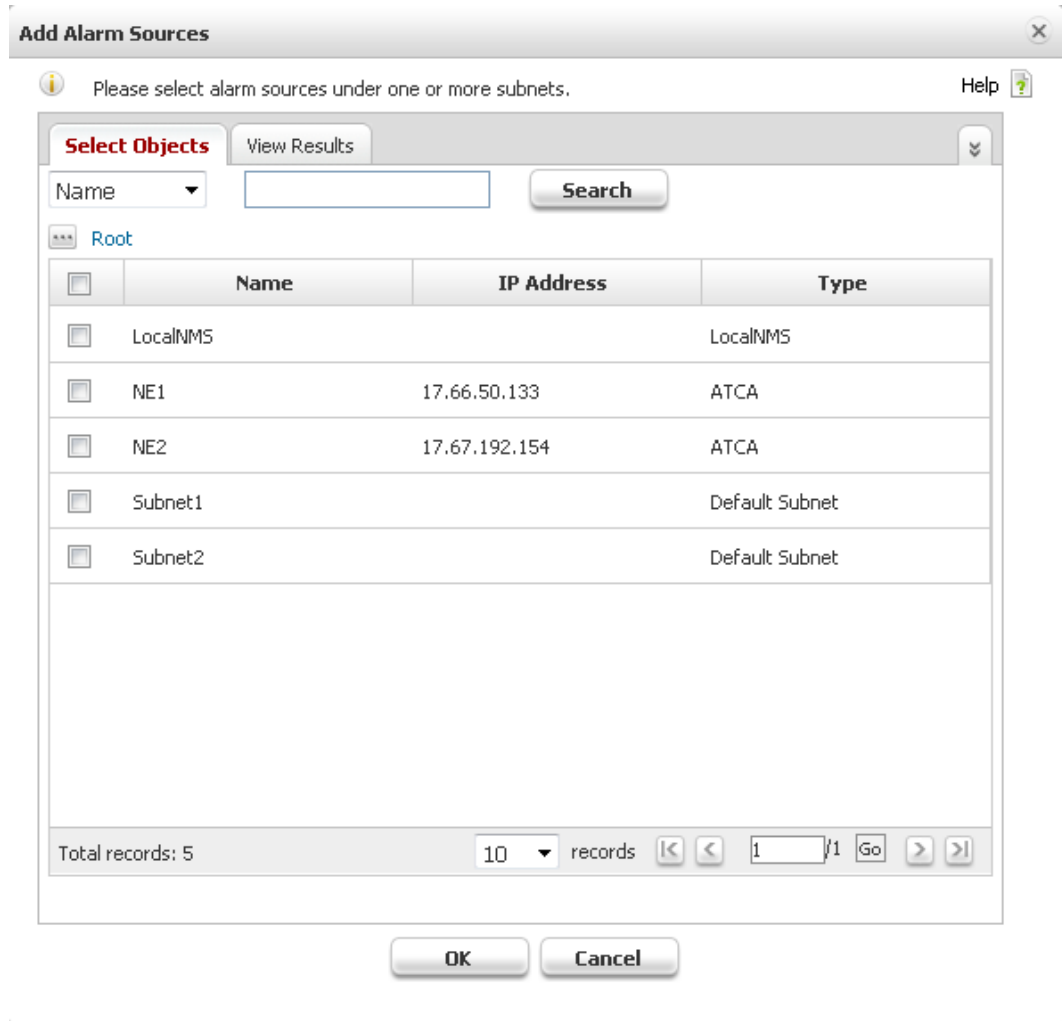
+ Add Alarm Sources - Delete

Previous Next Cancel

2. Under **Select Objects** in the **Add Alarm Sources** dialog box, select alarm sources.

 **TIP**

- Click a subnet name to open the list of devices or subnets.
- Click a node in the navigation tree, for example, **ROOT**. The related page is displayed.
- Set the keyword of **Name**, **IP Address**, or **Type** to search for the NEs or subnets that meet the search criteria.

**Figure 5-24** Selecting objects

3. On the **View Results** tab page, view the selected alarm sources.

 **NOTE**

- On the **View Results** tab page, you can click  in the **Operation** column to deselect the required alarm sources.
- You can click **Clear All** on the **View Results** tab page to clear the alarm sources on the **View Results** tab page.

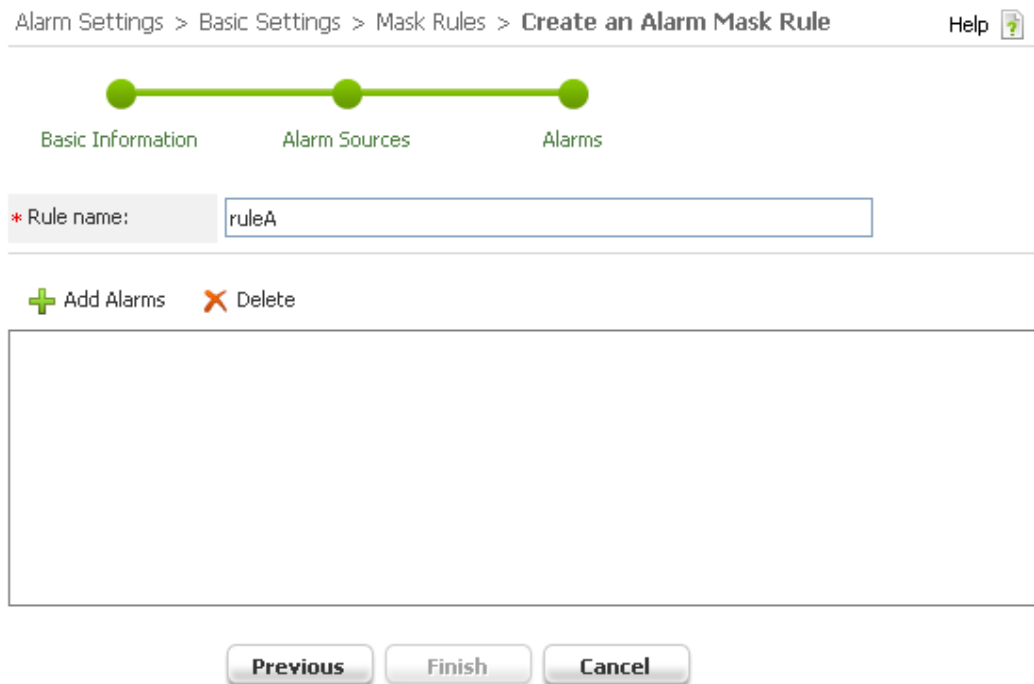
4. Click **OK**.
5. Click **Next**.

**Step 6** Select an alarm.

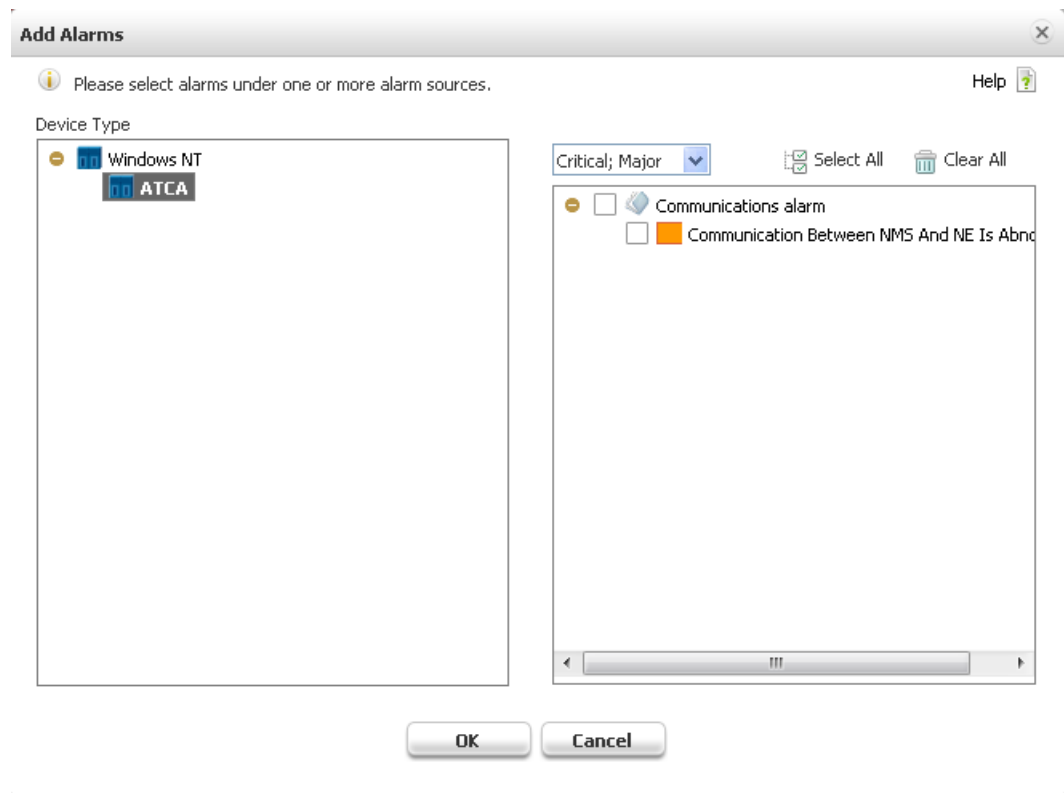
**NOTE**

- If you select a subnet under the **Alarm Sources** step, you can select an alarm under the **Alarms** step for all NEs in the subnet.
- If you select an NE under the **Alarm Sources** step, you can select an alarm under the **Alarms** step for only the selected NE.
- If you select only a resource of an NE under the **Alarm Sources** step, you can select an alarm under the **Alarms** step for the selected resource and the NE. In this case, the selected alarms are shielded.

1. Under **Alarms** step on the **Create an Alarm Mask Rule** page, click **Add Alarms**.

**Figure 5-25** Adding alarms

2. Under **Device Type** in the **Add Alarms** dialog box, select a device type.
  - After you select a device type, the alarms under the device type are displayed on the right pane.
  - A red asterisk (\*) is displayed in the upper right corner of the selected device type, which indicates that you selected the alarms under the device type.

**Figure 5-26** Selecting device type

3. In the **Add Alarms** dialog box, select an alarm.
  - Click **Select All** or **Clear All** to select or clear the selected alarm sources.
  - Select the alarms under multiple subnets as required. The alarms that you selected will not be displayed under these subnets.
  - In the alarm list area, set the alarm severity and select the required alarms.
4. Click **OK**.

**Step 7** Click **Finish**.

An alarm mask rule is enabled by default once it is created.

----End

## Follow-up Procedure

The following table describes the operations that you can perform after you create an alarm mask rule.

| Setting Alarm Masking Rules | Operation Method                                                                                                                                                                                               |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enabling an Alarm Mask Rule | Enable a disabled alarm mask rule.<br>On the <b>Mask Rules</b> page, select one or more mask rules, and click <b>Enable</b> .<br>If the <b>Enabled</b> column for a mask rule is displayed as <b>Enabled</b> , |

| Setting Alarm Masking Rules  | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | the mask rule is enabled, and the subsequently reported alarms will be masked based on the rule.                                                                                                                                                                                                                                                                                                                |
| Disabling an Alarm Mask Rule | Disable an alarm mask rule that is not used currently.<br>On the <b>Mask Rules</b> page, select one or more mask rules, and click <b>Disable</b> .<br>If the <b>Enabled</b> column for a mask rule is displayed as <b>Disabled</b> , the mask rule is disabled.                                                                                                                                                 |
| Deleting an Alarm Mask Rule  | Delete unnecessary mask rules to ensure sufficient memory and proper running of tasks on the server.<br>1. On the <b>Mask Rules</b> page, click  in the <b>Operation</b> column where the required mask rule is located.<br>2. In the <b>Confirm</b> dialog box, click <b>Yes</b> .                                          |
| Modifying an Alarm Mask Rule | Modify an alarm mask rule to meet management requirements.<br>1. On the <b>Mask Rules</b> page, click  in the <b>Operation</b> column where the required mask rule is located.<br>2. On the <b>Modify Alarm Mask Rule</b> page, modify the name and basic information about the mask rule, alarm sources, and masked alarms. |

## 5.3.2 Setting the Alarm Sound

You can specify alarm sounds for different alarm severities. When an alarm is generated, the sound box in the host produces a sound.

### Prerequisites

You have the operation rights for **Alarm Settings**.

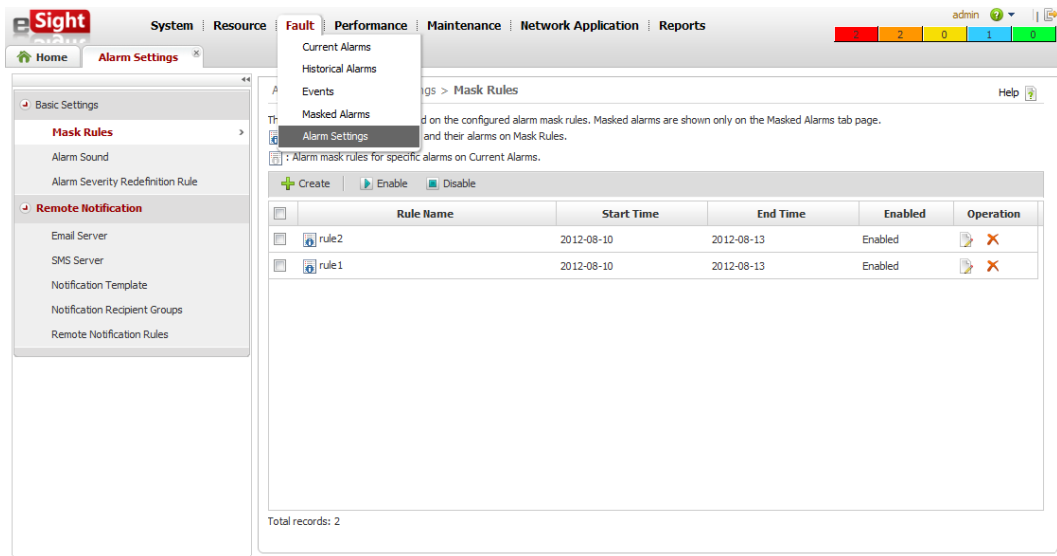
### Context

- By default the alarm sound is **Enable**.
- The default settings for different severities of alarms are:
  - **Critical: Critical.mp3**
  - **Major: Major.mp3**
  - **Minor: Minor.mp3**
  - **Warning: Warning.mp3**

### Procedure

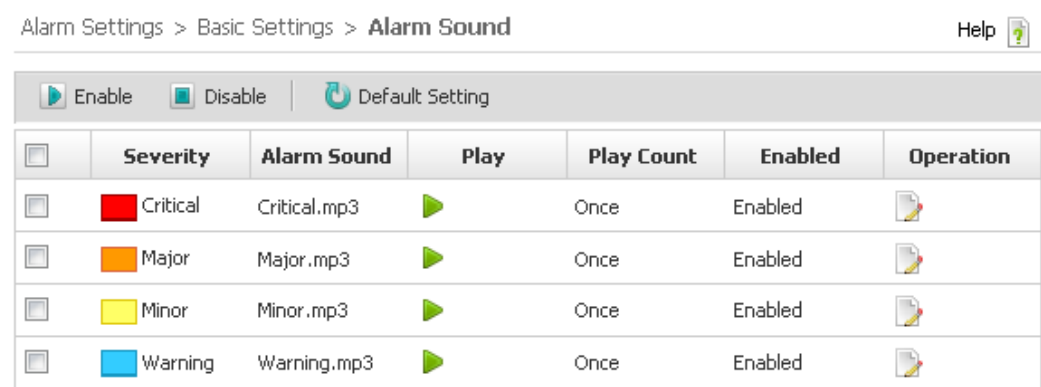
**Step 1** Choose **Fault > Alarm Settings** from the main menu.

Figure 5-27 Alarm settings



**Step 2** In the **Alarm Settings** window, choose **Basic Settings** > **Alarm Sound**.

Figure 5-28 Alarm sound



**Step 3** In the **Alarm Sound** page, you can perform the following operations.



| Setting Alarm Sound          | Operation Method                                                                                                                                                                                                                                    |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable alarm sound          | Select <b>Severity</b> and click <b>Disable</b> to disable the alarm sound for the severity.                                                                                                                                                        |
| Enable alarm sound           | Select <b>Severity</b> and click <b>Enable</b> to enable the alarm sound for the severity.                                                                                                                                                          |
| Play alarm sound             | Click  in the <b>Play</b> column to play the alarm sound.                                                                                                          |
| Change alarm sound           | Click  in the <b>Operation</b> column. On the <b>Set Alarm Sound</b> page, change the values of <b>Alarm sound</b> and <b>Play count</b> , and click <b>Save</b> . |
| Restore the default settings | Click <b>Default Setting</b> to restore the alarm sound to the initial setting.                                                                                                                                                                     |

----End

### 5.3.3 Creating an Alarm Filter Rule

If the default alarm filter rules cannot meet user requirements, you can create an alarm filter as required.

#### Prerequisites

You have the operation rights for **Current Alarms Management**.

#### Context

The default filter criteria rules are:

- All alarms
- Unacknowledged critical alarms
- Unacknowledged major alarms
- Uncleared critical alarms
- Uncleared major alarms
- Alarms generated during the past 24 hours



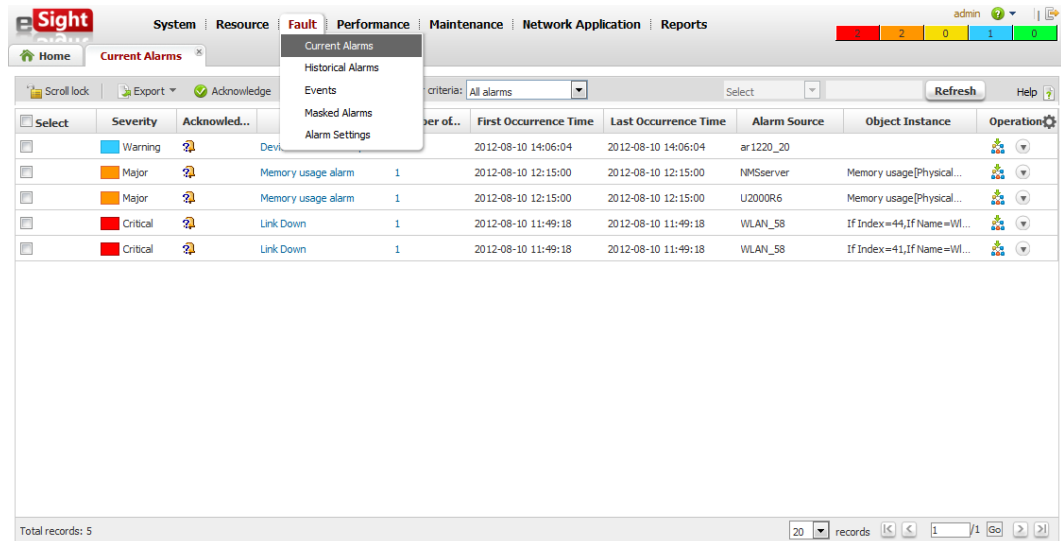
#### NOTE

The default alarm filter criteria rule cannot be deleted or modified.

#### Procedure

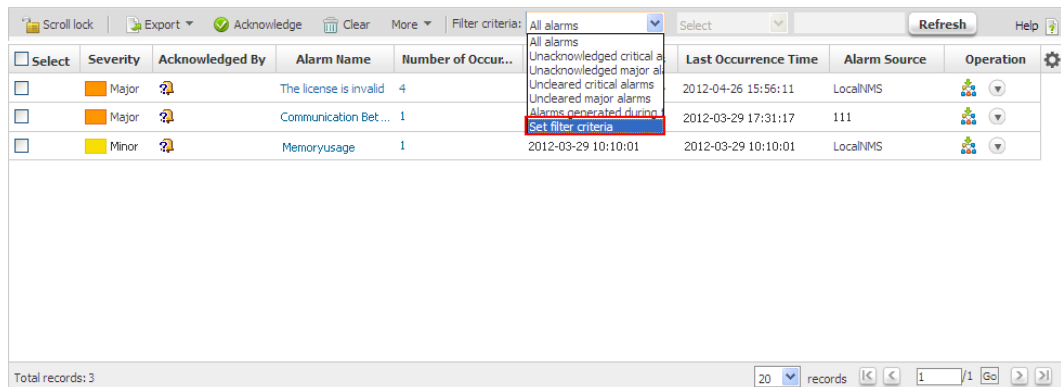
**Step 1** Choose **Fault** > **Current Alarms** from the main menu.

Figure 5-29 Current alarms



**Step 2** In the **Current Alarms** window, select **Set filter criteria** from the **Filter criteria** drop-down list on the toolbar.

Figure 5-30 Customizing the filter rule



**Step 3** In the **Set Filter Criteria** dialog box, you can perform the following operations.

| Setting Customizing Alarm Filter Criteria | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create customizing alarm filter criteria  | <p>When the default filter criteria rule of the eSight cannot meet the current management requirements, you can create user-defined filter criteria rule.</p> <ol style="list-style-type: none"><li>1. Click <b>Create</b>. In the <b>Set Filter Criteria</b> dialog box, set the name, alarm severity, acknowledgement status, clearance status, first occurrence time, NE type, alarm source, and event type.</li><li>2. Click <b>Save</b>.</li></ol>                                                                                                 |
| Delete customizing alarm filter criteria  | <p>Delete unnecessary user-defined filter criteria rule to ensure sufficient memory and proper running of tasks on the server.</p> <ol style="list-style-type: none"><li>1. Click  in the <b>Set Filter Criteria</b> dialog box to select a user-defined filter criteria rule, and click <b>Delete</b>.</li><li>2. In the <b>Confirm</b> dialog box, click <b>Yes</b>.</li></ol>                                                                                       |
| Modify customizing alarm filter criteria  | <p>Modify user-defined filter criteria rule to meet the latest management requirements.</p> <ol style="list-style-type: none"><li>1. Click  in the <b>Set Filter Criteria</b> dialog box to select a user-defined filter criteria rule. In the <b>Set Filter Criteria</b> dialog box, change the name, alarm severity, acknowledgement status, clearance status, first occurrence time, NE type, alarm source, and event type.</li><li>2. Click <b>Save</b>.</li></ol> |
| Copy customizing alarm filter criteria    | <p>Copy a user-defined filter criterion.</p> <ol style="list-style-type: none"><li>1. Click  in the <b>Set Filter Criteria</b> dialog box to select a filter criteria rule and click <b>Copy</b>. In the <b>Set Filter Criteria</b> dialog box, change the name, alarm severity, acknowledgement status, clearance status, first occurrence time, NE type, alarm source, and event type.</li><li>2. Click <b>Save</b>.</li></ol>                                     |

----End

## 5.3.4 Redefining the Severity of an Alarm

Redefining the severity of an alarm helps you to draw more or less attention to the alarm.

### Prerequisites

You have the operation rights for **Current Alarms Management**.

### Context

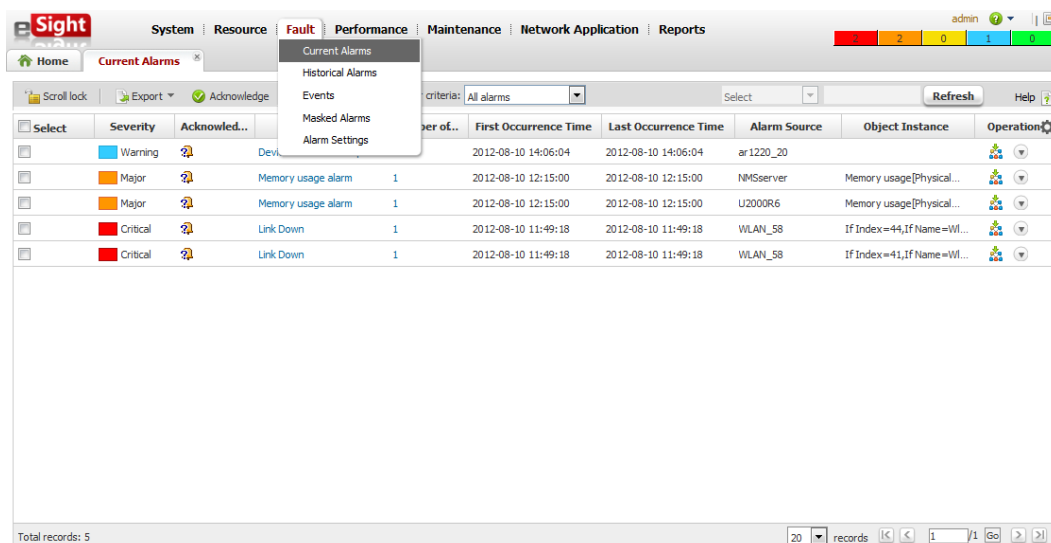
- The new alarm severity is applicable only to the alarms reported after redefinition.
- Only the severities of the alarms configured on the eSight can be redefined.
- When you redefine the severity of an alarm for the first time, the eSight generates an alarm severity redefinition rule on the **Alarm Severity Redefine Rule** page under **Alarm Settings**.

- When you redefine the severity of the alarm again, the eSight refreshes the alarm severity redefinition rule displayed on the **Alarm Severity Redefine Rule** page.
- An alarm severity redefinition rule is applicable only to the alarms with the same alarm name and NE type.
- A maximum of 500 alarm severity redefinition rules can be created.

## Procedure

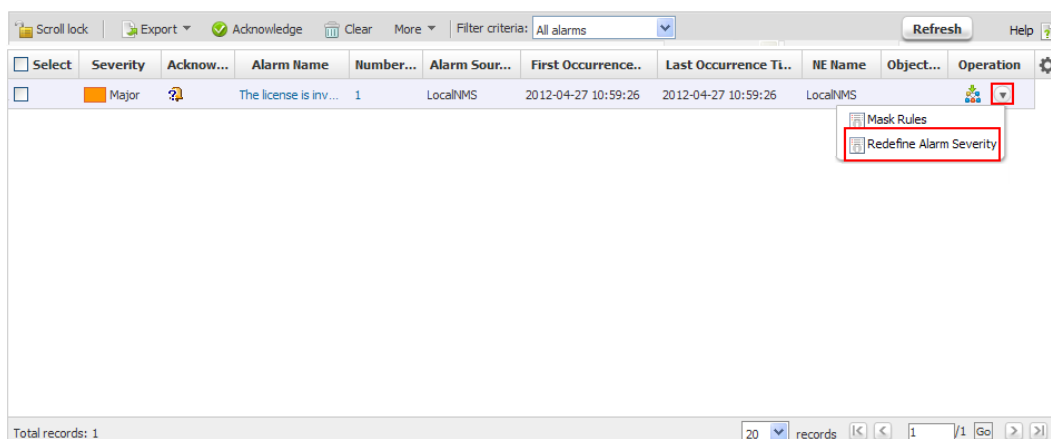
**Step 1** Choose **Fault > Current Alarms** from the main menu.

**Figure 5-31** Current alarms



**Step 2** In the alarm list of the **Current Alarms** window, click  in the **Operation** column of the required alarm, and select **Redefine Alarm Severity**.

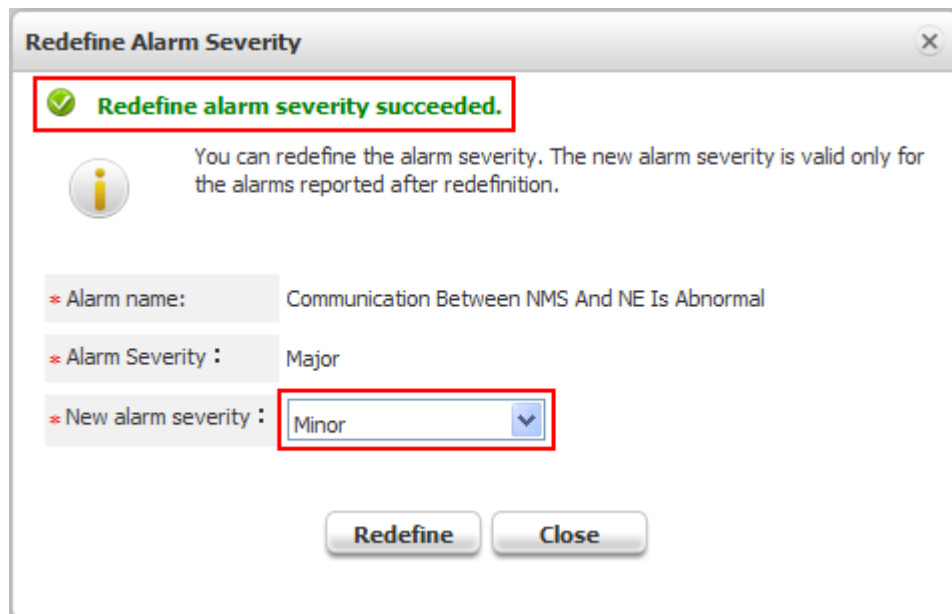
**Figure 5-32** Redefining Alarm Severity



**Step 3** In the **New alarm severity** drop-down list of the **Redefine Alarm Severity** dialog box, select a new severity. Then click **Redefine**.

The eSight displays a message saying that the alarm severity is successfully redefined.

**Figure 5-33** Selecting a new alarm severity



**Step 4** Click **Close**.

----End

## Follow-up Procedure

After you redefine the severity of an alarm, you can view or delete the alarm severity redefinition rule on the **Alarm Severity Redefine Rule** page.



### NOTE

You can view or delete an alarm severity redefinition rule only when you have the operation rights of **Alarm Settings**.

**Table 5-4** Managing an alarm severity redefinition rule

| Managing an Alarm Severity Redefinition Rule | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View an alarm severity redefinition rule     | You can view the information about an alarm severity redefinition rule in the eSight.<br><ol style="list-style-type: none"><li>1. Choose <b>Fault &gt; Alarm Settings</b> from the main menu.</li><li>2. In the <b>Alarm Settings</b> window, choose <b>Basic Settings &gt; Alarm Severity Redefine Rule</b>.</li><li>3. On the <b>Alarm Severity Redefine Rule</b> page, view <b>Alarm Name</b>, <b>Managed Object Type</b>, <b>Alarm Severity</b>, and <b>New Alarm Severity</b> of the alarm severity redefinition rule.</li></ol> |
| Delete an alarm severity redefinition rule   | When you need to restore the severity of an alarm, you can delete the corresponding alarm severity redefinition                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Managing an Alarm Severity Redefinition Rule | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | <p>rule.</p> <ol style="list-style-type: none"><li>1. Choose <b>Fault &gt; Alarm Settings</b> from the main menu.</li><li>2. In the <b>Alarm Settings</b> window, choose <b>Basic Settings &gt; Alarm Severity Redefine Rule</b>.</li><li>3. On the <b>Alarm Severity Redefine Rule</b> page, click  in the <b>Operation</b> column of the required alarm severity redefinition rule.</li><li>4. In the <b>Confirm</b> dialog box, click <b>Yes</b>.</li></ol> |

## 5.4 Monitoring Alarms

The eSight provides physical view, alarm board, and alarm bar chart to help you monitor alarms, learn about alarm status, and take proper measures.

### 5.4.1 Browsing Current Alarms

You can set the filter criteria in the current alarm list to view the alarms to be concerned and handled.

#### Prerequisites

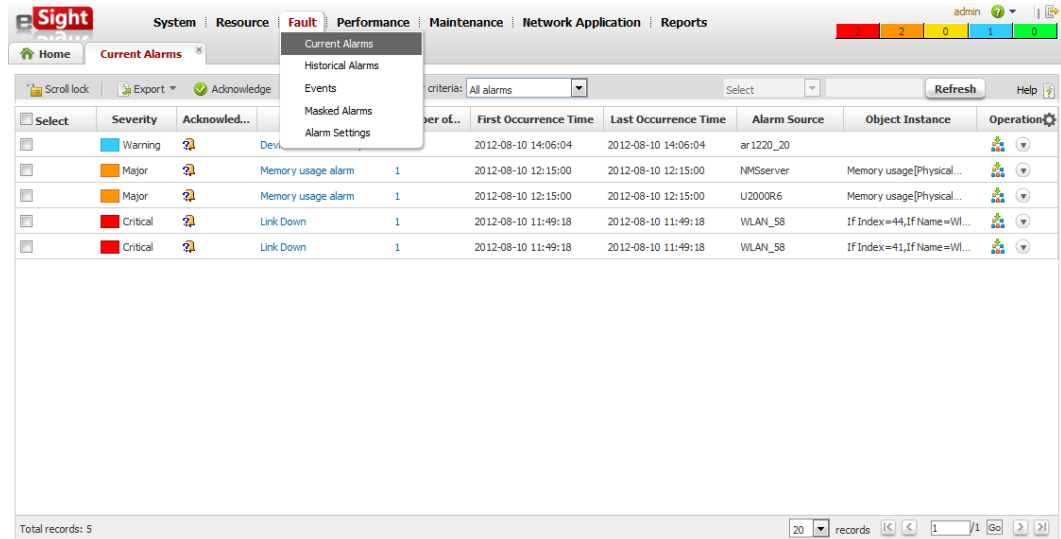
You have the operation rights for **Current Alarms Management**.

#### Context

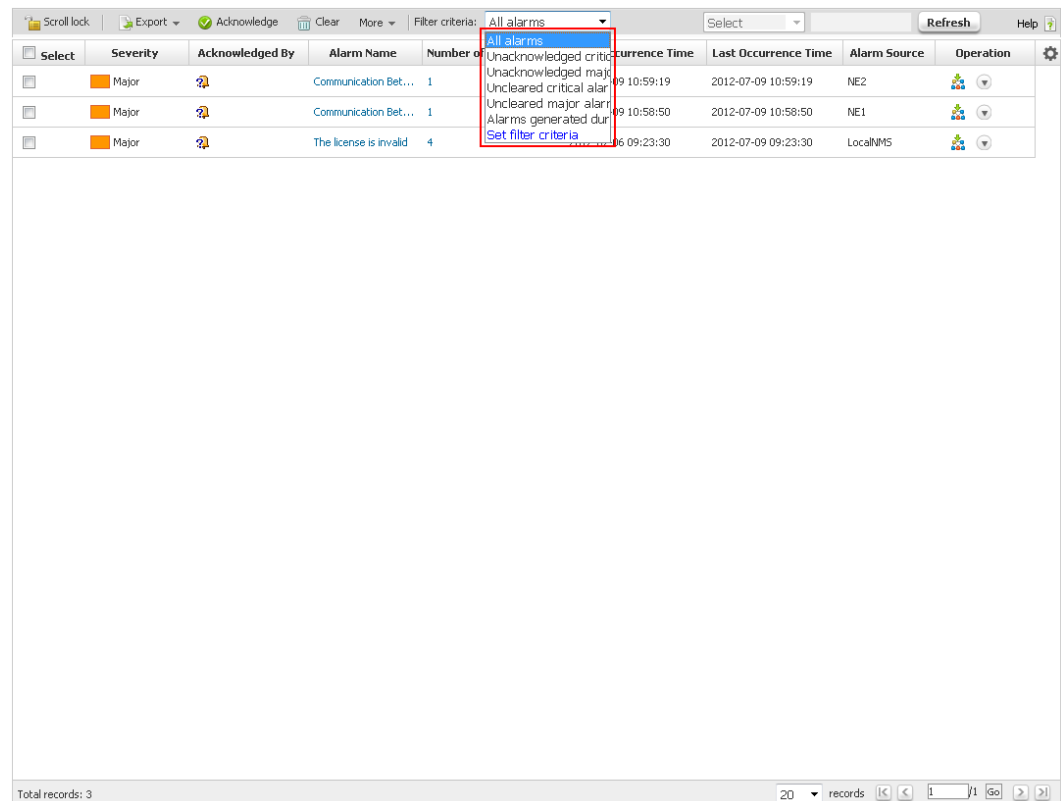
- The current alarm list represents the merged alarms. For example, if a new alarm is reported and meets the merging rule, the information about the alarm will overwrite the previous alarm information, and the number of alarms is increased by one. If a new alarm is reported and does not meet the merging rule, it is displayed as a new record in the current alarm list.  
Alarm merging rule: If alarms have the same alarm source, location information, and alarm ID, the alarms are reported as only one record.
- The system always searches for alarms based on the filter criteria rule you select.

#### Procedure

**Step 1** Choose **Fault > Current Alarms** from the main menu.

**Figure 5-34** Current alarms

**Step 2** In the **Current Alarms** window, select filter criteria rule from the **Filter criteria** drop-down list and perform a search. You can customize filter criteria rule if required. For details, see [5.3.3 Creating an Alarm Filter Rule](#).

**Figure 5-35** Customizing the filter rule

**Step 3** In the **Current Alarms** window, you can perform the following steps:

| Management Alarms | Operation Method                                                                                                                                                                                                                                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lock alarms       | <p>Click <b>Scroll lock</b>. The alarms in the current list are locked.</p> <p>In addition, <b>Scroll lock</b> is automatically changed to <b>Scroll unlock</b>.</p>                                                                                                                                                                                                                                   | <p>If the alarms in the current list are locked, note that:</p> <ul style="list-style-type: none"><li>Newly reported alarms can be displayed in the current alarm list only after you click <b>Scroll unlock</b>.</li><li>When an alarm is available, you can perform operations such as acknowledging or clearing the alarm, or viewing details about the alarm. When an alarm is unavailable, you cannot perform any operations on the alarm.</li></ul> <p><b>NOTE</b></p> <p>If you can select the check box next to an alarm, the alarm is available. If the check box is dimmed, the alarm is unavailable.</p> <ul style="list-style-type: none"><li>If you acknowledge or clear an alarm when you click <b>Scroll lock</b>, the alarm can be updated to the historical alarm list only when you click <b>Scroll unlock</b>.</li></ul> |
| Unlock alarms     | <p>Click <b>Scroll unlock</b>. The eSight reports alarms to the alarm list automatically.</p> <p>In addition, <b>Scroll unlock</b> is automatically changed to <b>Scroll lock</b>.</p>                                                                                                                                                                                                                 | <p>When the current alarm list is in the unlocked status, you cannot select filter rule for search. You can perform a search only after the current alarm list becomes locked.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Search alarm      | <p>You can perform a search by using either of the following methods:</p> <ul style="list-style-type: none"><li>Click <b>Search</b> without setting any search criteria. All alarms are displayed in the current list.</li><li>When the current alarm list is in the locked state, select a search scope from the drop-down list and enter a value in the text box, and click <b>Search</b>.</li></ul> | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Acknowledge       | <p>Select one or more alarms and click <b>Acknowledge</b>.</p>                                                                                                                                                                                                                                                                                                                                         | <ul style="list-style-type: none"><li>If the alarm is acknowledged, <b>Acknowledged By</b> displays the user who acknowledges the alarm.</li><li>If the alarm is unacknowledged,</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



| Management Alarms                                       | Operation Method                                                                                                                                                                                                                                                                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                         |                                                                                                                                                                                                                                                                                                                                               | <b>Acknowledged By</b> displays  .                                                                                                                                                                                                                                                                                   |
| Unacknowledge                                           | Select one or more alarms and choose <b>More &gt; Unacknowledge</b> .                                                                                                                                                                                                                                                                         | After an alarm is unacknowledged, its status is changed from <b>Acknowledged</b> to <b>Unacknowledged</b> .                                                                                                                                                                                                                                                                                             |
| Clear                                                   | Select one or more uncleared alarms and click <b>Clear</b> .                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"><li>The background color of clear alarms is green.</li><li>The background color of uncleared alarms is white.</li></ul>                                                                                                                                                                                                                                               |
| Mask Alarm                                              | <ol style="list-style-type: none"><li>Click  in the <b>Operation</b> column where the required alarm is located, and select <b>Mask Rules</b>.</li><li>In the <b>Mask Rules</b> dialog box, set the rule name and shielding date. Click <b>OK</b>.</li></ol> | <ul style="list-style-type: none"><li>The newly created alarm mask rule is in enabled status by default.</li><li>A mask rule is valid only to the alarms reported when the masking rule is enabled and valid. The masking rule does not take effect for the alarms reported before the masking rule is configured.</li><li>You cannot set a mask rule for a performance alarm or clear alarm.</li></ul> |
| Customize the columns to be displayed in the alarm list | Click  . On the displayed page, set the columns to be displayed in the alarm list, and click <b>OK</b> .                                                                                                                                                   | -                                                                                                                                                                                                                                                                                                                                                                                                       |
| Locate to Topo                                          | Click  in the <b>Operation</b> column where the required alarm record is located.                                                                                                                                                                          | eSight locates the NE in the managed object that generates the alarm in the physical view.                                                                                                                                                                                                                                                                                                              |
| Redefine the severity of an alarm                       | For details, see <a href="#">5.3.4 Redefining the Severity of an Alarm</a> .                                                                                                                                                                                                                                                                  | After you redefine the severity of an alarm, the new alarm severity is valid only for newly reported alarms.                                                                                                                                                                                                                                                                                            |
| Alarm Details                                           | Click <b>Alarm Name</b> of which you want to view details.                                                                                                                                                                                                                                                                                    | The <b>Alarm Details</b> dialog box displays the name, probable cause, and proposed repair actions for the selected alarm.                                                                                                                                                                                                                                                                              |
| Alarm Logs                                              | Click <b>Number of Occurrences</b> about which you want to view the log information.                                                                                                                                                                                                                                                          | The <b>Alarm Logs</b> dialog box displays the alarm log related to this alarm record.                                                                                                                                                                                                                                                                                                                   |
| Export                                                  | Select one or more alarms and choose <b>Export &gt; Selected</b>                                                                                                                                                                                                                                                                              | -                                                                                                                                                                                                                                                                                                                                                                                                       |

| Management Alarms | Operation Method                                                                                                             | Description |
|-------------------|------------------------------------------------------------------------------------------------------------------------------|-------------|
|                   | <b>Records</b> to export the alarm information.<br><br>If you want to export all alarms, choose <b>Export</b> > <b>All</b> . |             |

----End

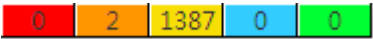
## 5.4.2 Monitoring Alarms on the Alarm Panel

You can view the alarm panel to learn about the number of different severities of alarms or learn about the alarm status from the alarm panel or alarm sound.

### Prerequisites

You have the operation rights for **Current Alarms Management**.

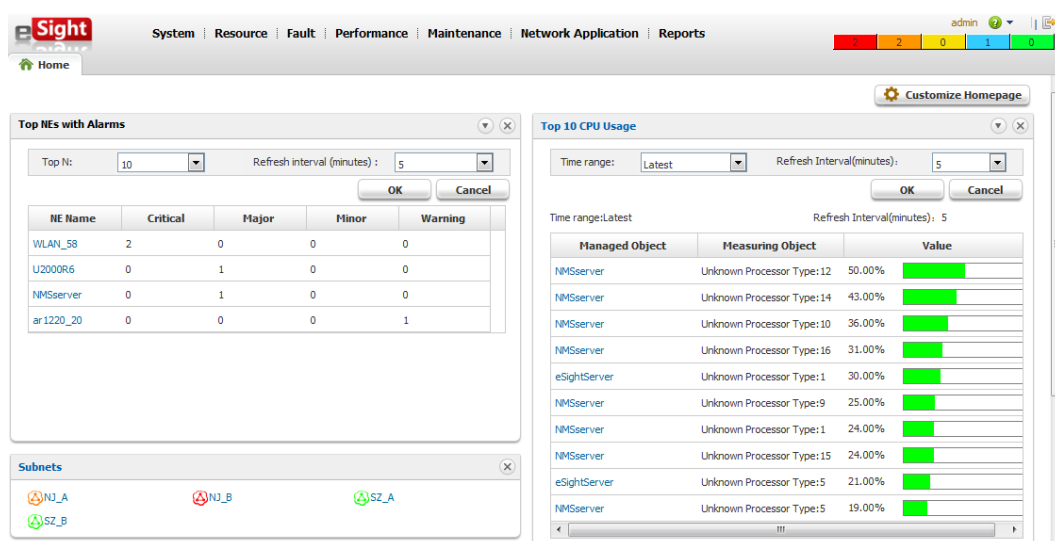
### Context

The alarm panel  is displayed at the upper right corner, and displays the critical alarms, major alarms, minor alarms, warning alarms, and clear alarms from left to right.

### Procedure

- Step 1** On the alarm panel at the upper right corner, view the critical alarms, major alarms, minor alarms, warning alarms, and clear alarms.

Figure 5-36 Alarm panel



----End

### 5.4.3 Monitoring Alarms in the Physical View

The physical view allows you to monitor the alarms of NEs real time.

#### Prerequisites

You have the operation rights for **Current Alarms Management**.

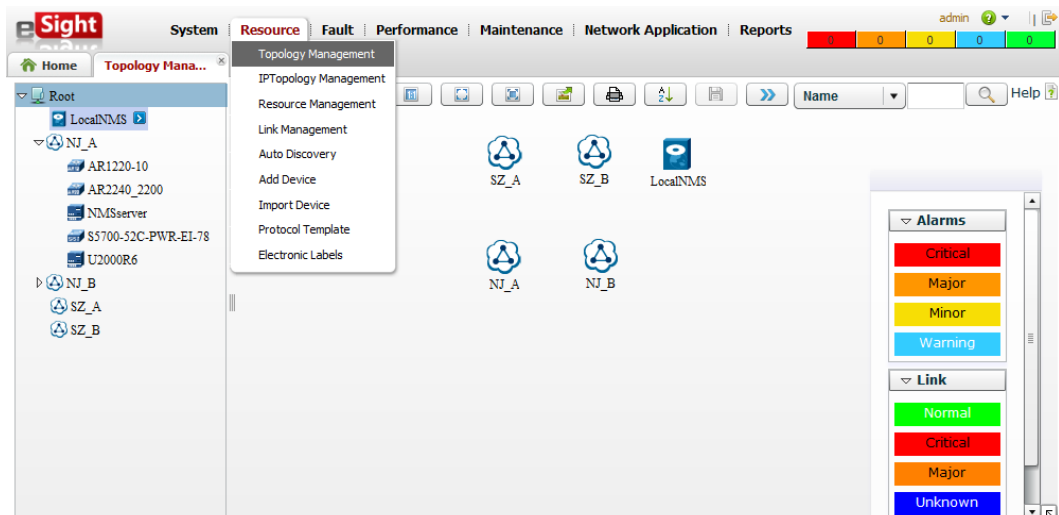
#### Context

In the physical view, the NE icon is displayed in the color of the corresponding alarm severity. If an NE generates multiple alarms at the same time, the NE icon is displayed in the color of the highest severity among the generated alarms.

#### Procedure

**Step 1** Choose **Resource > Topology Management** from the main menu.

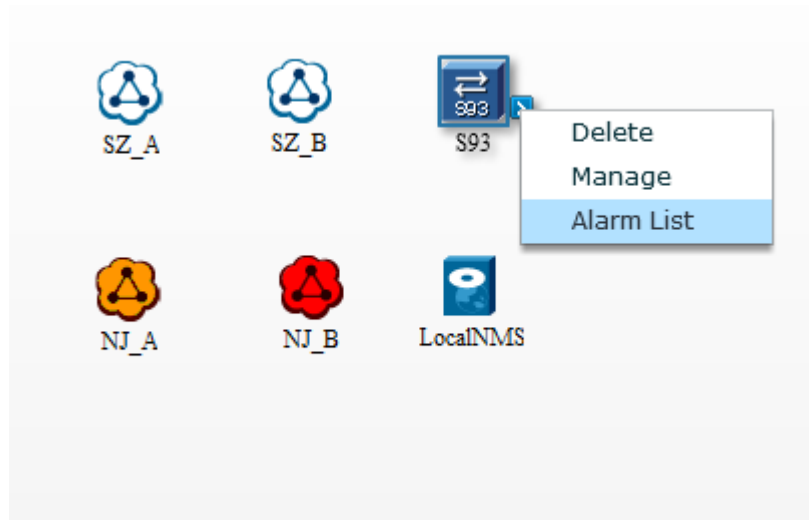
**Figure 5-37** Topology Management



**Step 2** In the **Topology Management** window, view the alarm state and NE position based on the displayed tip.

- The tip includes the highest severity of an NE and number of alarms of the highest severity generated by the NE.
- The tip also includes the NE position information that helps you understand the relationship between the current NE and other NEs and handle the alarms in a timely manner.

**Step 3** In the **Topology Management** window, select an icon of the NE which has generated an alarm. Click  and choose **Alarm List** from the shortcut menu.

**Figure 5-38** Selecting the Alarm List

**Step 4** In the NE management window, view the active alarms of the NE.

----End

## 5.4.4 Monitoring Alarms by Using the NE Management Window

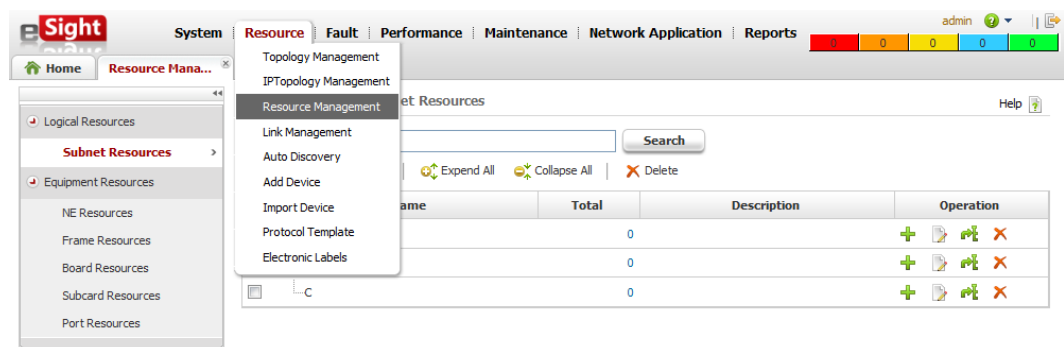
This topic describes how to view the alarm information about the NEs managed by the eSight under resource management. The alarm information reflects the running status of an NE, which helps discover and resolve the fault as soon as possible.

### Prerequisites

- You have the operation rights for **Current Alarms Management**.
- NEs whose alarms are monitored can be managed by the resource manager, and their alarms can also be managed.

### Procedure

**Step 1** Choose **Resource > Resource Management** from the main menu.

**Figure 5-39** Resource management

**Step 2** Choose **Equipment Resources > NE Resources** from the navigation tree on the left, Click the NE name.

**Figure 5-40** NE resources

|                   | Name              | IP Address    | Type                | Version            | Manufacturer | Timezone            | Comments | Operation |                   |
|-------------------|-------------------|---------------|---------------------|--------------------|--------------|---------------------|----------|-----------|-------------------|
|                   | AR1220-10         | 10.137.59.10  | AR1220              | VRP5.90 V200R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
|                   | AR2240_2200       | 10.137.59.220 | AR2240              | VRP5.11 V200R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
|                   | NMSserver         | 10.137.59.43  | MicrosoftWindows... | --                 | Microsoft    | UTC+08:00 Beijin... |          |           |                   |
|                   | S5700-S2C-PWR-EI- | 10.137.59.78  | S5700-S2C-PWR-EI    | VRP5.70 V100R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
|                   | S93               | 10.137.61.37  | S9312               | VRP5.11 V200R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
|                   | U2000R6           | 10.137.59.30  | MicrosoftWindows... | --                 | Microsoft    | UTC+08:00 Beijin... |          |           |                   |
|                   | U2000V1R2C01      | 10.137.59.33  | MicrosoftWindows... | --                 | Microsoft    | UTC+08:00 Beijin... |          |           |                   |
|                   | VASP_204          | 10.137.59.204 | SPU                 | VRP5.70 V200R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
|                   | WLAN_58           | 10.137.59.58  | SPU                 | VRP5.70 V200R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
|                   | ar1220_20         | 10.137.59.208 | AR1220VW            | VRP5.11 V200R00... | Huawei       | UTC+08:00 Beijin... |          |           |                   |
| Total records: 16 |                   |               |                     |                    |              |                     |          |           | 10 records 1/2 Go |

**Step 3** In the NE management window, view the active alarms of the NE.

----End

## 5.4.5 Handling Alarms

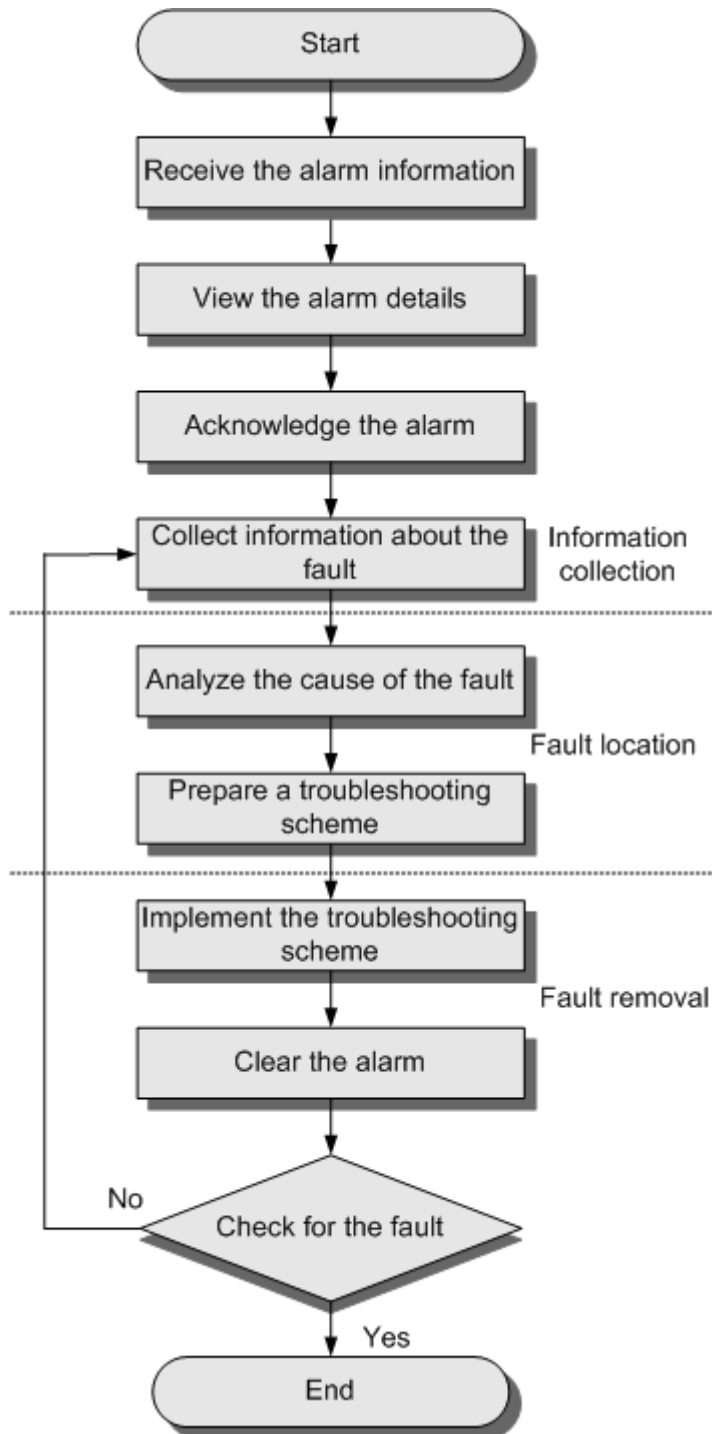
When an alarm occurs, you can handle the alarm to troubleshoot the fault. Handling alarms involves viewing alarm details, acknowledging alarms, and clearing alarms.

### 5.4.5.1 Procedure for Handling Alarms

This topic describes the procedure for handling alarms in the eSight.

## Flow Chart of Handling Alarms

Figure 5-41 Procedure for handling alarms



## Procedure Description

**Table 5-5** Description of procedure for handling alarms

| Step | Operation                            | Description                                                                                                                                                                                                                                                                                                             |
|------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Receive the alarm information        | Receive the alarm information and start handling the alarm. Set the alarm notification mode in the eSight to ensure that the related operators can receive the notification in time.<br><br>For details about how to configure an alarm notification mode, see <a href="#">5.2 Setting Remote Alarm Notifications</a> . |
| 2    | View the alarm details               | View the alarm details, including the location, cause, and solution for the alarm.                                                                                                                                                                                                                                      |
| 3    | Acknowledge the alarm                | Acknowledge the alarm to show that the alarm is being tracked to avoid duplicate handling.                                                                                                                                                                                                                              |
| 4    | Collect information about the fault  | Collect fault information by identifying and querying the alarm.                                                                                                                                                                                                                                                        |
| 5    | Analyze the cause of the fault       | Analyze the cause of the fault based on the symptom.                                                                                                                                                                                                                                                                    |
| 6    | Prepare a troubleshooting scheme     | Prepare a troubleshooting scheme based on the alarm details, running status of the NE and network, and suggested solution.                                                                                                                                                                                              |
| 7    | Implement the troubleshooting scheme | Troubleshoot the fault according to the scheme.                                                                                                                                                                                                                                                                         |
| 8    | Clear the alarm                      | Remove the condition of generating the alarm. If the condition of generating the alarm is removed, a clear alarm is reported to the eSight.                                                                                                                                                                             |
| 9    | Check for the fault                  | After troubleshooting, check if the fault is rectified.                                                                                                                                                                                                                                                                 |

### 5.4.5.2 Viewing the Details about an Alarm

You can view the details about current alarms, historical alarms, and masked alarms in the eSight. Alarm details include the alarm name, advice, and location information.

#### Parameters in the Alarm Details dialog box items

The **Alarm Details** dialog box displays the name, additional information, and solution for the selected alarm.

**Table 5-6** Parameters in the Alarm Details dialog box

| Parameter  | Description                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------|
| Alarm name | Indicates the name of an alarm. You can quickly find the alarm information by alarm name. For example, if a license file |

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | expires, you can learn the cause for generating the alarm based on the alarm name.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Object instance               | Indicates the location information. The location information helps quickly find the cause for generating the alarm and analyze how to clear the alarm.                                                                                                                                                                                                                                                                                                                                                                            |
| Severity                      | Indicates the severity of an alarm. The severity of an alarm can be critical, major, minor, or warning.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Proposed repair actions       | Allows you to view the suggestion for clearing an alarm and helps you quickly locate and rectify the fault.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Number of occurrences         | Indicates the number of occurrences of an alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Last occurrence time          | Indicates the time on which the latest alarm is generated on the managed object.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| First occurrence time         | Indicates the time on which the first alarm is generated on the managed object.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cleared time                  | Indicates the time on which a clear alarm is generated on the managed object.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Cleared                       | Indicates the clear status of an alarm, for example, <b>Uncleared</b> or <b>Cleared</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cleared by                    | Indicates the user who manually clears an alarm, for example, user <b>admin</b> . If the alarm is automatically cleared, the parameter is empty.                                                                                                                                                                                                                                                                                                                                                                                  |
| Acknowledge status            | Indicates the acknowledgment status of an alarm, for example, <b>Unacknowledged</b> or <b>Acknowledged</b> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Acknowledged time             | Indicates the time on which the acknowledgment status of an alarm changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Alarm serial number           | Indicates the serial number of an alarm. The serial number identifies an alarm record in the eSight.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Equipment alarm serial number | Indicates the serial number of a device. The serial number identifies an alarm of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Clear method                  | <p>Indicates the method of clearing an alarm. This parameter can be set to <b>ADAC</b> or <b>ADMC</b>.</p> <ul style="list-style-type: none"><li>• <b>ADAC</b><br/>ADAC indicates an ADAC fault. After an ADAC fault is rectified, the system automatically detects the rectification and reports a clear alarm.</li><li>• <b>ADMC</b><br/>ADMC indicates an ADCM fault. After an ADCM fault is rectified, the system cannot detect the rectification and report the clear alarm. You need to clear the alarm manually.</li></ul> |
| Clear type                    | Indicates the clear type of an alarm, such as <b>Normal clearing</b> , <b>Manual clearing</b> , <b>Configuration clearing</b> , and <b>Correlated</b>                                                                                                                                                                                                                                                                                                                                                                             |



| Parameter              | Description                                                                                                                                                                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <b>clearing.</b>                                                                                                                                                                                                                                         |
| Alarm ID               | Indicates the ID of an alarm. The ID is the primary keyword of the static information table of alarms and uniquely identifies an alarm.                                                                                                                  |
| Alarm source           | Indicates the NE where an alarm is generated.                                                                                                                                                                                                            |
| NE type                | Indicates the type of an NE. Each NE has a unique type.                                                                                                                                                                                                  |
| Event type             | Indicates the type of an event.                                                                                                                                                                                                                          |
| Probable cause         | Indicates the possible causes that an alarm is generated.                                                                                                                                                                                                |
| Additional information | Indicates additional parameters of an alarm, such as the dynamic information and extensibility of the alarm information.                                                                                                                                 |
| Additional text        | Indicates a text that provides additional alarm information and extensibility of alarm information.                                                                                                                                                      |
| Threshold information  | Indicates the threshold information about an alarm that the threshold is exceeded.<br><b>NOTE</b><br>A performance alarm and a SLA alarm provides its threshold information.                                                                             |
| Notification ID        | Indicates the notification ID of an alarm. The notification ID is included in the reported alarm information, including alarm generation, alarm clearance, acknowledgment status change, and alarm severity change. The alarm notification ID is unique. |

### 5.4.5.3 Acknowledging an Alarm

This topic describes how to acknowledge an alarm. Acknowledging an alarm is to indicate that the alarm has been handled and can be ignored.

#### Prerequisites

You have the operation rights for **Current Alarms Management**.

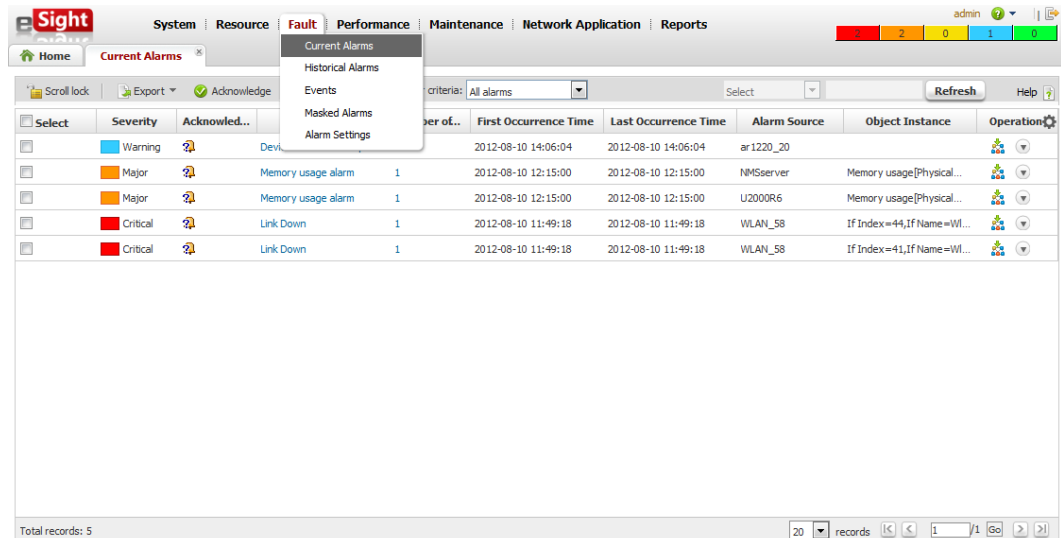
#### Context

- If the alarm is acknowledged, **Acknowledged By** displays the users who acknowledged the alarm.
- If the alarm is unacknowledged, **Acknowledged By** displays .

#### Procedure

**Step 1** Choose **Fault > Current Alarms** from the main menu.

Figure 5-42 Current alarms

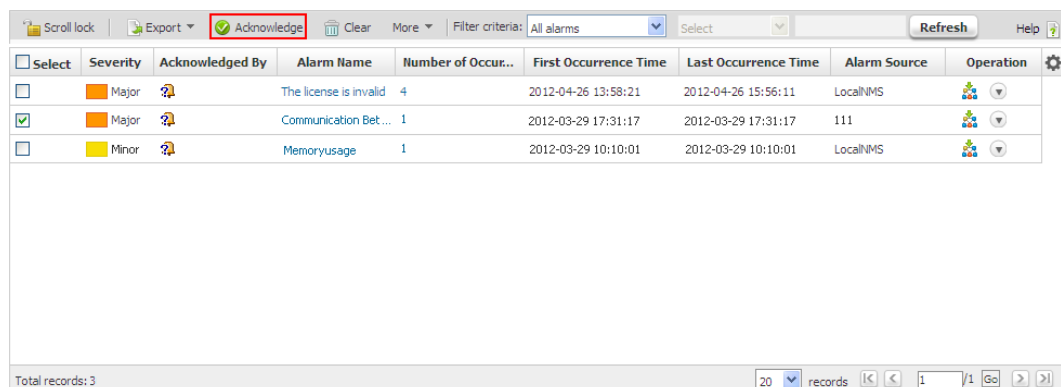


**Step 2** In the **Current Alarms** window, select filter criteria. You can also customize the filter criteria. For details, see [5.3.3 Creating an Alarm Filter Rule](#).

**Step 3** In the search results window, select one or more alarms and click **Acknowledge**.

**Acknowledged By** displays the users who acknowledges the alarms.

Figure 5-43 Acknowledging alarms



----End

## Follow-up Procedure

If you want to acknowledge the alarm again, choose **More > Unacknowledge**.

### 5.4.5.4 Clearing an Alarm

If an alarm cannot be cleared automatically or does not exist on an NE, you need to manually clear the alarm. If the alarm is cleared, the fault is rectified.

## Prerequisites

You have the operation rights for **Current Alarms Management**.

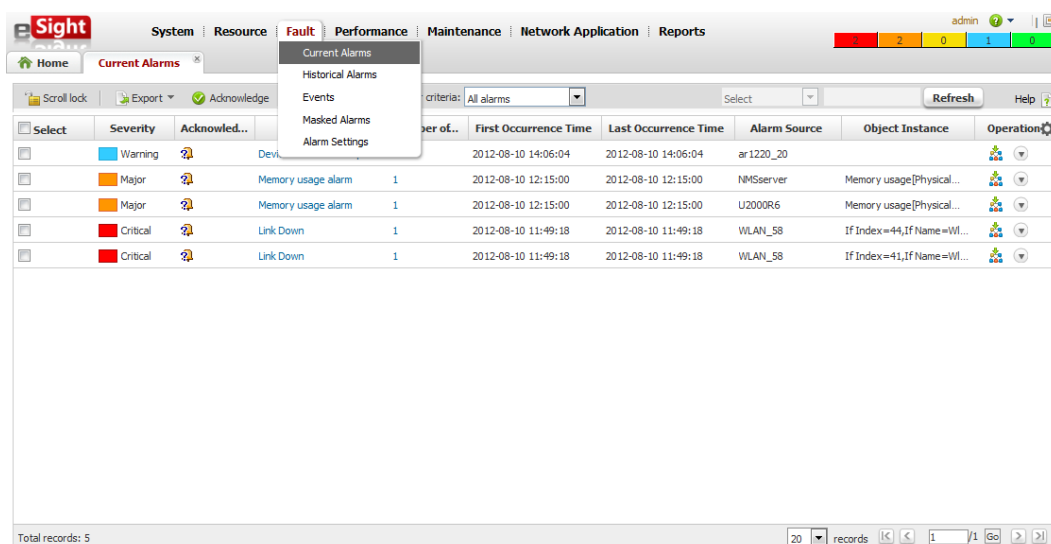
## Context

- After you manually clear an alarm, the clear alarm command is sent by the eSight to the NE, and the NE clears the alarm.
- The clear alarm is mapping to the alarm. When a fault occurs, an alarm is generated. When the fault is rectified, a clear alarm is generated and the alarm is cleared.
- Alarms and clear alarms are identified based on their colors.
  - The background color of clear alarms is green.
  - The background color of uncleared alarms is white.

## Procedure

**Step 1** Choose **Fault > Current Alarms** from the main menu.

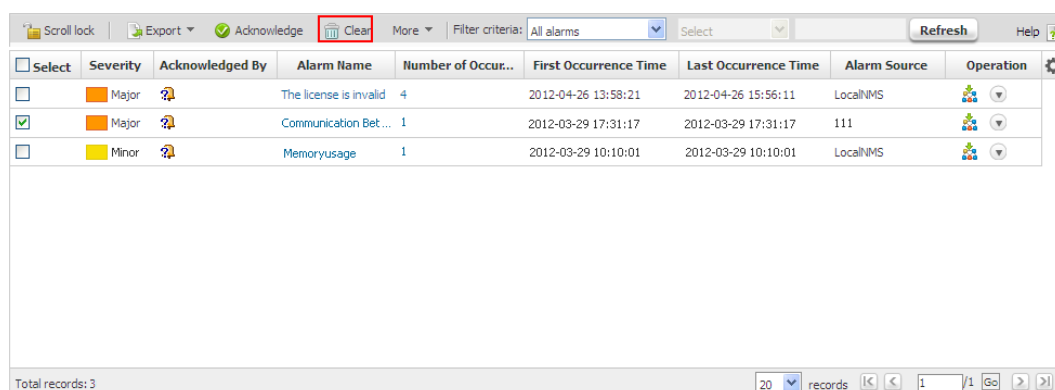
**Figure 5-44** Current alarms



**Step 2** In the **Current Alarms** window, select filter criteria. You can also customize the filter criteria. For details, see [5.3.3 Creating an Alarm Filter Rule](#).

**Step 3** In the **Current Alarms** window, select one or more alarms and click **Clear**.

The cleared alarms are displayed in green.

**Figure 5-45** Clearing alarms

| Select                              | Severity | Acknowledged By | Alarm Name             | Number of Occur... | First Occurrence Time | Last Occurrence Time | Alarm Source | Operation |
|-------------------------------------|----------|-----------------|------------------------|--------------------|-----------------------|----------------------|--------------|-----------|
| <input type="checkbox"/>            | Major    |                 | The license is invalid | 4                  | 2012-04-26 13:58:21   | 2012-04-26 15:56:11  | LocalNMS     |           |
| <input checked="" type="checkbox"/> | Major    |                 | Communication Bet...   | 1                  | 2012-03-29 17:31:17   | 2012-03-29 17:31:17  | 111          |           |
| <input type="checkbox"/>            | Minor    |                 | Memory usage           | 1                  | 2012-03-29 10:10:01   | 2012-03-29 10:10:01  | LocalNMS     |           |

Total records: 3

----End

## 5.5 Alarm Analysis

By querying and analyzing historical alarms and events and masked alarms, you can learn about the alarm trend of an NE to determine whether to upgrade the NE.

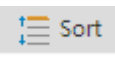
### 5.5.1 Querying a Historical Alarm

You can quickly find the desired historical alarms based on specified search criteria.

#### Prerequisites

You have the operation rights for **Browse Historical Alarms**.

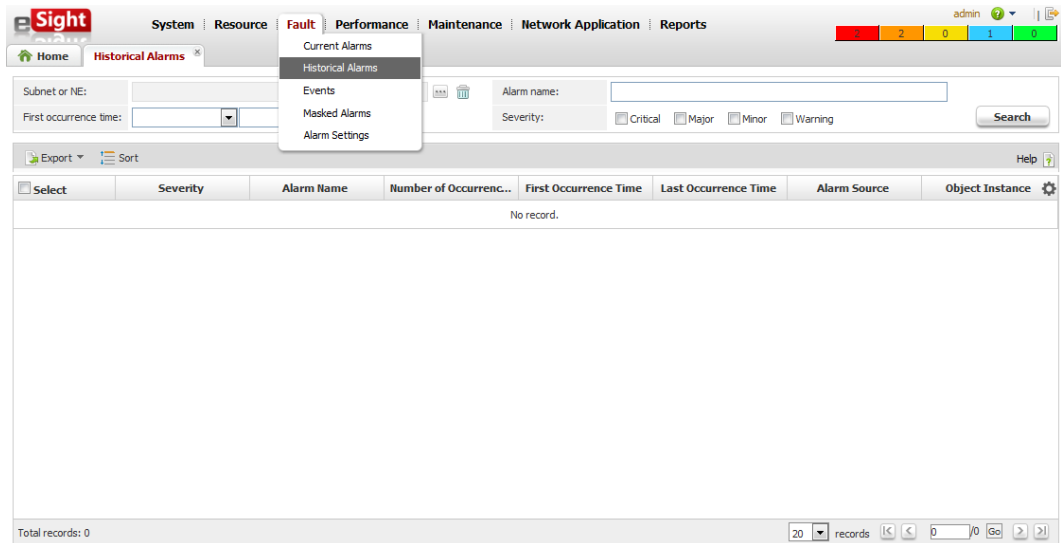
#### Context

- The alarms that are acknowledged and cleared are displayed in the historical alarm list.
- The query result is generated based on the existing data in the database. If the database is empty, there is no matching query result.
- When you query historical alarms, you can perform the following settings:
  - Click  to customize the information you want to query.
  - Click  to sort alarms in the **Sort** dialog box.

#### Procedure

**Step 1** Choose **Fault > Historical Alarms** from the main menu.

Figure 5-46 Historical alarms



**Step 2 Optional:** In the **Historical Alarms** window, set the search information in the search bar and click **Search**.

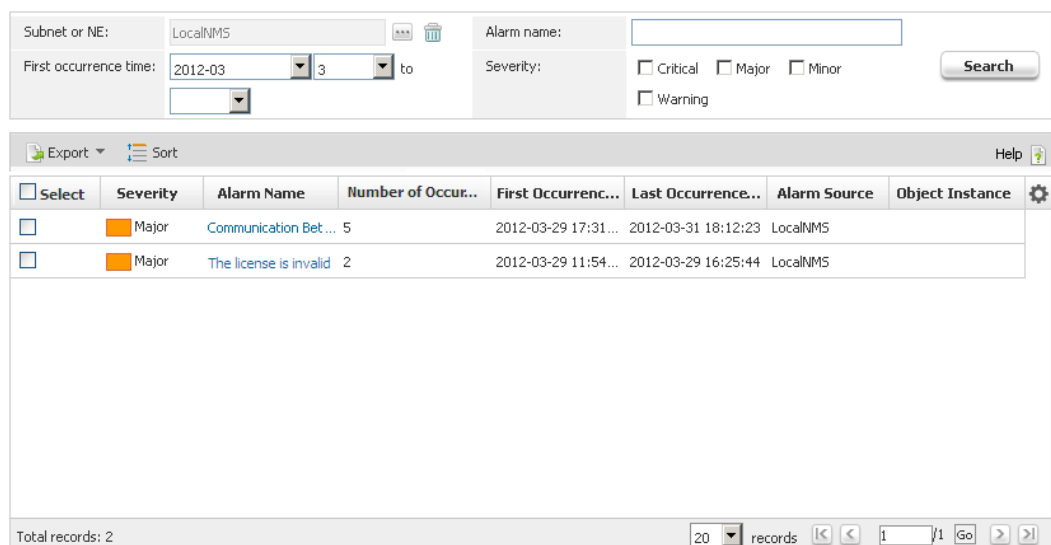
- **Subnet or NE:** click . In the **Select Subnet or NE** dialog box, select the required subnet or NE.

**NOTE**

If you want to re-select another alarm source, click to clear the alarm source that is currently selected.

- **Alarm name:** enter the name of a historical alarm.
- **First occurrence time:** select a start and end dates.
- **Severity:** select the severity of a historical alarm.

Figure 5-47 Viewing historical alarms



**Step 3** In the **Historical Alarms** window, you can perform the following operations.

| Querying Historical Alarms | Operation Method                                                                                                                                                                                                                                                                                      |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarm Details              | 1. Click <b>Alarm Name</b> .<br>2. In the <b>Alarm Details</b> dialog box, view the alarm severity, possible causes, and rectification suggestion.                                                                                                                                                    |
| Export                     | Select one or more alarms and choose <b>Export &gt; Selected Records</b> to export the alarm information.<br><br><b>NOTE</b><br>If you want to export all alarms, choose <b>Export &gt; All</b> . If you set search criteria, only the historical alarms meeting the search criteria can be exported. |

----End

## 5.5.2 Querying an Event

You can query events to learn about the information sent from a device to the eSight.

### Prerequisites

You have the operation rights for **Browse Events**.

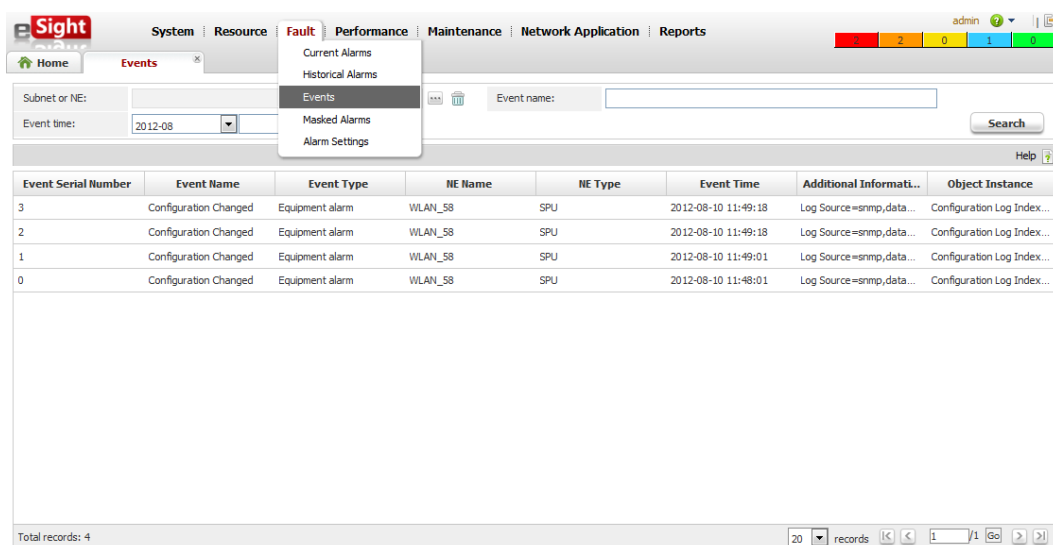
### Context

An event is the notification of anything that takes place in the eSight reported by the device.

### Procedure

**Step 1** Choose **Fault > Events** from the main menu.

**Figure 5-48** Events



**Step 2 Optional:** In the **Events** window, set the search information in the search bar and click **Search**.

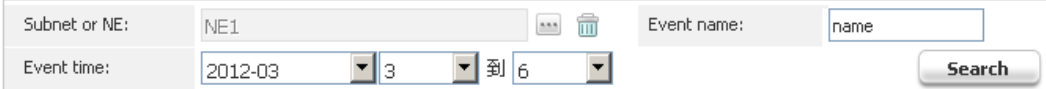
- **Subnet or NE:** click . In the **Select Subnet or NE** dialog box, select an event source. If a subnet is selected, the event source is the NE under the subnet.

**NOTE**

If you want to re-select an event source, click  to clear the currently selected event source.

- **Event name:** set an event name.
- **Event time:** select a start and end dates.

**Figure 5-49** Searching for events



The search bar contains the following fields and controls:

- Subnet or NE:** A text input field containing "NE1". To its right are two icons: a plus sign in a square and a trash can.
- Event name:** A text input field containing "name".
- Event time:** A date range selector showing "2012-03" in a dropdown, followed by a "3" in a dropdown, then the Chinese character "到" (to), followed by a "6" in a dropdown.
- Search:** A button with the text "Search".

**Step 3** In the **Events** window, you can view the events found.

----End

## 5.5.3 Querying a Masked Alarm

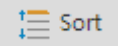
This topic describes how to quickly query the desired masked alarms.

### Prerequisites

You have the operation rights for **Browse Masked Alarms**.

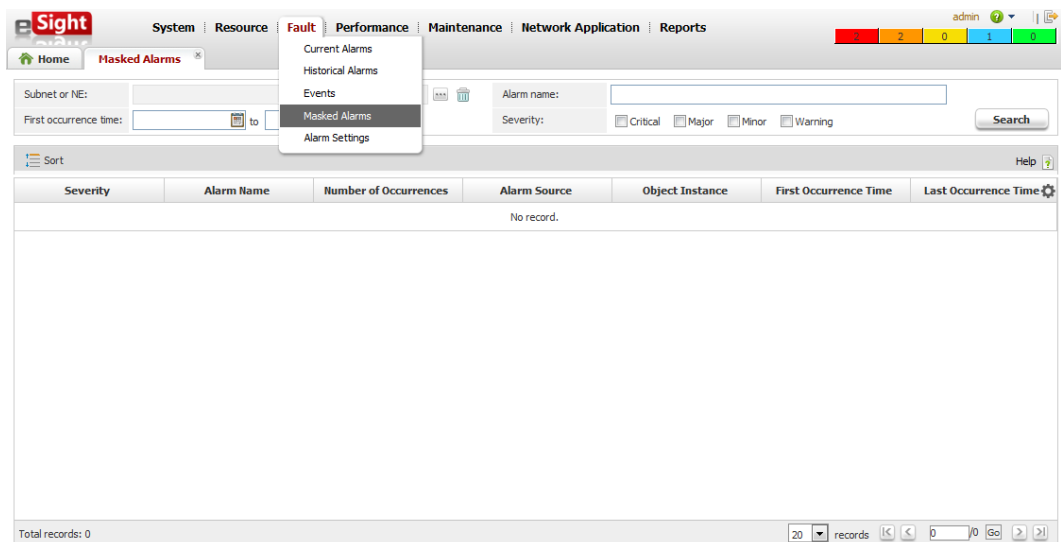
### Context

When you query masked alarms, you can perform the following settings:

- Click  to customize the information you want to query.
- Click  to sort alarms in the **Sort** dialog box.

### Procedure

**Step 1** Choose **Fault > Masked Alarms** from the main menu.

**Figure 5-50** Masked alarms

**Step 2** In the **Masked Alarms** window, set the search information in the search bar and click **Search**.

- **Subnet or NE:** click . In the **Select Subnet or NE** dialog box, select the required alarm sources.

 **NOTE**

If you want to re-select alarm sources, click , The selected alarm sources are cleared.

- **Alarm name:** enter the name of a masked alarm.
- **First occurrence time:** select the first time of masking the alarm.
- **Severity:** select the severity of a masked alarm.

**Figure 5-51** Searching for mask alarms

|                        |                                                                                                                                                                                                  |               |                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| Subnet or NE:          | LocalNMS                   | Alarm name:   | name                                                                                                                             |
| First occurrence time: | 2012-03-31  to 2012-08-03  | Severity:     | <input type="checkbox"/> Critical <input type="checkbox"/> Major <input type="checkbox"/> Minor <input type="checkbox"/> Warning |
|                        |                                                                                                                                                                                                  | <b>Search</b> |                                                                                                                                  |

**Step 3** In the alarm list, click the required alarm name.

The **Alarm Details** dialog box displays the name, cause, and solution for the selected alarm.

----End

## 5.6 Example: Typical Fault Management Operations

This topic describes an example about how to perform fault management operations. From the example, you will learn about the procedure and basic operations about fault management.



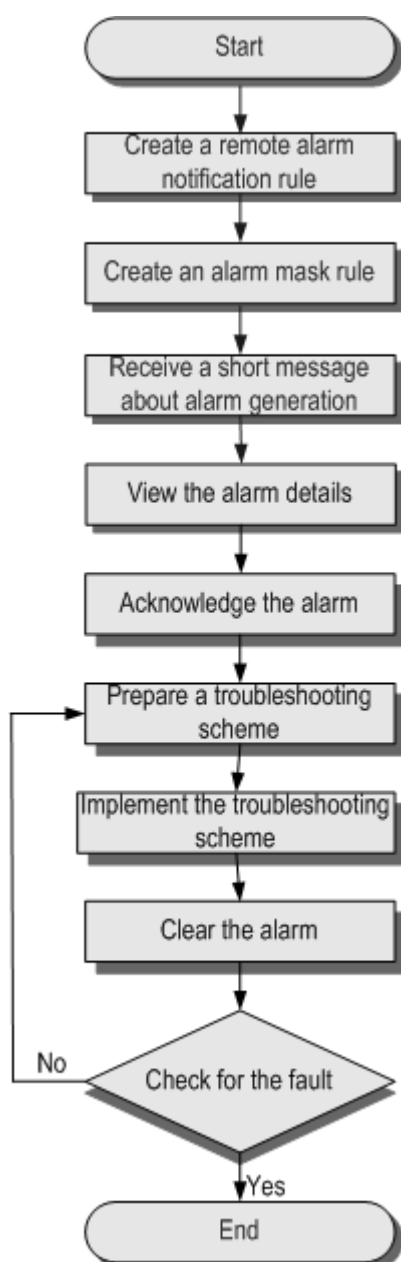
## Context

Assume that the administrator needs to handle personal affairs on December 25, 2011. To monitor and handle the faults of the NEs A, B, and C during absence in real time, the administrator needs to set the fault monitoring rules first. In addition, NE B will be upgraded from 2011-12-25 16:00 to 2011-11-26 10:00.

A large number of alarms that do not require attention will be reported during NE upgrade. In this case, you can create an alarm mask rule to mask them. The masked alarms are automatically placed in the masked alarm list.

Before start, the administrator needs to plan the procedure, as shown in [Figure 5-52](#).

**Figure 5-52** Procedure



## Procedure

### Step 1 Create a remote alarm notification rule.

The administrator thinks that it is very convenient to notify by SMS. After the administrator creates a remote alarm notification rule, the eSight sends the alarm information about NEs A, B, and C to the administrator by SMS.

1. Choose **Fault > Alarm Settings** from the main menu.  
Set the SMS server and notification template. For details, see [5.2.1 Procedure for Setting Remote Notification](#).
2. Create a recipient group **xef** and add the administrator to the group.
  - a. In the **Alarm Settings** window, choose **Remote Notification > Notification Recipient Groups**.
  - b. On the **Notification Recipient Groups** page, click **Create**.
  - c. On the **Create Recipient Group** page, set the recipient group name to **xef**. Then click **Create**.
  - d. In the **Create Recipient** dialog box, set the recipient name to **Li**, enter the mobile phone number of the recipient, and click **OK**.
  - e. Click **Save**.
3. Create a remote alarm notification rule **alarm**.
  - a. In the **Alarm Settings** window, choose **Remote Notification > Remote Notification Rules**.
  - b. On the **Remote Notification Rules** page, choose **Create > By Alarm**.
  - c. On the **Create by Alarm** page, set the rule name to **alarm**. Then click **Add Alarm Sources**.
  - d. Under **Alarm Sources** in the **Add Alarm Sources** dialog box, select NEs A, B, and C, and click **OK**.
  - e. Click **Next**. Under **Alarms/Events** step, click **Add Alarms and Events**.
  - f. Under **Device Type** in the **Add Alarms and Events** dialog box, select a device type. On the **Alarm List** tab page, select all alarm severities, and click **Select All**. On the **Event List** tab page, click **Select All**.  
Perform the preceding steps to set other devices one by one. Then click **OK**.
  - g. Click **Next**. In the **Notification Recipient Groups** area, select **xef** from the **Group** drop-down list.
  - h. Click **Finish**.

The created remote notification rule is enabled by default.

### Step 2 Create a mask rule **NE\_B**.

A large number of alarms that do not require attention are reported when an NE is upgraded. In this case, you can create an alarm mask rule to mask the alarms reported by NE B during the upgrade. The masked alarms are automatically placed in the list of masked alarms.

1. In the **Alarm Settings** window, choose **Basic Settings > Mask Rules**.
2. On the **Mask Rules** page, click **Create**.
3. On the **Create an Alarm Mask Rule** page, set the following parameters:
  - Rule name: **NE\_B**
  - Date: from 2011-12-25 16:00 to 2011-12-26 10:00

- Time: Only during following periods
- 4. Click **Next**. Under **Alarm Sources** step, click **Add Alarm Sources**.
- 5. Under **Select Objects** in the **Add Alarm Sources** dialog box, select NE B and click **OK**.
- 6. Click **Next**. Under **Alarms** step, click **Add Alarms**.
- 7. Under **Device Type** in the **Add Alarms** dialog box, select a device type. In the right area, select all alarm severities, and click **Select All**. Then click **OK**.
- 8. Click **Finish**.

The created alarm mask rule is enabled by default.

**Step 3** The administrator receives a short message "The license is invalid" from the eSight.

**Step 4** View the alarm details.

1. [Log in to the eSight](#).
2. Choose **Fault > Current Alarms**. In the **Current Alarms** window, a message indicating **The license is invalid** is displayed.
3. Clicks the alarm. In the **Alarm Details** dialog box, view the alarm details.

**Step 5** Acknowledge the alarm.

Based on the alarm details, it is found that the fault can be rectified and the alarm can be cleared. In the **Current Alarms** window, you can select the alarm and click **Acknowledge** to acknowledge the alarm.

**Step 6** Prepare the troubleshooting scheme.

Based on the repair suggestions in the alarm details and the running status of the eSight, you can handle the alarm.

**Step 7** Troubleshoot the fault.

Contact the administrator to apply for a new license and import the license to the eSight.

**Step 8** Check the troubleshooting result.

Choose **Fault > Historical Alarms**. You can find the alarm **The license is invalid**.

----**End**

# 6 Performance Management

## About This Chapter

Performance management provides the capabilities for network maintenance personnel to understand and manage the performance of the network. Network maintenance personnel can optimize the performance of the network by monitoring the operating status of the network and its services within a period of time.

### 6.1 Overview of Performance Management Operations

This topic describes the performance management operations.

### 6.2 Performance Monitoring Process

The eSight collects performance data on managed NEs, and displays the collection result for users to analyze. This topic describes the performance monitoring process.

### 6.3 Setting Performance Monitoring

By monitoring and collecting NE or network performance data, network maintenance personnel can detect and rectify potential faults in advance.

### 6.4 Browsing Performance Monitoring Data

You can browse performance monitoring data to get familiar with the network running status, and locate and rectify potential faults in advance.

### 6.5 Example: Typical Performance Management Operations

This topic describes an example about how to perform performance management operations. From the example, you will learn about the procedure and basic operations about performance management.

## 6.1 Overview of Performance Management Operations

This topic describes the performance management operations.

### Context

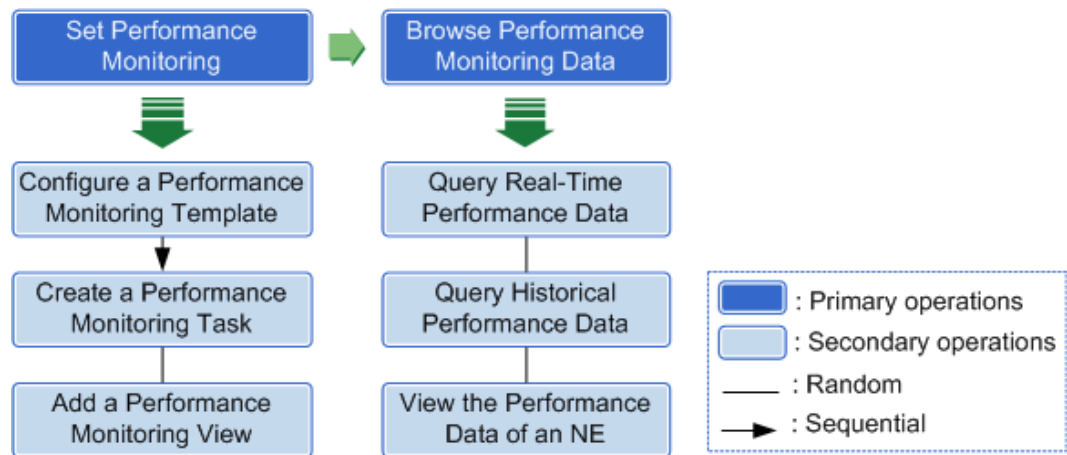
Before performing performance management operations, you need to be familiar with the basic concepts about performance management, such as performance indicators and

thresholds. See [1.2.5 Basic Concepts of Performance Management](#). Understanding these concepts will help you avoid errors when performing performance management operations.

## Overview of Performance Management Operations

[Figure 6-1](#) shows the overview of performance management operations. For details, click the operation in the overview.

**Figure 6-1** Overview of performance management operations



[Table 6-1](#) describes the performance management operations.

**Table 6-1** Performance management operations

| Operation                                                           | Description                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">6.3.1 Configuring a Performance Monitoring Template</a> | A performance monitoring template allows you to collect KPI data on NEs. After an NE is created, the eSight automatically creates performance data collection tasks for the NE based on the template settings, collects data, and generates alarms.       |
| <a href="#">6.3.2 Creating a Performance Monitoring Task</a>        | To start a performance monitoring task for collecting performance data, you must first create a performance monitoring task.                                                                                                                              |
| <a href="#">6.3.3 Adding a Performance Monitoring View</a>          | A performance monitoring view provides real-time graphical monitoring for all performance indicators. In a performance monitoring view, you can monitor multiple objects for one performance indicator or multiple performance indicators for one object. |
| <a href="#">6.4.1 Querying Real-Time Performance Data</a>           | You can query real-time performance data in a performance monitoring view. The performance monitoring view can graphically show performance data changes.                                                                                                 |
| <a href="#">6.4.2 Querying Historical Performance Data</a>          | You can query historical performance data in a specified period to get familiar with the network or service running status.                                                                                                                               |

| Operation                                                   | Description                                                                                                                       |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">6.4.3 Viewing the Performance Data of an NE</a> | The eSight monitors NE performance indicators in real time. Tables and diagrams are used to display the real-time NE performance. |

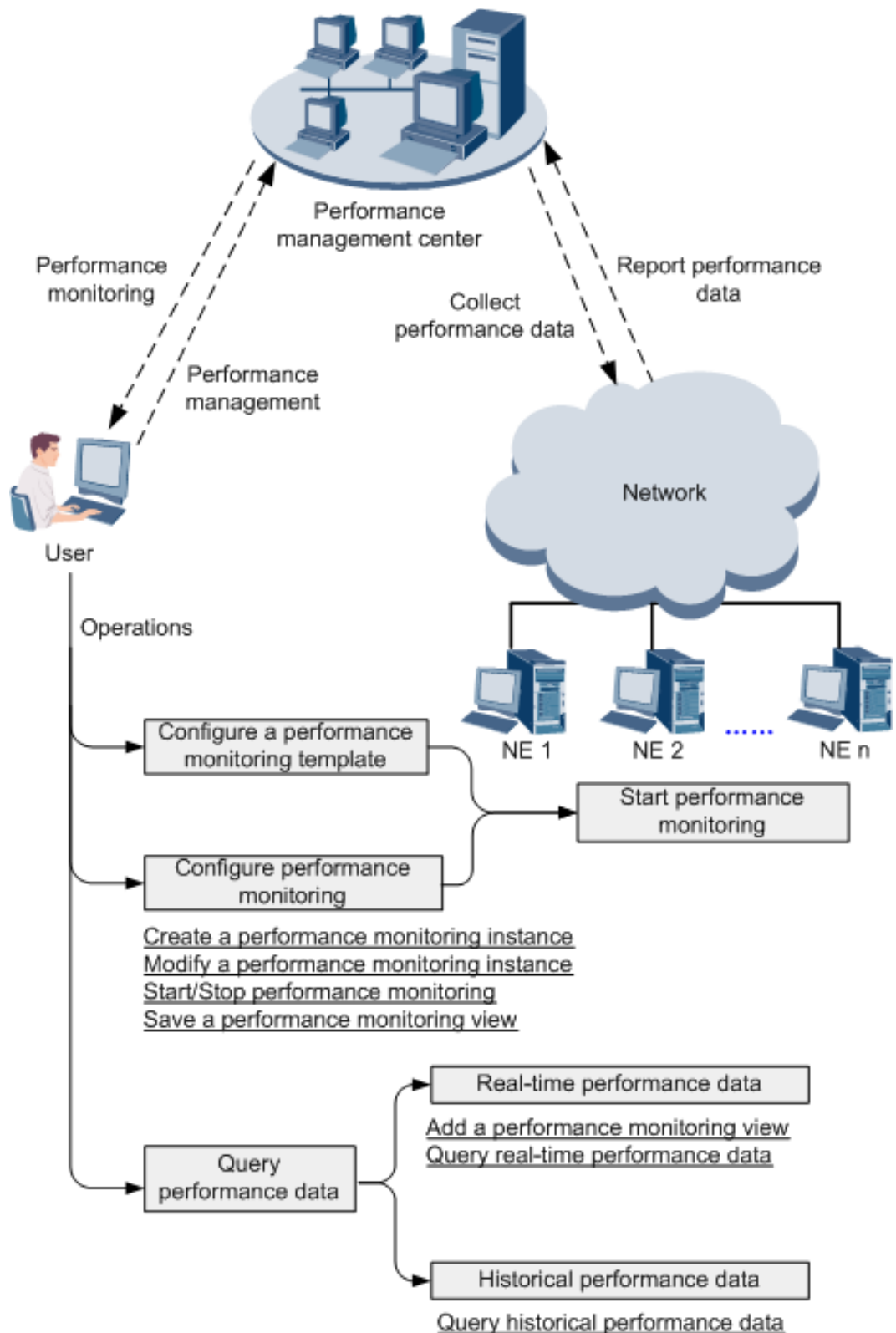
## 6.2 Performance Monitoring Process

The eSight collects performance data on managed NEs, and displays the collection result for users to analyze. This topic describes the performance monitoring process.

### Performance Monitoring Process

[Figure 6-2](#) shows the performance monitoring process. The two sides connected to the eSight are users and NEs. After you enable performance monitoring on the eSight client, the eSight collects performance data of NEs and presents the data for viewing.

**Figure 6-2** Performance monitoring process



## Process of Monitoring NE Performance on the User Side

The process of monitoring NE performance on the user side is as follows:

1. **6.3.1 Configuring a Performance Monitoring Template:** As the NEs of the same type have the same attributes, you can preset performance monitoring parameters in a template. Monitoring tasks are automatically added to the **Monitoring Configuration** window based on the template settings, performance data is automatically collected, and related alarms are generated and reported.
2. **6.3.2 Creating a Performance Monitoring Task:** Create a performance monitoring instance on a monitoring object, and enable/disable the performance monitoring instance to collect performance data. You can modify attributes for a monitoring object, and monitor the data collection and alarm status in real time for all performance monitoring instances.
3. **Querying Performance Monitoring Data:** The performance monitoring data reported by NEs are stored in the performance database of the eSight. Performance monitoring data includes real-time performance data and historical performance data.
  - **Real-time performance data:** In a performance monitoring view, the NE performance data are displayed in real time, and the changes in the performance data trends are displayed in graphics.
  - **Historical performance data:** The performance data within a specified period can be queried, which helps learn about the operating status of the network or service in the period. Historical performance data can be displayed in tables or curve diagrams.

## 6.3 Setting Performance Monitoring

By monitoring and collecting NE or network performance data, network maintenance personnel can detect and rectify potential faults in advance.

### 6.3.1 Configuring a Performance Monitoring Template

A performance monitoring template allows you to collect KPI data on NEs. After an NE is created, the eSight automatically creates performance data collection tasks for the NE based on the template settings, collects data, and generates alarms.

#### Prerequisites

You have the operation rights for **Template Configuration**.

#### Context

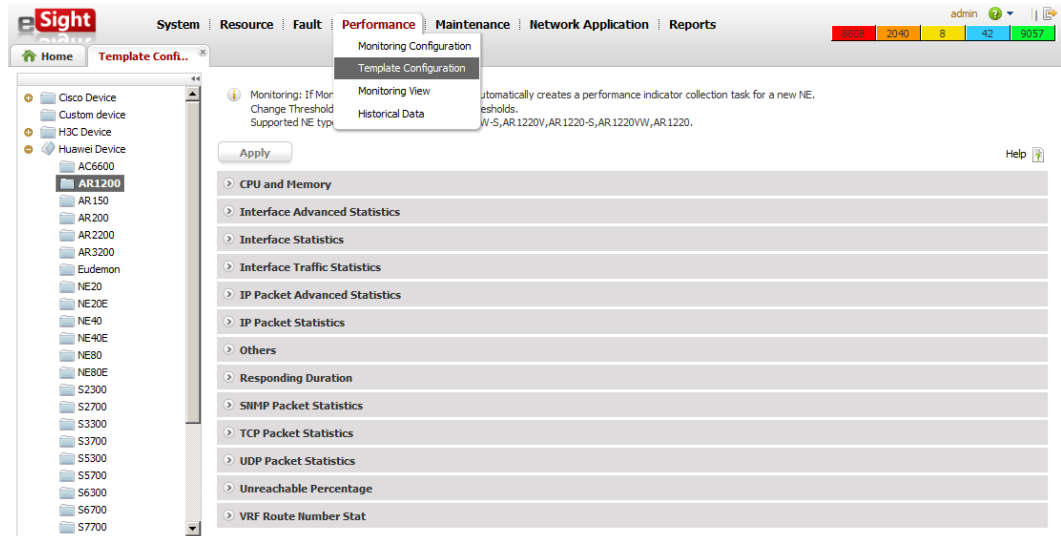
The NEs of the same type have the same attributes. You can place the attributes in a performance monitoring template, and set the attributes to be monitored by default. When a new NE is accessed, the NE automatically inherits the settings in the template to possess the default monitoring and alarm reporting capabilities. The settings in the performance monitoring template can be applied to NEs in batches, which facilitates creation and delivery of performance collection tasks.

#### Procedure

- Step 1** Choose **Performance > Template Configuration** from the main menu.



Figure 6-3 Template configuration



**Step 2** In the navigation tree of the **Template Configuration** window, select an NE type. All performance indicators of this NE type are displayed in collapsed mode on the right page.

**Step 3** Click  to expand the performance counters.

Figure 6-4 Expanding the performance counters

| CPU and Memory                       |                   |          |       |       |         |                                                                                       |                                                                                       |
|--------------------------------------|-------------------|----------|-------|-------|---------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Interface Advanced Statistics        |                   |          |       |       |         |                                                                                       |                                                                                       |
| Indicator Name                       | Collection Period | Critical | Major | Minor | Warning | Change Thresholds                                                                     | Monitoring                                                                            |
| Broadcast packet receiving rate      | 15 minutes        |          |       |       |         |  |  |
| Broadcast packet sending rate        | 15 minutes        |          |       |       |         |  |  |
| Multicast packet receiving rate      | 15 minutes        |          |       |       |         |  |  |
| Multicast packet sending rate        | 15 minutes        |          |       |       |         |  |  |
| Non-unicast packet receiving rate    | 15 minutes        |          |       |       |         |  |  |
| Non-unicast packet sending rate      | 15 minutes        |          |       |       |         |  |  |
| Rate for receiving packets with u... | 15 minutes        |          |       |       |         |  |  |
| Unicast packet receiving rate        | 15 minutes        |          |       |       |         |  |  |
| Unicast packet sending rate          | 15 minutes        |          |       |       |         |  |  |
| Interface Statistics                 |                   |          |       |       |         |                                                                                       |                                                                                       |
| Interface Traffic Statistics         |                   |          |       |       |         |                                                                                       |                                                                                       |

**Step 4** Click . In the **Change Thresholds** dialog box, set the conditions of generating or clearing an alarm and repetition times, and click **OK**.

**CAUTION**

After the thresholds are changed, all previous alarms are cleared.

For example, if **Number of repetitions** is set to 3, it indicates that performance value of three consecutive performance collection periods exceeds the threshold so that the alarm is reported.

**Figure 6-5** Changing thresholds

**Step 5** Set the performance collection period.

**Step 6** Set **Monitoring** for the performance indicator.

- Select **Monitoring**.

When a new NE of the same type is connected, the eSight automatically adds the monitoring task of the performance indicator in the **Monitoring Configuration** window.

- Deselect **Monitoring**.

When a new NE of the same type is connected, the eSight does not automatically create performance monitoring tasks for the NE. However, the eSight allows you to select **Enable Template** to reference the settings of the performance monitoring template when you set indicator attributes.

**Step 7** Click **Apply**.

----End

## Result

If the alarm threshold is set, when the condition of generating an alarm is met, the eSight automatically generates an alarm and sends it to the active alarm window.

## 6.3.2 Creating a Performance Monitoring Task

To start a performance monitoring task for collecting performance data, you must first create a performance monitoring task.

### Prerequisites

You have permission **Monitoring Configuration**.

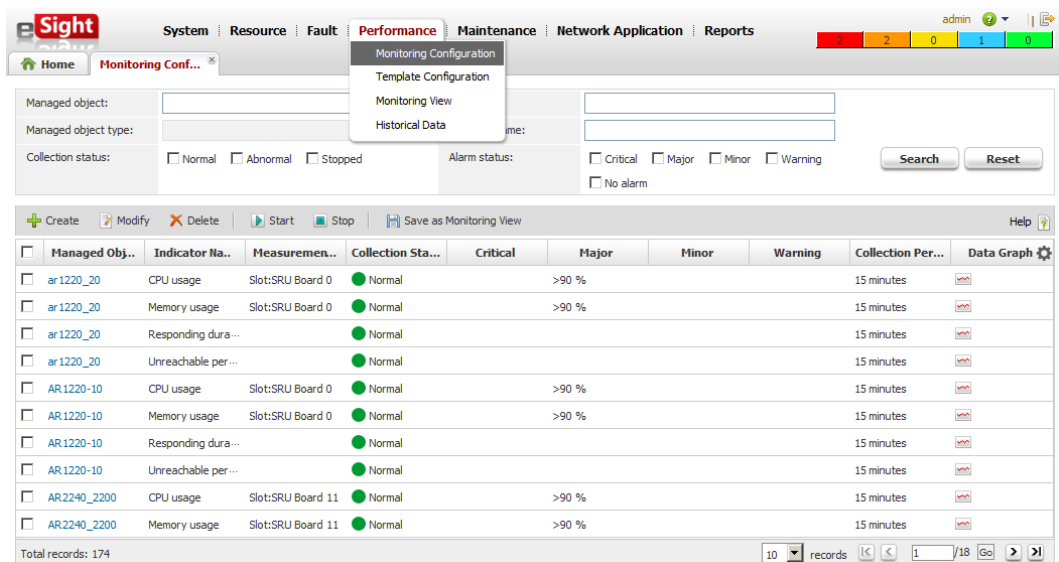
### Context

You can enter or select measurement objects.

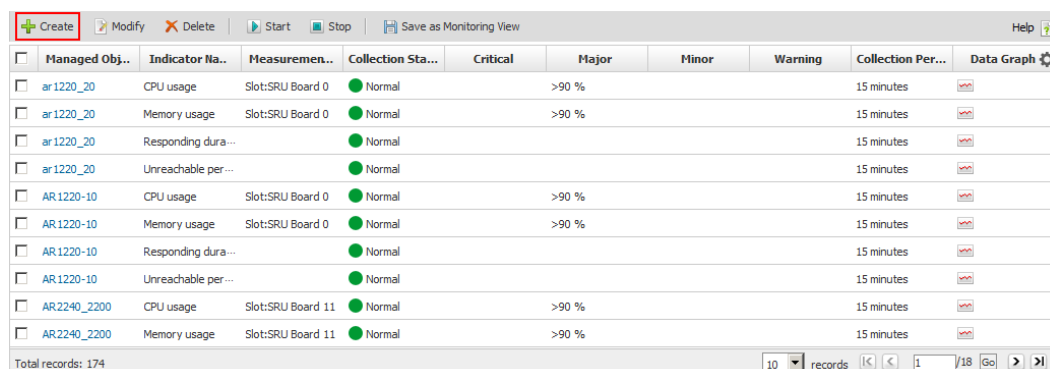
### Procedure

**Step 1** Choose **Performance** > **Monitoring Configuration** from the main menu.

**Figure 6-6** Monitoring configuration



**Step 2** In the **Monitoring Configuration** window, click **Create**.

**Figure 6-7** Operation entry to creating a performance monitoring task

| Managed Obj...                       | Indicator Na...    | Measuremen...     | Collection Sta... | Critical | Major | Minor | Warning | Collection Per... | Data Graph |
|--------------------------------------|--------------------|-------------------|-------------------|----------|-------|-------|---------|-------------------|------------|
| <input type="checkbox"/> ar1220_20   | CPU usage          | Slot:SRU Board 0  | ● Normal          |          | >90 % |       |         | 15 minutes        |            |
| <input type="checkbox"/> ar1220_20   | Memory usage       | Slot:SRU Board 0  | ● Normal          |          | >90 % |       |         | 15 minutes        |            |
| <input type="checkbox"/> ar1220_20   | Responding dura... |                   | ● Normal          |          |       |       |         | 15 minutes        |            |
| <input type="checkbox"/> ar1220_20   | Unreachable per... |                   | ● Normal          |          |       |       |         | 15 minutes        |            |
| <input type="checkbox"/> AR1220-10   | CPU usage          | Slot:SRU Board 0  | ● Normal          |          | >90 % |       |         | 15 minutes        |            |
| <input type="checkbox"/> AR1220-10   | Memory usage       | Slot:SRU Board 0  | ● Normal          |          | >90 % |       |         | 15 minutes        |            |
| <input type="checkbox"/> AR1220-10   | Responding dura... |                   | ● Normal          |          |       |       |         | 15 minutes        |            |
| <input type="checkbox"/> AR1220-10   | Unreachable per... |                   | ● Normal          |          |       |       |         | 15 minutes        |            |
| <input type="checkbox"/> AR2240_2200 | CPU usage          | Slot:SRU Board 11 | ● Normal          |          | >90 % |       |         | 15 minutes        |            |
| <input type="checkbox"/> AR2240_2200 | Memory usage       | Slot:SRU Board 11 | ● Normal          |          | >90 % |       |         | 15 minutes        |            |

Total records: 174

**Step 3** Select a managed object.

1. On the **Create a performance monitoring task** page, click **Select Managed Objects**.

**Figure 6-8** Operation entry to selecting managed objects

Monitoring Configuration > Create a performance monitoring task

To configure a performance monitoring template, perform the following steps: 1. Select managed objects. 2. Select their indicators. 3. Select the measurement objects for the indicators.

**Select Managed Objects** | Select Indicators | Modify Properties | Help

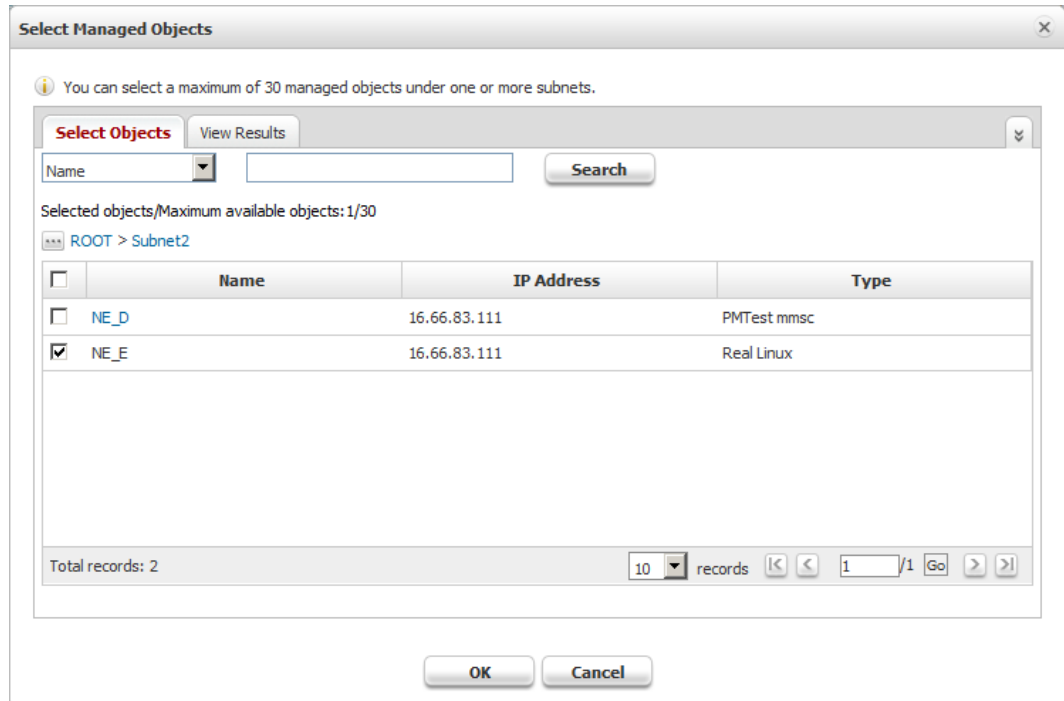
| Managed Objects | Object Type | IP Address | Measuremen... | Operation |
|-----------------|-------------|------------|---------------|-----------|
| No record.      |             |            |               |           |

OK Cancel

2. On the **Select Objects** tab page of the **Select Managed Objects** dialog box, select managed objects.

 **TIP**

- Click a subnet name to open the list of devices or subnets.
- Click a node in the navigation tree, for example, **ROOT**. The related page is displayed.
- Set the keyword of **Name**, **IP Address**, or **Type** to search for the NEs or subnets that meet the search criteria.

**Figure 6-9** Selecting managed objects

3. On the **View Results** tab page, view the selected managed objects.

 **NOTE**

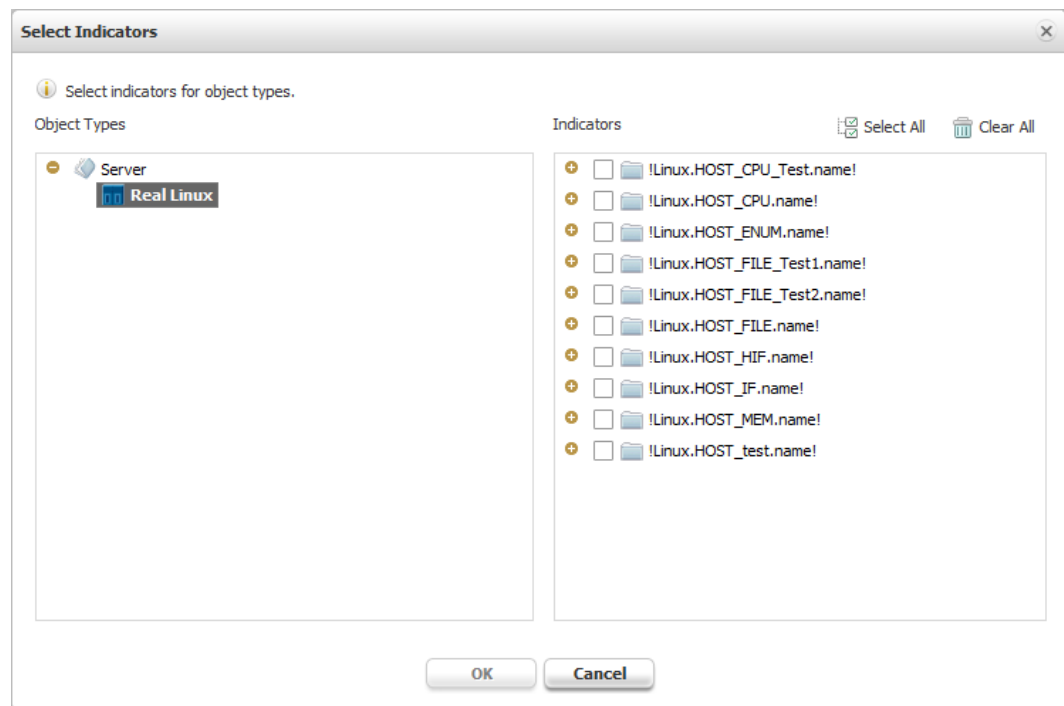
- On the **View Results** tab page, you can click  in the **Operation** column to deselect the required object.
- You can click **Clear All** on the **View Results** tab page to clear the managed objects on the **View Results** tab page.

4. Click **OK**.

**Step 4** Select an indicator.

1. On the **Create a performance monitoring task** page, click **Select Indicators**.
2. In the **Select Indicators** dialog box, select an object type from **Object Types**.

**Figure 6-10** Selecting indicators



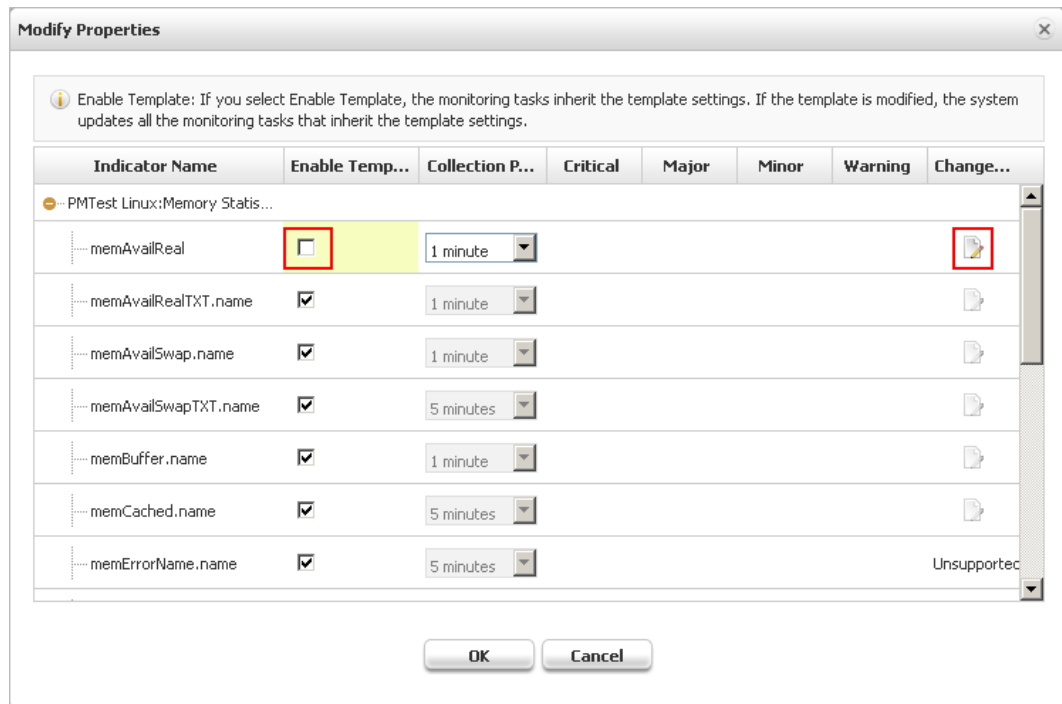
3. Select an indicator from **Indicators** and click **OK**.

**Step 5 Optional:** Customize the collection interval and threshold of performance monitoring.

1. On the **Create a performance monitoring task** page, click **Modify Properties**.
2. In the **Modify Properties** dialog box, deselect **Enable Template** of the target indicator.

**NOTE**

- If **Enable Template** is selected, the monitoring instance uses the attributes in the template. To modify the attributes, you must deselect **Enable Template**.
- If **Enable Template** is selected, after you modify the attributes in the performance monitoring template, the related performance counter automatically uses the new attributes.
- The attribute modification result about the performance counter is effective for all NEs that involve this performance counter.

**Figure 6-11** Setting not to enable the template

3. Click  in the **Change Thresholds** column of the target indicator.
4. In the **Change Thresholds** dialog box, modify the threshold of generating or clearing an alarm, and repetition times. Click **OK**.

**CAUTION**

After the thresholds are changed, all previous alarms are cleared.

For example, if **Number of repetitions** is set to 3, it indicates that performance value of three consecutive performance collection periods exceeds the threshold so that the alarm is reported.

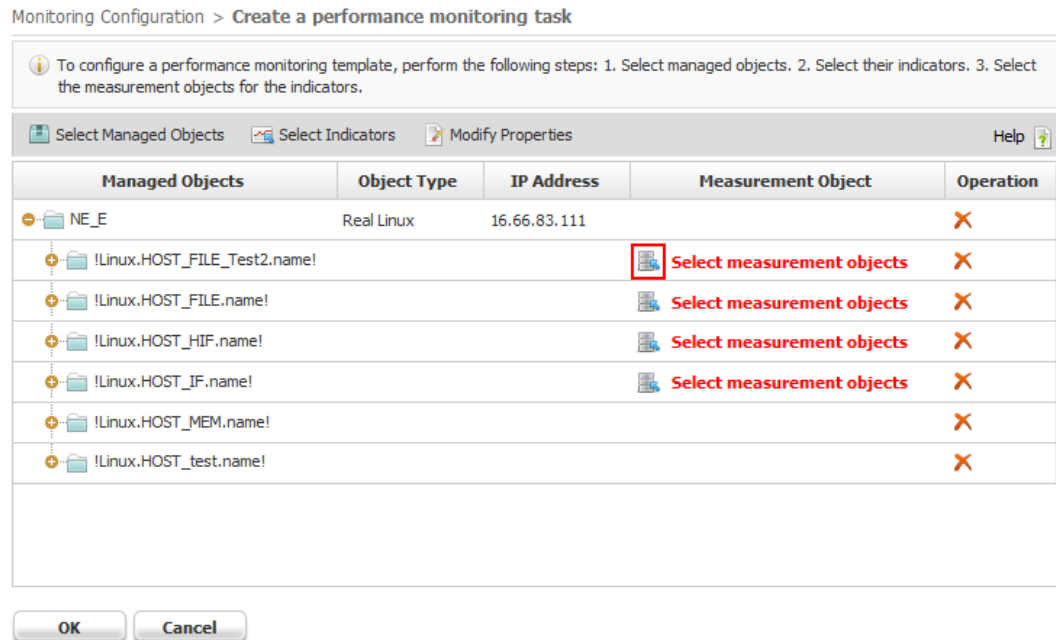
5. In the **Modify Properties** dialog box, click **OK**.

**Step 6** Select a measurement object.

You must select measurement objects for all the selected performance indicators. If some performance indicators do not have measurement objects, you do not need to select measurement objects for them.

1. Click  in the **Measurement Object** column of the selected indicator.

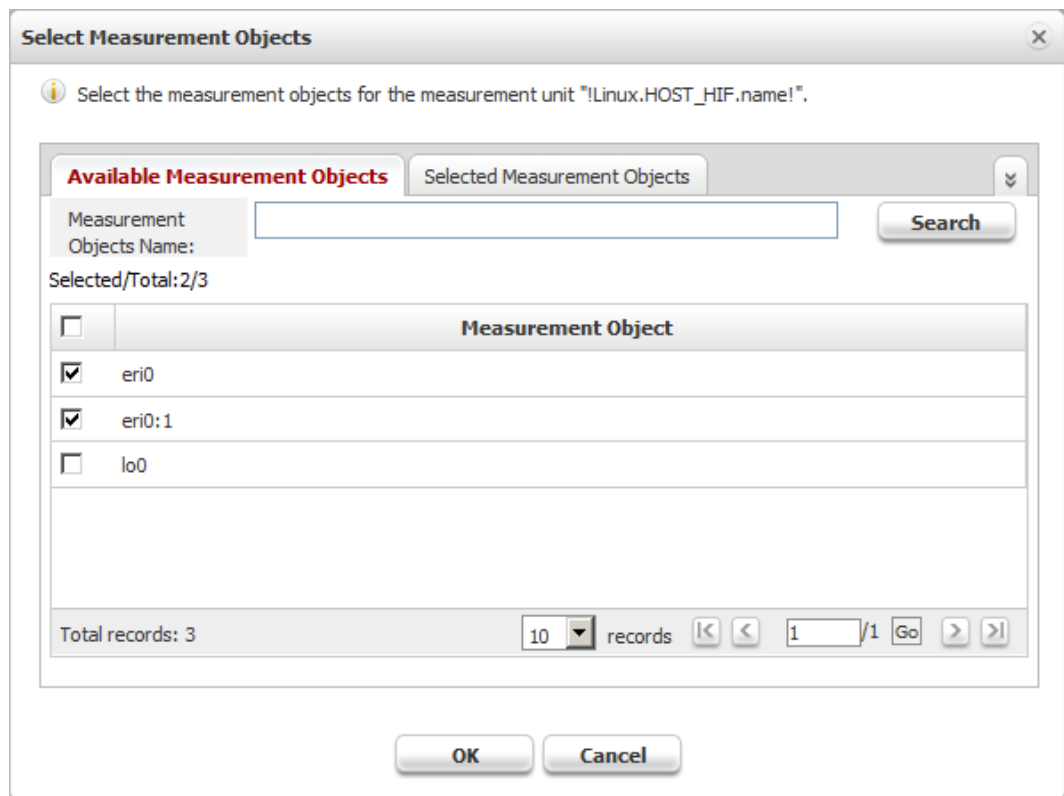
**Figure 6-12** Operation entry to selecting measurement object



2. In the **Select Measurement Objects** dialog box, select or enter measurement objects.
  - Select measurement object for a performance indicators:
    - a. In the **Select Measurement Objects** dialog box, select a measurement object on the **Available Measurement Objects** tab page.  
In the **Measurement Objects Name** text box, enter keywords, and click **Search**.



**Figure 6-13** Selecting measurement object

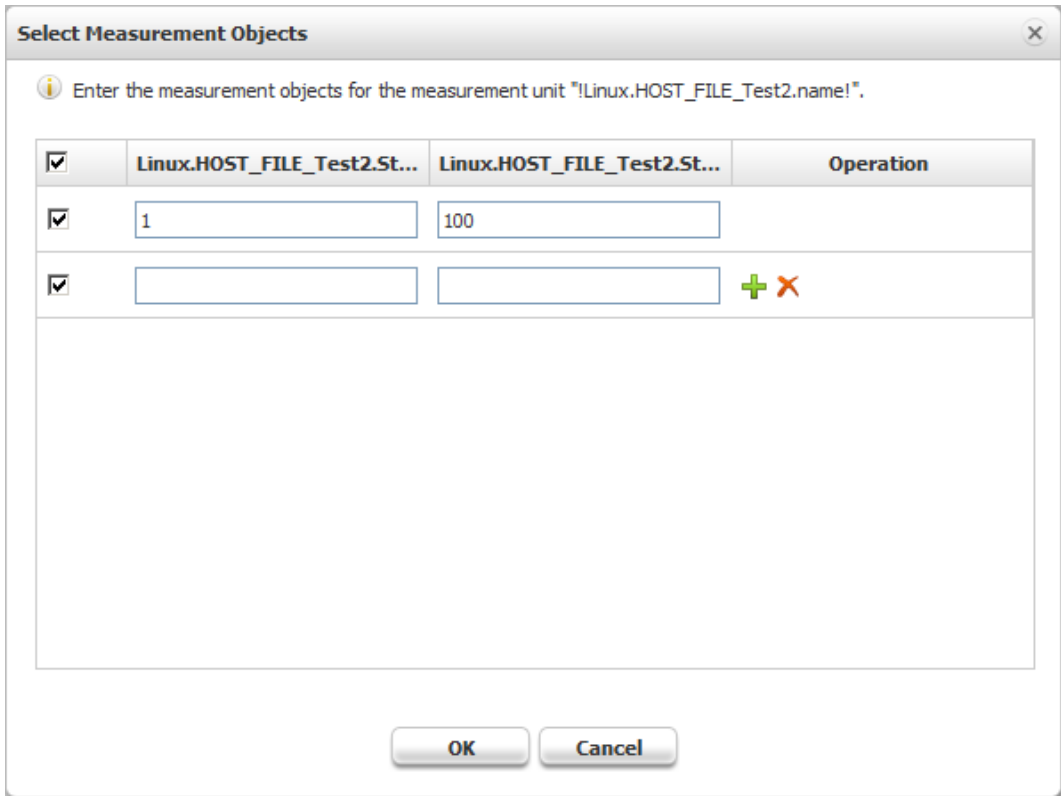


- b. On the **Selected Measurement Objects** tab page, view the selected measurement objects.

On the **Selected Measurement Objects** tab page, select one or more measurement objects; or click **Delete** to deselect a measurement object.

- c. Click **OK**.
- Enter measurement object for a performance indicators:
  - a. In the **Select Measurement Objects** dialog box, select measurement objects from the measurement objects provided by the eSight by default.

Figure 6-14 Selecting or entering measurement objects



- b. Click . In the displayed text box, enter the measurement object information.

**NOTE**

- Click to delete the measurement object.
  - You cannot delete the measurement objects provided by the eSight by default.
- c. Click **OK**.

**Step 7** On the **Create a performance monitoring task** page, click **OK**.

**Step 8** On the **Operation Results** page, click **Finish**.

After a monitoring task is successfully created, the task is started by default. In the monitoring task list, you can view the data collection status of the tasks.

----End

**Follow-up Procedure**

After a monitoring task is successfully created, you can perform the following steps:

| Setting Performance Monitoring Task     | Operation Method                                                                                                                                 |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifying a Performance Monitoring Task | You can modify a performance monitoring task to meet management requirements.<br>1. In the <b>Monitoring Configuration</b> window, select one or |

| Setting Performance Monitoring Task                          | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                              | <p>more tasks, and click <b>Modify</b>.</p> <p>2. In the <b>Modify Properties</b> dialog box, modify the indicator attributes, such as, the threshold of generating an alarm.</p> <p><b>CAUTION</b><br/>After the thresholds are changed, all previous alarms are cleared.</p>                                                                                                                                                                                                                                                                                                                                                 |
| Deleting a Performance Monitoring Task                       | <p>You can delete unnecessary tasks to ensure sufficient memory and proper running of tasks on the server.</p> <p>In the <b>Monitoring Configuration</b> window, select one or more tasks, and click <b>Delete</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                        |
| Starting a Performance Monitoring Task                       | <p>You can start a performance monitoring task to enable the eSight to monitor performance indicators and collect data, and report alarms.</p> <p>In the <b>Monitoring Configuration</b> window, select one or more tasks whose <b>Collection Status</b> is <b>Stopped</b>, and click <b>Start</b>.</p>                                                                                                                                                                                                                                                                                                                        |
| Stopping a Performance Monitoring Task                       | <p>You can stop the tasks that do not require attention to ensure sufficient memory and proper running of tasks on the server.</p> <p>In the <b>Monitoring Configuration</b> window, select one or more tasks, and click <b>Stop</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| Viewing the historical performance data of a monitoring task | <p>You can view the historical performance data of a monitoring task by using the <b>Data Graph</b> and <b>Data Table</b>.</p> <p>1. In the <b>Monitoring Configuration</b> window, click  in the <b>Data Graph</b> column for the required monitoring task.</p> <p>2. On the <b>Data Graph</b> and <b>Data Table</b> tab pages, view the historical performance data of the monitoring task. For details, see steps <a href="#">Step 6</a> and <a href="#">Step 7</a> in <a href="#">6.4.2 Querying Historical Performance Data</a>.</p> |

### 6.3.3 Adding a Performance Monitoring View

A performance monitoring view provides real-time graphical monitoring for all performance indicators. In a performance monitoring view, you can monitor multiple objects for one performance indicator or multiple performance indicators for one object.

#### Prerequisites

- You have the operation rights for **Monitoring View** and **Monitoring Configuration**.
- At least one performance monitoring task exists.

#### Context

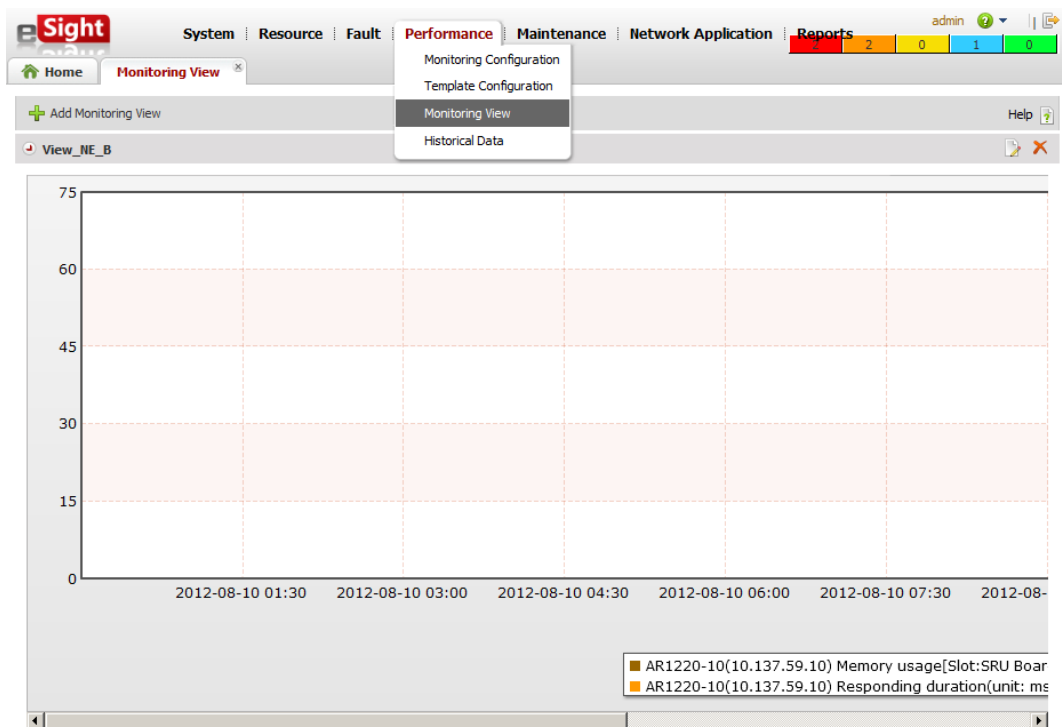
- The counters in the performance monitoring view must be of numeric type.
- You can add a maximum of 10 performance monitoring views and add a maximum of six performance counters in a performance monitoring view.

- The performance monitoring view name is case insensitive. For example, the view name **View AA**, **View aA**, and **View aa** are regarded as a same view name.

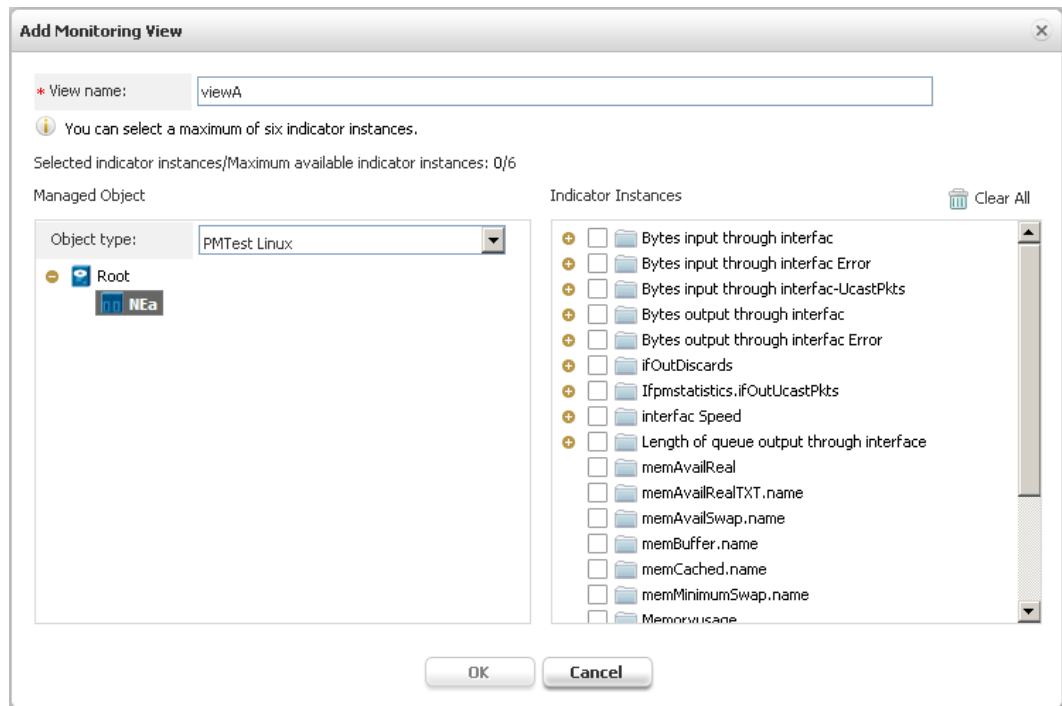
## Procedure

- Create a performance monitoring view on the main page.
1. Choose **Performance** > **Monitoring View** from the main menu.

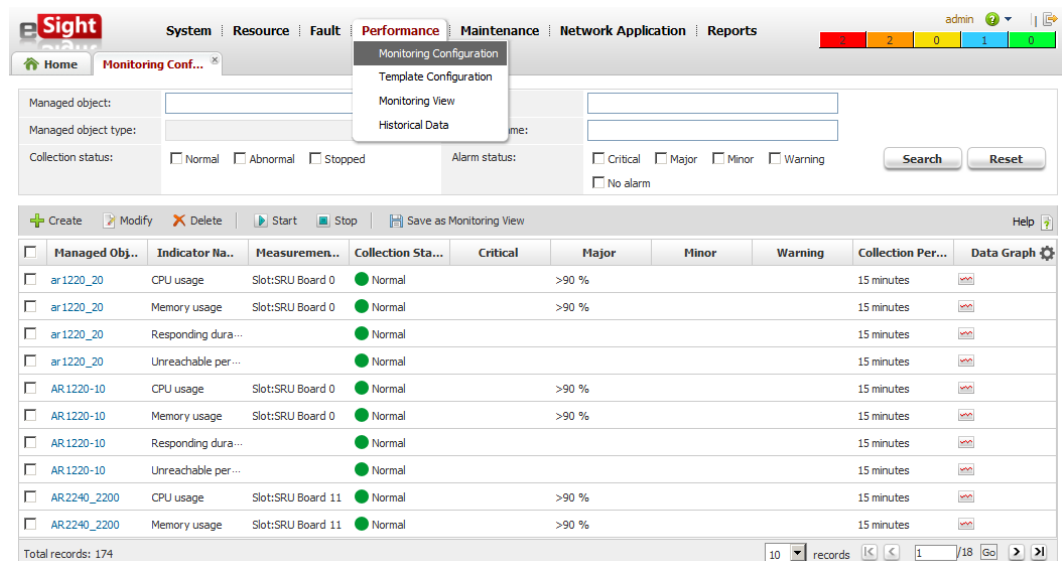
**Figure 6-15** Monitoring view



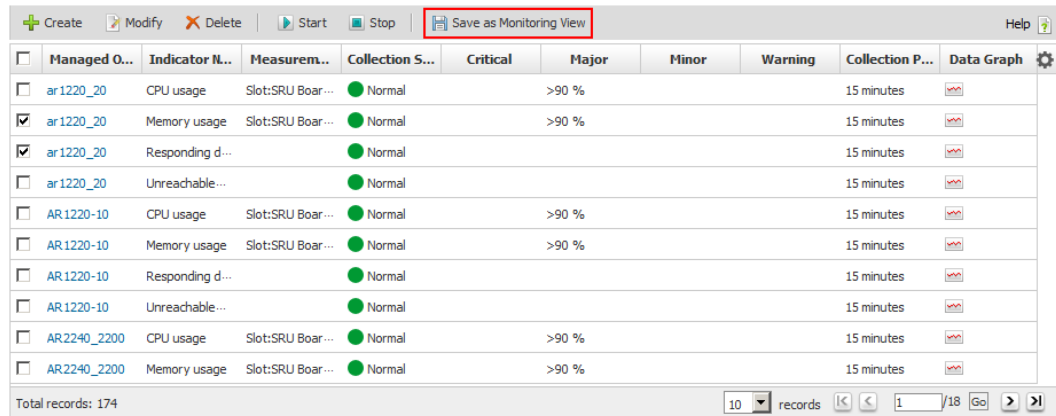
2. In the **Monitoring View** window, click **Add Monitoring View**.
3. In the **Add Monitoring View** dialog box, set the view name, and select a managed object in **Managed Object**.

**Figure 6-16** Setting the performance monitoring view parameters

4. In **Indicator Instances**, select indicators to be added to the performance monitoring view, and click **OK**.
- In the performance monitoring task, save the monitoring task as a performance monitoring view.
1. Choose **Performance > Monitoring Configuration** from the main menu.

**Figure 6-17** Monitoring configuration

2. **Optional:** In the **Monitoring Configuration** window, set the filter criteria and click **Search**. The performance monitoring tasks that meet the filter criteria are displayed.
3. In the **Monitoring Configuration** window, select one or more monitoring tasks, and click **Save as Monitoring View**.

**Figure 6-18** Saving as the monitoring view

4. In the **Add Monitoring View** window, set the view name, and click **OK**.
5. In the **Information** dialog box, click **OK**.
6. Choose **Performance > Monitoring View** from the main menu. In the **Monitoring View** window, view the saved views.

----End

## Follow-up Procedure

After adding a performance monitoring view, you can perform the following steps:

| Setting Performance Monitoring View      | Operation Method                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifying a Performance Monitoring Vieww | <p>You can modify the performance monitoring view to meet management requirements.</p> <ol style="list-style-type: none"><li>1. In the <b>Monitoring View</b> window, click  of the monitoring view.</li><li>2. In the <b>Modify Monitoring View</b> window, modify the view name, and add or delete indicator instances in the view.</li></ol> |
| Deleting a Performance Monitoring View   | <p>You can delete unnecessary performance monitoring views to release resources for creating more views.</p> <p>In the <b>Monitoring View</b> window, click  of the monitoring view.</p>                                                                                                                                                        |



### NOTE

After modifying or deleting a view, if you are querying the view on another client, the system displays a dialog box prompting you to update the view. You can click **OK** in the dialog box to update the view.

## 6.4 Browsing Performance Monitoring Data

You can browse performance monitoring data to get familiar with the network running status, and locate and rectify potential faults in advance.

### 6.4.1 Querying Real-Time Performance Data

You can query real-time performance data in a performance monitoring view. The performance monitoring view can graphically show performance data changes.

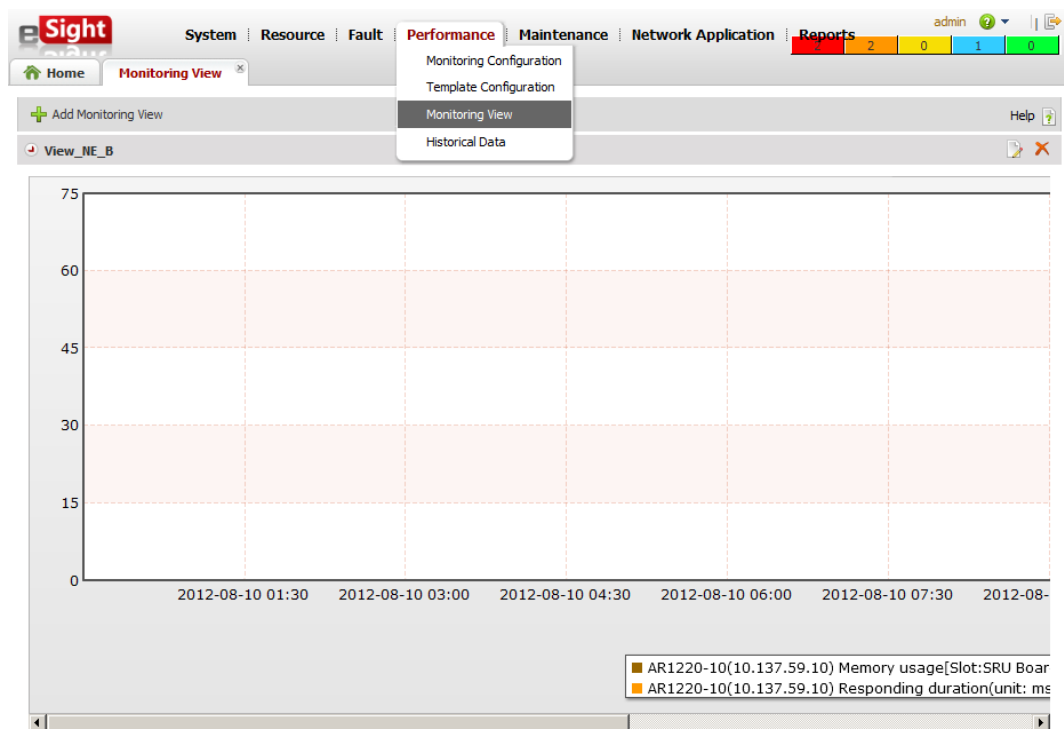
#### Prerequisites

- You have the operation rights for **Monitoring View**.
- A performance monitoring view has been added for the performance counters to be queried.

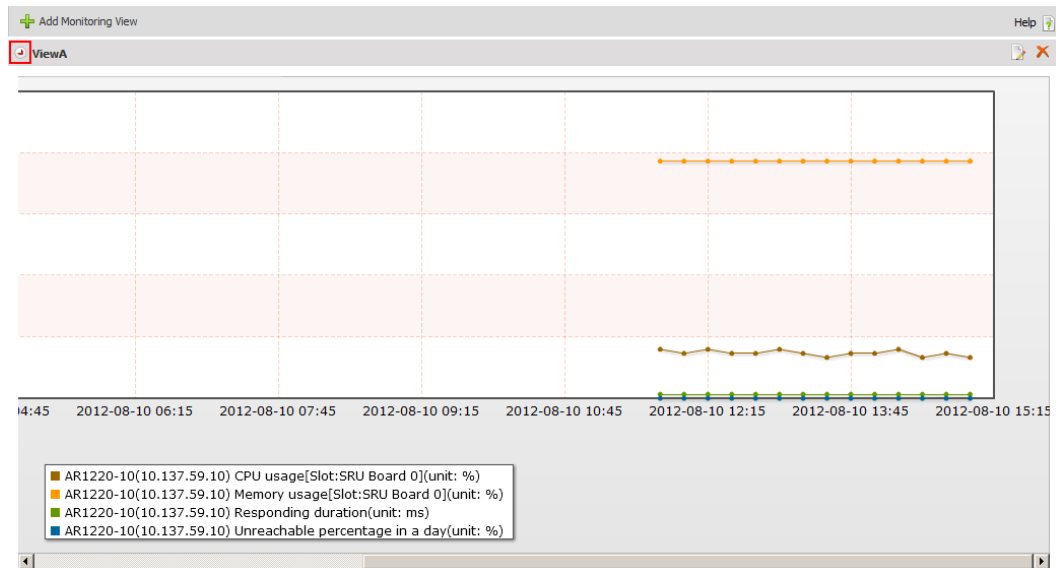
#### Procedure

**Step 1** Choose **Performance > Monitoring View** from the main menu.

**Figure 6-19** Monitoring view



**Step 2** Click  to display the proper performance monitoring view.

**Figure 6-20** Expanding the performance monitoring view

----End

## 6.4.2 Querying Historical Performance Data

You can query historical performance data in a specified period to get familiar with the network or service running status.

### Prerequisites

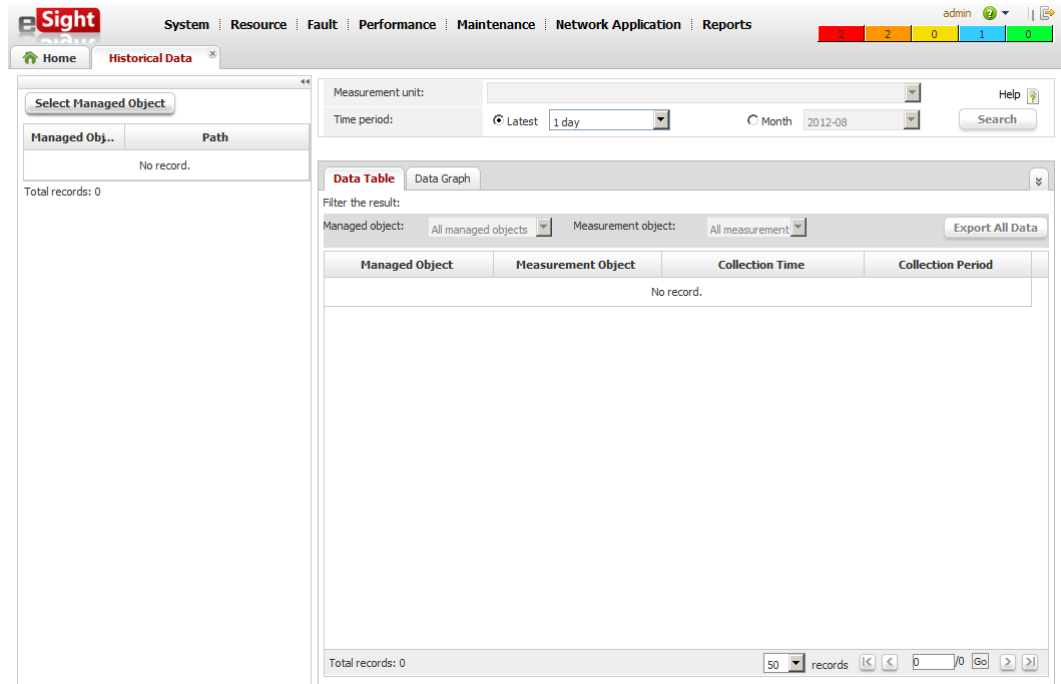
You have the operation rights for **Historical Data**.

### Procedure

**Step 1** Choose **Performance > Historical Data** from the main menu.



**Figure 6-21** Historical data



**Step 2** In the **Historical Data** window, click **Select Managed Object**.

**Step 3** In the **Select Managed Object** dialog box, click  next to **Object type**. Then in the **Select Object Type** dialog box, select the type of the objects to be queried.

**Figure 6-22** Selecting the object type

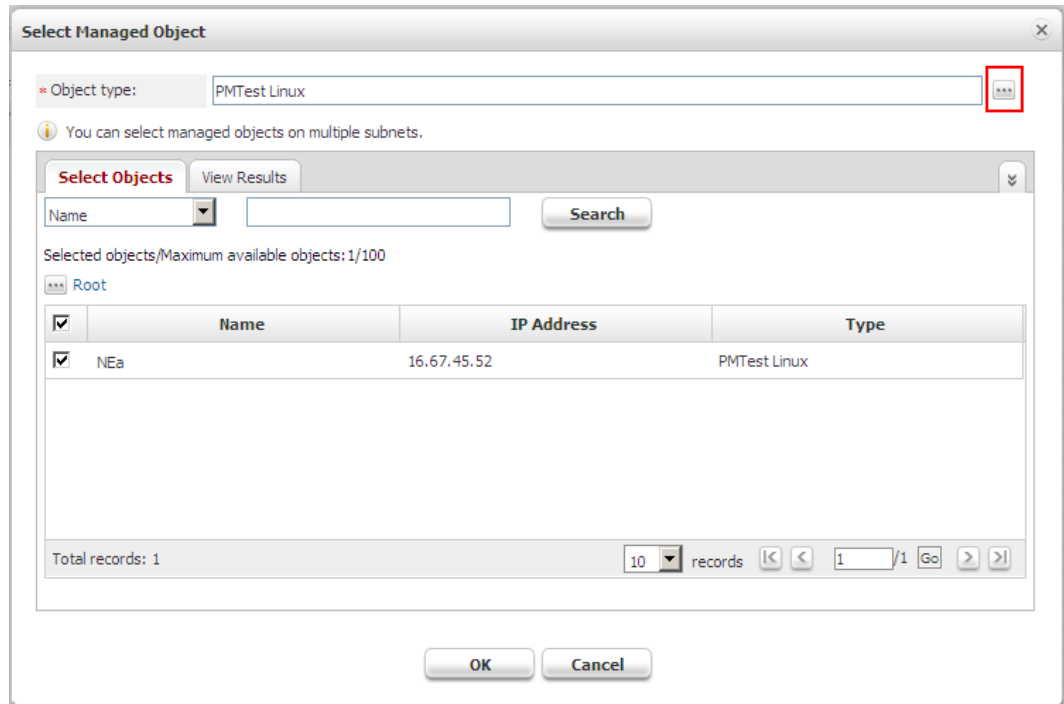
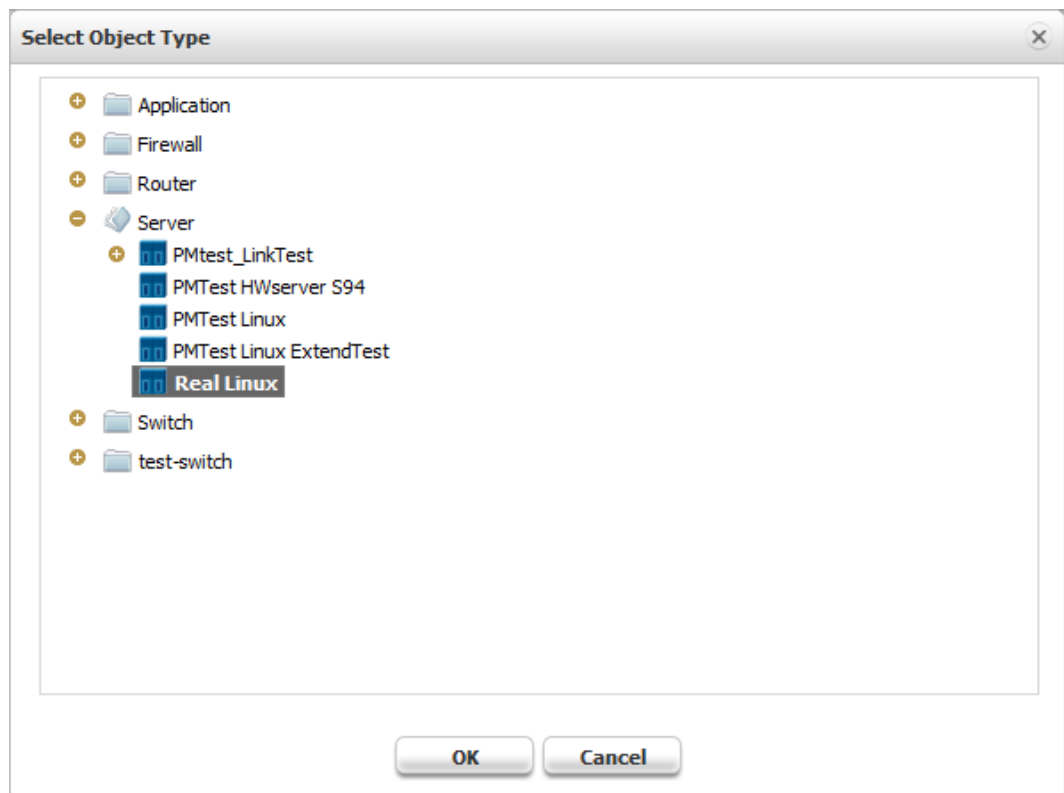


**Figure 6-23** Selecting the object type to be queried



**Step 4** In the **Select Object Type** dialog box, click **OK**.

The **Select Objects** tab page in the **Select Managed Object** dialog box dynamically displays all managed objects of this type.

**Step 5** Select managed objects.

1. On the **Select Objects** tab page of the **Select Managed Object** dialog box, select managed objects.

 **TIP**

- Click a subnet name to open the list of devices or subnets.
- Click a node in the navigation tree, for example, **ROOT**. The related page is displayed.
- Set the keyword of **Name**, **IP Address**, or **Type** to search for the NEs or subnets that meet the search criteria.

2. On the **View Results** tab page, view the selected managed objects.



**NOTE**

- On the **View Results** tab page, you can click  in the **Operation** column to deselect the required object.
- You can click **Clear All** on the **View Results** tab page to clear the managed objects on the **View Results** tab page.

3. Click **OK**.

On the left of the **Historical Data** window, the selected managed objects are displayed in **Managed Objects**.

**Step 6** Set **Measurement unit** and **Time period**, and click **Search**. Performance data that meets the search criteria is displayed in the **Data Table** area.



**NOTE**

Select **Managed object** or **Measurement object** to filter performance data for a specified managed object or measurement object.

Measurement objects are available only for managed objects that contain measurement objects.

**Figure 6-24** Setting the search criteria

Measurement unit: Interface performance statistics  
Time period: Latest 1 day Month 2012-04 Search

Filter the result:  
Managed object: All managed objects Measurement object: All measurement Export All Data

| Managed Obj.. | Measuremen.. | Collection Time  | Collection Pe.. | Bytes output.. | Ifpmstatistic.. | ifOutDiscards.. |
|---------------|--------------|------------------|-----------------|----------------|-----------------|-----------------|
| NE1           | eri0         | 2012-04-01 10:52 | 1 minute        |                |                 |                 |
| NE1           | eri0:1       | 2012-04-01 10:52 | 1 minute        |                |                 |                 |
| NE1           | lo0          | 2012-04-01 10:52 | 1 minute        |                |                 |                 |
| NE1           | eri0         | 2012-04-01 10:53 | 1 minute        |                | 161774          | 0               |
| NE1           | eri0:1       | 2012-04-01 10:53 | 1 minute        |                | 0               | 0               |
| NE1           | lo0          | 2012-04-01 10:53 | 1 minute        |                | 410516          | 0               |
| NE1           | eri0         | 2012-04-01 10:54 | 1 minute        |                | 162842          | 0               |
| NE1           | eri0:1       | 2012-04-01 10:54 | 1 minute        |                | 0               | 0               |
| NE1           | lo0          | 2012-04-01 10:54 | 1 minute        |                | 405289          | 0               |
| NE1           | eri0         | 2012-04-01 10:55 | 1 minute        |                | 163722          | 0               |

**Step 7 Optional:** Set the curve diagram to show the performance monitoring data.

1. On the **Data Graph** tab page, click **Select Instances**.

**Figure 6-25** Selecting instances

Measurement unit: Interface performance statistics  
Time period: Latest 1 day Month 2012-04 Search

Data Table **Data Graph**

Indicator name: Bytes input through interfac(Byte) **Select Instances**

2. In the **Select Instances** dialog box, select object instances related to measurement objects, and click **OK**.

The **Data Graph** tab page displays the diagram of performance indicators.

**NOTE**

- You can select a maximum of six object instances. In the diagram, performance indicators of object instances are represented by curves in different colors.
- When more than 180 performance data records are found, the eSight averages the data within a period of time and displays the data in the line graph.

----End

## Follow-up Procedure

On the **Data Table** tab page, click **Export All Data** to save the collected performance data as a **.csv** file on the local computer.

### 6.4.3 Viewing the Performance Data of an NE

The eSight monitors NE performance indicators in real time. Tables and diagrams are used to display the real-time NE performance.

#### Prerequisites

- You have the operation rights for **Monitoring Configuration** and **KPI Browsing**.
- The NEs to be viewed can be managed by the resource manager, and their performance data can also be managed.

#### Context

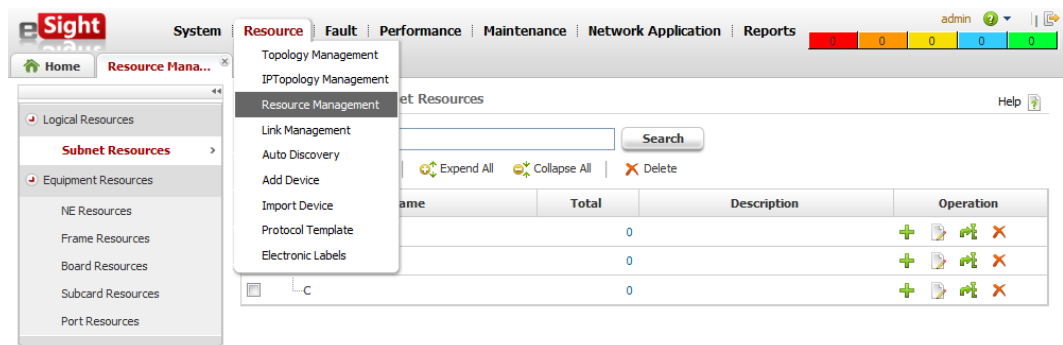
The eSight provides the **Resource Management** and **Performance Management** entries for you to view the NE performance.

#### Procedure

**Step 1** Access the NE management window.

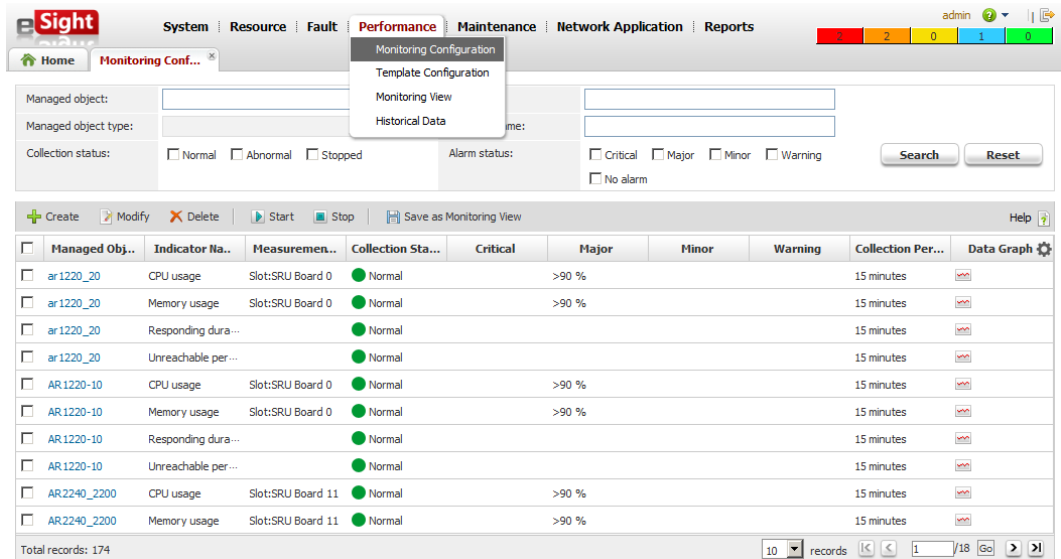
- Access the NE management window through the **Resource Management** entry.
1. Choose **Resource > Resource Management** from the main menu.

**Figure 6-26** Resource management



2. Choose **Equipment Resources > NE Resources**, click the NE name.
- Access the NE management window through the **Performance Management** entry.
1. Choose **Performance > Monitoring Configuration** from the main menu.

Figure 6-27 Monitoring configuration



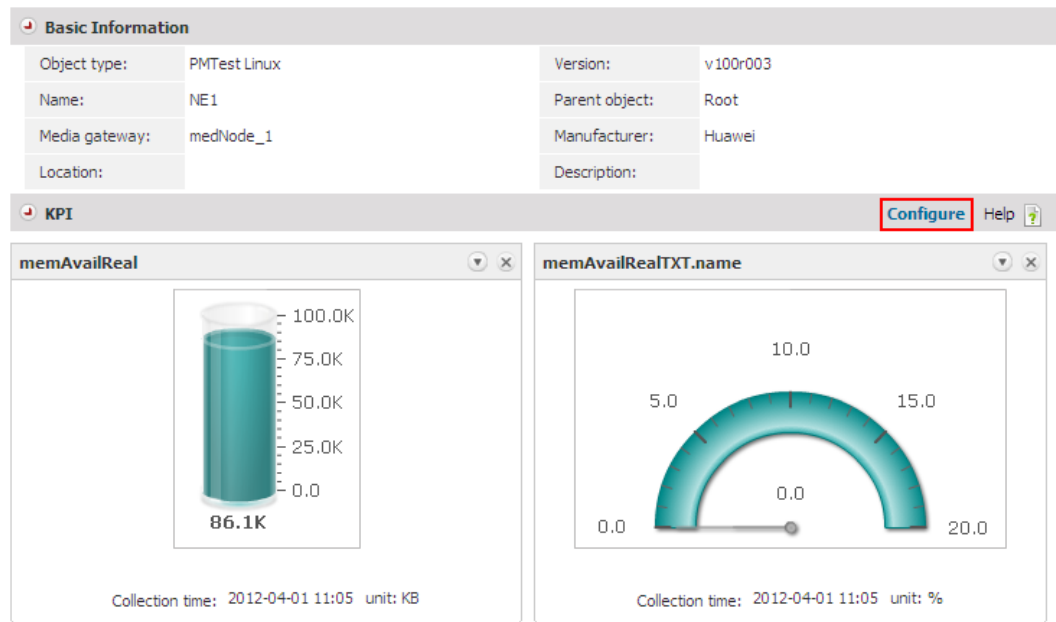
2. In the performance monitoring list of the **Monitoring Configuration** window, click the name of the target monitoring task in the **Managed Object** column.

Figure 6-28 NE management

| Managed Obj... | Indicator Na...    | Measuremen...     | Collection Sta... | Critical | Major | Minor | Warning | Collection Per... | Data Graph |
|----------------|--------------------|-------------------|-------------------|----------|-------|-------|---------|-------------------|------------|
| ar1220_20      | CPU usage          | Slot:SRU Board 0  | Normal            |          | >90 % |       |         | 15 minutes        |            |
| ar1220_20      | Memory usage       | Slot:SRU Board 0  | Normal            |          | >90 % |       |         | 15 minutes        |            |
| ar1220_20      | Responding dura... |                   | Normal            |          |       |       |         | 15 minutes        |            |
| ar1220_20      | Unreachable per... |                   | Normal            |          |       |       |         | 15 minutes        |            |
| AR1220-10      | CPU usage          | Slot:SRU Board 0  | Normal            |          | >90 % |       |         | 15 minutes        |            |
| AR1220-10      | Memory usage       | Slot:SRU Board 0  | Normal            |          | >90 % |       |         | 15 minutes        |            |
| AR1220-10      | Responding dur...  |                   | Normal            |          |       |       |         | 15 minutes        |            |
| AR1220-10      | Unreachable per... |                   | Normal            |          |       |       |         | 15 minutes        |            |
| AR2240_2200    | CPU usage          | Slot:SRU Board 11 | Normal            |          | >90 % |       |         | 15 minutes        |            |
| AR2240_2200    | Memory usage       | Slot:SRU Board 11 | Normal            |          | >90 % |       |         | 15 minutes        |            |

## Step 2 View the basic NE information and performance indicators.

1. On the **Basic Information** tab page, view the basic NE information and performance indicators.
2. Set the indicators to be displayed in a diagram.  
You can select a maximum of 20 indicators.
  - a. Click **Configure** in the row where the **KPI** title exists.

**Figure 6-29** Performance KPI

- b. In the **Configure** dialog box, select the indicator to be displayed in a diagram, and click **OK**.

**TIP**

- You can click  corresponding to the target indicator view to delete the diagram of the indicator.
- Click  corresponding to the target indicator view and select **Indicator Details**. On the **KPI Indicator Details** tab page, view indicator changes at different collection time points in the diagram of the indicator that is automatically displayed.
- If an indicator corresponding to multiple measurement objects, click  corresponding to the target indicator view and select **Measurement Object**. In the displayed window, add or delete measurement objects in the diagram.

**Step 3** Set NE monitoring.

1. Choose **Performance > Monitoring Configuration** from the main menu.
2. On the **Monitoring Configuration** tab page, you can manage monitoring tasks and save monitoring tasks in a performance monitoring view. For details, see [6.3.2 Creating a Performance Monitoring Task](#) and [6.3.3 Adding a Performance Monitoring View](#).

**Step 4** View indicator details.

1. In the navigation area of the NE management window, choose **Performance Status**, and view performance counter graphs.
2. On the **Performance Status** tab page, click  in the row where the target indicator title exists to display and view the performance indicator diagram.
3. Click  in the row where the target indicator title exists. In the **Select Measurement Objects** dialog box, select measurement objects. For details, see [Step 6 in 6.3.2 Creating a Performance Monitoring Task](#).

Indicator details of each measurement object is displayed as a curve in the performance view. Therefore, if there are multiple measurement objects, multiple curves are displayed.

4. Click  in the row where the target indicator title exists. In the **Modify Properties** dialog box, modify the collection period and threshold of the performance indicator. For details, see [Step 5](#) in [6.3.2 Creating a Performance Monitoring Task](#).

----End

## 6.5 Example: Typical Performance Management Operations

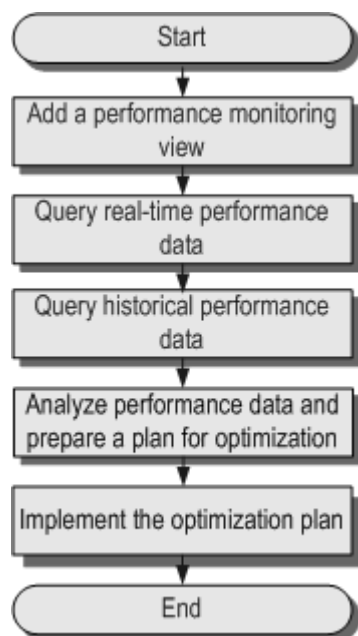
This topic describes an example about how to perform performance management operations. From the example, you will learn about the procedure and basic operations about performance management.

### Context

A maintenance engineer found that the service processing quality of device A was low and wants to check whether the performance of device A satisfies service running requirements. The engineer collected performance data of device A for analysis.

Before start, the engineer planned the procedure, as shown in [Figure 6-30](#).

**Figure 6-30** Procedure



### Procedure

- Step 1** Add the performance monitoring view of device A.



1. Choose **Performance > Monitoring View** from the main menu.
2. In the **Monitoring View** window, click **Add Monitoring View**.
3. In the **Add Monitoring View** dialog box, set the view name. In **Managed Object**, select device A.
4. In **Indicator Instances**, select the related performance indicator, and then click **OK**.

**Step 2** In the added performance monitoring view, view the real-time performance data of device A.

**Step 3** Query the historical performance data of device A.

1. Choose **Performance > Historical Data** from the main menu.
2. In the **Historical Data** window, click **Select Managed Object**.
3. In the **Select Managed Object** dialog box, select device A and click **OK**.
4. Set **Measurement unit** and **Time period**. Then click **Search**.

**Step 4** Analyze data and prepare a plan for optimization.

Check whether device A satisfies service running requirements based on the collected performance data. Then prepare a plan for optimization.

**Step 5** Carry out the plan.

----End

---

# 7 Report Management

---

## About This Chapter

eSight provides the report management function such as querying and collecting statistics on stock resource data, alarm resource data, service resource data, resource monitoring data, and system performance data on the entire network.

### [7.1 Overview of Report Management Operations](#)

The overview of report management operations helps to learn about report management operations. In the overview of report management operations, you are perform operations as required.

### [7.2 Setting the Report System Parameters](#)

Customers can customize configuration items such as the report storage area, logo and busy time configuration as required.

### [7.3 Creating a Report](#)

A user can create a report task to execute a report. After generated, the report is automatically saved to the storage area and may trigger email forward operation according to the configuration.

### [7.4 Viewing Reports](#)

After eSight generates a report according to the report task, you can view the report content as required to maintain the live network.

### [7.5 Viewing Quick Reports](#)

You can use quick reports to rapidly view statistics about a single counter of an object without creating tasks or preparing design files. This topic uses the number of terminals requesting association as an example to describe how to view quick reports.

### [7.6 Maintaining the Report System](#)

Periodically maintain the report system as required.

## 7.1 Overview of Report Management Operations

The overview of report management operations helps to learn about report management operations. In the overview of report management operations, you are perform operations as required.

Figure 7-1 shows the overview of report management operations. For details, click operations in the overview.

**Figure 7-1** Overview of report management operations

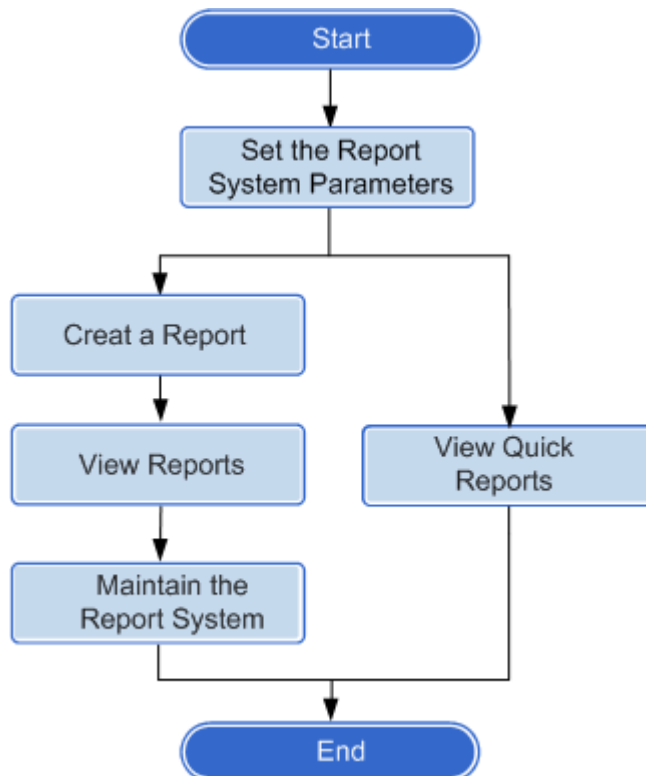


Table 7-1 describes the report management operations.

**Table 7-1** Report management operations

| Operation                                            | Description                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Setting the report system parameters</a> | eSight configures the report system by default. Customers can customize configuration items such as the report storage area, logo, and busy time configuration as required. <ul style="list-style-type: none"><li>• Configure the report storage area.</li><li>• Configure the logo of report customers.</li><li>• Configure the busy time.</li></ul> |
| <a href="#">Creating a report</a>                    | eSight generates reports based on report tasks, automatically stores periodical reports to the report storage area, and sends reports to customers by                                                                                                                                                                                                 |

| Operation                                     | Description                                                                                                                                                                                       |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | email.                                                                                                                                                                                            |
| <a href="#">Viewing reports</a>               | You can view report content.                                                                                                                                                                      |
| <a href="#">Viewing quick reports</a>         | You can use quick reports to rapidly view statistics about a single counter of an object without creating tasks or preparing design files.                                                        |
| <a href="#">Maintaining the report system</a> | You can maintain report tasks as follows: <ul style="list-style-type: none"><li>• Modifying a report task</li><li>• Managing report storage space</li><li>• Managing report task status</li></ul> |

## 7.2 Setting the Report System Parameters

Customers can customize configuration items such as the report storage area, logo and busy time configuration as required.

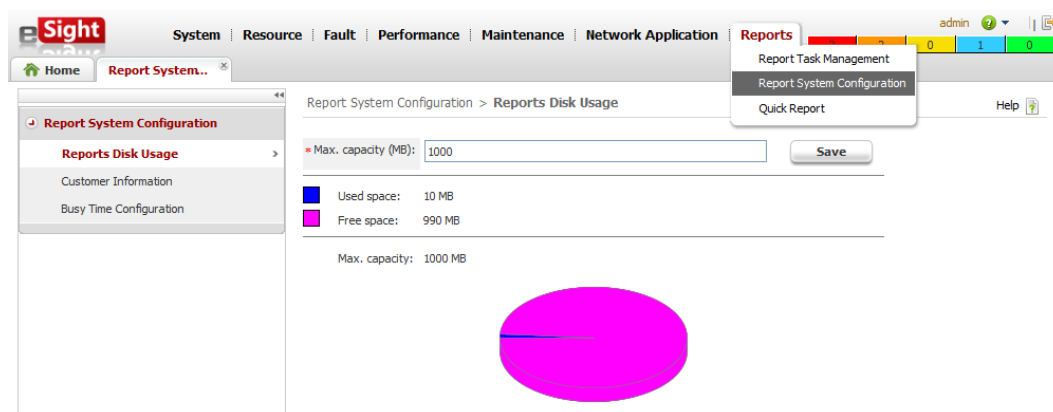
### 7.2.1 Setting the Busy Time Range

After the busy time range set, you can focus on reports in the busy time range.

#### Procedure

**Step 1** Choose **Reports > Report System Configuration** from the main menu.

**Figure 7-2** Report system configuration



**Step 2** In the navigation tree, choose **Report System Configuration > Busy Time Configuration**.

**Step 3** Select the busy time range and click **OK**.

**Figure 7-3** Busy time configuration

Report System Configuration > **Busy Time Configuration** Help ?

You can set the aggregation busy time range. The aggregation time is expressed in intervals. Each check box represents a time range of one hour.

|    |                                      |                                      |                                      |                                                 |                                                 |                                      |
|----|--------------------------------------|--------------------------------------|--------------------------------------|-------------------------------------------------|-------------------------------------------------|--------------------------------------|
| AM | <input type="checkbox"/> 00:00~01:00 | <input type="checkbox"/> 01:00~02:00 | <input type="checkbox"/> 02:00~03:00 | <input type="checkbox"/> 03:00~04:00            | <input type="checkbox"/> 04:00~05:00            | <input type="checkbox"/> 05:00~06:00 |
|    | <input type="checkbox"/> 06:00~07:00 | <input type="checkbox"/> 07:00~08:00 | <input type="checkbox"/> 08:00~09:00 | <input checked="" type="checkbox"/> 09:00~10:00 | <input checked="" type="checkbox"/> 10:00~11:00 | <input type="checkbox"/> 11:00~12:00 |
| PM | <input type="checkbox"/> 12:00~13:00 | <input type="checkbox"/> 13:00~14:00 | <input type="checkbox"/> 14:00~15:00 | <input checked="" type="checkbox"/> 15:00~16:00 | <input checked="" type="checkbox"/> 16:00~17:00 | <input type="checkbox"/> 17:00~18:00 |
|    | <input type="checkbox"/> 18:00~19:00 | <input type="checkbox"/> 19:00~20:00 | <input type="checkbox"/> 20:00~21:00 | <input type="checkbox"/> 21:00~22:00            | <input type="checkbox"/> 22:00~23:00            | <input type="checkbox"/> 23:00~00:00 |

**Step 4 Optional:** Click **Reset** to restore the latest configuration before the busy time range is set.

----End

## 7.2.2 Configuring the Report System

Configure the space of the report storage area and customer information by means of report system configuration.

### Procedure

**Step 1** Choose **Reports > Report System Configuration** from the main menu.

**Figure 7-4** Report system configuration

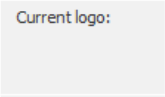
**Step 2** In the navigation tree on the left, choose **Configure Report System > Reports Disk Usage**. In the pane on the right, set the maximum value of the storage area and click **Save**.

You can view the usage of the storage area on the lower part of the window.

**Step 3** In the navigation tree on the left, choose **Configure Report System > Customer Information**. In the pane on the right, click to select the customer logo and click **Upload**.

**Figure 7-5** LOGO settings

Report System Configuration > Customer Information Help ?

Current logo: 

New logo:    Upload

Recommended logo resolution is 64 x 64 pixels. Max file size is 3 MB.

**TIP**

- If you select an improper picture but have not uploaded the picture, click  to clear the operation and reselect a picture.
- If you wish to replace an uploaded picture, select a new one and upload it.

----End

## 7.3 Creating a Report

A user can create a report task to execute a report. After generated, the report is automatically saved to the storage area and may trigger email forward operation according to the configuration.

### Procedure

**Step 1** Choose **Reports > Report Task Manager** from main menu.

**Figure 7-6** Report task manager

**Sight** System | Resource | Fault | Performance | Maintenance | Network Application | **Reports** admin ? 

[Home](#) **Report Task Ma...**

Type: All Status: All File category:  Task name:  File name:  Search

 Create  Delete Help ?

| <input type="checkbox"/> | Task name                         | File name                 | File category      | Type    | Status   | Latest execute ti...   | Next execution         | Operation                                                                                                                                                                                                                                                         |
|--------------------------|-----------------------------------|---------------------------|--------------------|---------|----------|------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | NE CPU Usage Report               | NE CPU Usage Report       | Performance report | Monthly | Enabled  |                        | 2012-09-01 04:00:00... |    |
| <input type="checkbox"/> | Interface Traffic Performance Rep | Interface Traffic Perf... | Performance report | Monthly | Enabled  |                        | 2012-09-01 04:00:00... |    |
| <input type="checkbox"/> | Link Connection Report            | Link Connection Report    | Alarm report       | Instant | Complete | 2012-08-10 15:59:59... |                        |    |

Total records: 3 20 records 1/1 Go

**Step 2** Click **Create** and select a design file.

**Figure 7-7** Selecting a design file

Report Task Management > Create Task Help ?

Select a file Set task parameters

File category:  File name:

|                                  | File name                                 | Type       | File category      | Description                                                               | Operation |
|----------------------------------|-------------------------------------------|------------|--------------------|---------------------------------------------------------------------------|-----------|
| <input checked="" type="radio"/> | NE CPU Usage Report                       | Predefined | Performance report | Max. and average NE CPU usage in a time segment                           |           |
| <input type="radio"/>            | TopN NE CPU Usage Report                  | Predefined | Performance report | TOP-N Max. and Avg. NE CPU usage in a time segment                        |           |
| <input type="radio"/>            | NE Memory Usage Report                    | Predefined | Performance report | Max. and average NE memory usage in a time segment                        |           |
| <input type="radio"/>            | TopN NE Memory Usage Report               | Predefined | Performance report | TOP-N Max. and Avg. NE memory usage in a time segment                     |           |
| <input type="radio"/>            | Interface Traffic Performance Report      | Predefined | Performance report | Interface rate and bandwidth usage in a time segment                      |           |
| <input type="radio"/>            | TopN Interface Traffic Performance Report | Predefined | Performance report | TOP-N Interface rate and bandwidth usage in a time segment                |           |
| <input type="radio"/>            | Device Alarm Severity Report              | Predefined | Alarm report       | Distribution of critical, major, minor, and warning NE alarms in a tim... |           |
| <input type="radio"/>            | TopN Device Alarm Severity Report         | Predefined | Alarm report       | TOP-N Distribution of critical, major, minor, and warning NE alarms i...  |           |
| <input type="radio"/>            | Interface Connection Report               | Predefined | Alarm report       | Number of times each interface is disconnected in a time segment          |           |
| <input type="radio"/>            | NE Connection Report                      | Predefined | Alarm report       | Number of times each NE is disconnected in a time segment                 |           |

Total records: 34 10 records < 1 / 4 >

**TIP**

When multiple design files are available, you can set **File category** or **File name** and click **Search**. The necessary files are displayed in the list on the lower part of the window.

Click **Upload file**. In the window that is displayed, set the information on the custom design file and click **OK**. Upload the custom design file.

**NOTE**

- If the selected design file type is performance report, you must perform the operation of [6.3.2 Creating a Performance Monitoring Task](#).

**Step 3** Click **Next** and set the following parameters as required.

**Figure 7-8** Parameter setting

Report Task Management > Create Task Help ?

Select a file Set task parameters

**Enter Task Information**

File category: Performance report

File name: NE CPU Usage Report

\* Task name: NE CPU Usage Report

\* Type: Generate a report on statistics of recent 1 month or last month at the specified time every month.

☐ Instant ☒ Periodical,  generate on the  day of each month.

Statistical period:  ☐ Busy

Timezone:

☐ Send email

**Table 7-2** Parameter Description

| Parameter | Description                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type      | <ul style="list-style-type: none"><li>Instant: Create an instant report. An instant report is generated when an instant task is created and executed manually.</li><li>Periodical: Create a periodical report. A periodical report is generated according to the period set in the task created.</li></ul> |

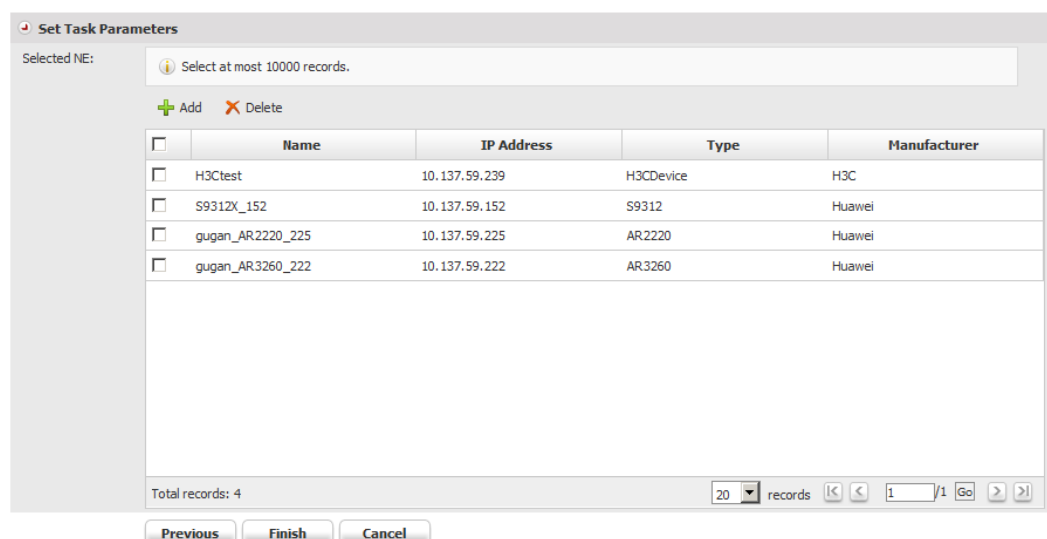
| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <p><b>NOTE</b></p> <p>By default, eSight generates reports at 04:00 every day. You can change the time for generating periodical reports in the <b>eSight server installation directory</b>\AppBase\bin\runtime.center\config\report\report_conf.xml file. Then you must restart eSight for the change to take effect.</p> <p>If the configured date where reports are generated does not exist, eSight generates reports in the last day of the current month. Take a monthly report as an example. If the configured date is the 31th day, June 30 is the date during which reports are generated in June.</p> |
| Statistical period | <p>You can set the statistical period of the periodical report in either of the following ways:</p> <p>Take a monthly report as an example. The report is generated on May 11, 2011. If the statistical period is set to <b>Recent 1 month</b>, data from April 11, 2011 to May 10, 2011 is collected. If the statistical period is set to <b>Last month</b>, data from April 1, 2011 to April 30, 2011 is collected.</p> <p>Select <b>Busy</b>. eSight displays data only in the busy time range during the statistics period.</p>                                                                              |
| Timezone           | Set the timezone for generating periodical reports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Step 4 Optional:** Select **Send email** to set parameters related to email forward. A report is sent to a user.

**Step 5** Set the task parameters and click **Finish**.

The values of the parameters vary with the design file.

**Figure 7-9** Set the task parameters



----End



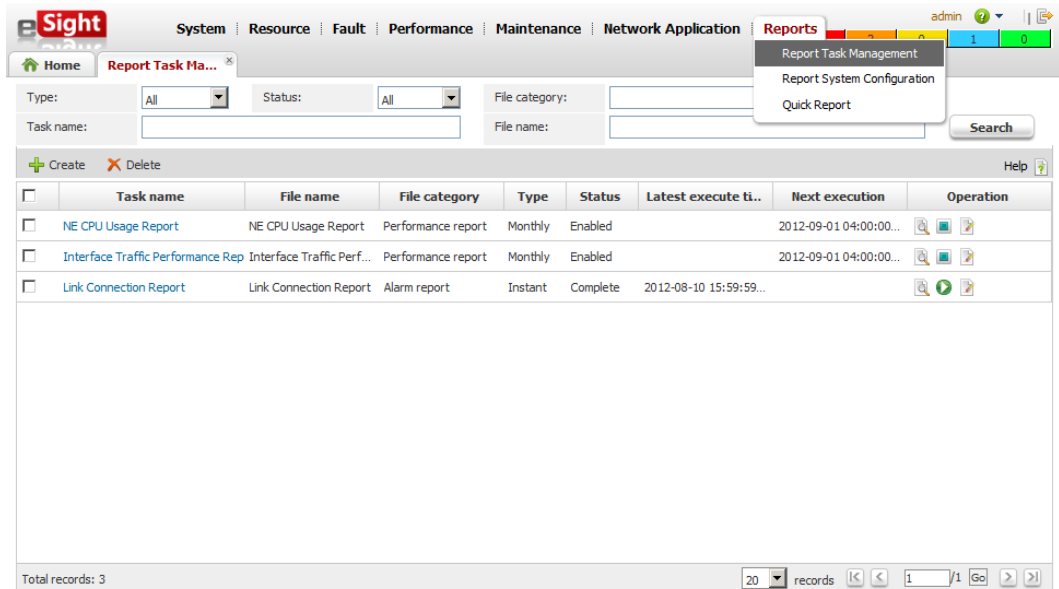
## 7.4 Viewing Reports

After eSight generates a report according to the report task, you can view the report content as required to maintain the live network.

### Procedure

**Step 1** Choose **Reports** > **Report Task Manager** from main menu.

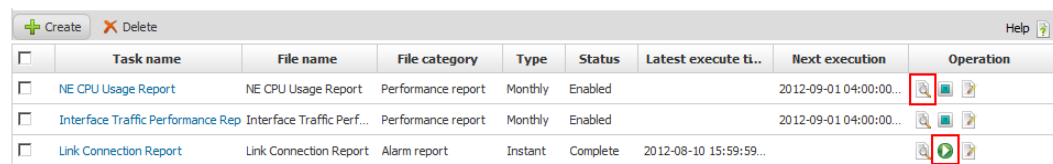
**Figure 7-10** Report task manager



**Step 2** View reports.

- For a periodical report, click  after the report. In the window that is displayed, you can view the report information.
- For an instant report
  - Optional:** Click  to execute the task immediately.
  - Click  after the report. In the window that is displayed, you can view the report information.

**Figure 7-11** Viewing reports



----End

## 7.5 Viewing Quick Reports

You can use quick reports to rapidly view statistics about a single counter of an object without creating tasks or preparing design files. This topic uses the number of terminals requesting association as an example to describe how to view quick reports.

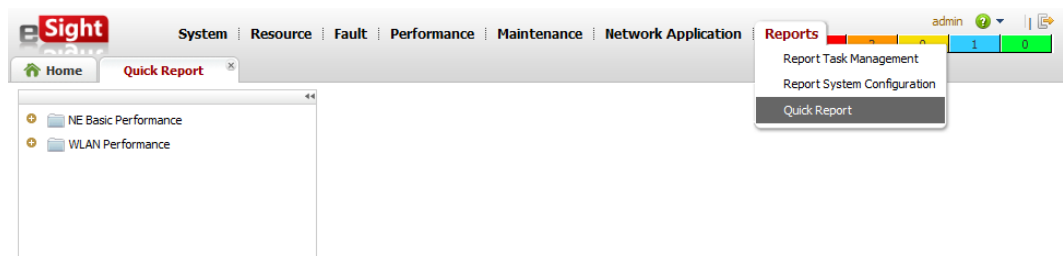
### Prerequisites

You have performed the operation of [6.3.2 Creating a Performance Monitoring Task](#).

### Procedure

**Step 1** Choose **Reports > Quick Report**.

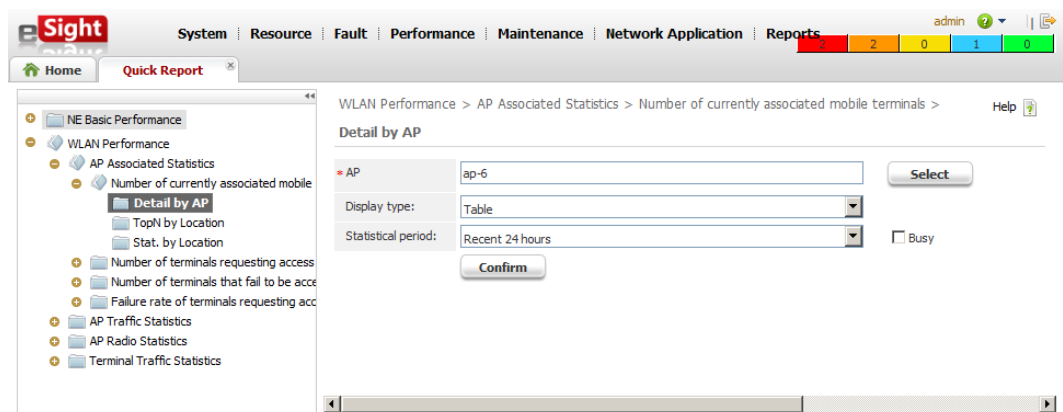
Figure 7-12 Quick report



**Step 2** Collect statistics on mobile terminals that request to be associated.

- Collect statistics on mobile terminals that request to be associated with an AP.
1. In the navigation tree, choose **WLAN Performance > AP Associated Statistics > Number of currently associated mobile terminals > Detail by AP**.

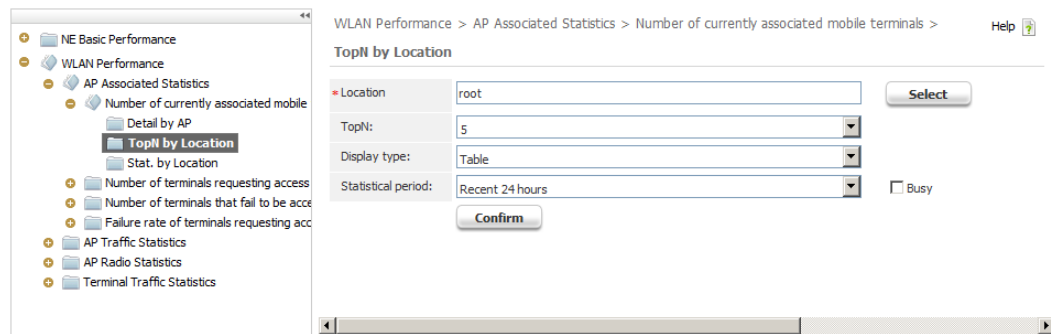
Figure 7-13 Detail by AP



2. Set the Top-N, display type, and statistics period.
3. **Optional:** Select **Busy**. eSight displays data only in the busy time range during the statistics period.
4. Click **Confirm**.

- Collect statistics on mobile terminals that request to be associated with APs in a region.
1. In the navigation tree, choose **WLAN Performance > AP Associated Statistics > Number of currently associated mobile terminals > TopN by Location**.

**Figure 7-14** TopN by Location



2. Set the location, TopN, display type, and statistics period.
3. **Optional:** Select **Busy**. eSight displays data only in the busy time range during the statistics period.
4. Click **Confirm**.

**Step 3** Perform either of the following operation on the report generation page.

- Click **Refresh** to refresh the report.
  - Click **Export** and select the format to export the report.
  - Click **Chart Type** and select the report type to display the report.
  - Set the statistical range.
1. Set the time range.
  2. Set the statistical range.
  3. **Optional:** If **Busy** is selected, eSight displays only data in the busy time range of **Stat Period**.
  4. Click **Confirm**.

**Figure 7-15** Report generation page

WLAN Performance > AP Associated Statistics > Number of currently associated mobile terminals > [Help](#) 

**Detail by AP**

---

 Refresh  Export  Chart Type [Back](#)

◀ 2012-08-03 16:39:58 ~ 2012-08-10 16:39:57 ▶

Statistical period: Recent 7 days ☐ Busy

| AC Name | Measurement Object | Max.Value(Entries) | Occurred At              |
|---------|--------------------|--------------------|--------------------------|
| WLAN_58 | ap-6               | 0                  | 2012-08-10 11:45:00 UT.. |
| WLAN_58 | ap-6               | 0                  | 2012-08-10 12:45:00 UT.. |
| WLAN_58 | ap-6               | 0                  | 2012-08-10 13:45:00 UT.. |
| WLAN_58 | ap-6               | 0                  | 2012-08-10 14:45:00 UT.. |
| WLAN_58 | ap-6               | 0                  | 2012-08-10 15:45:00 UT.. |

----End

## 7.6 Maintaining the Report System

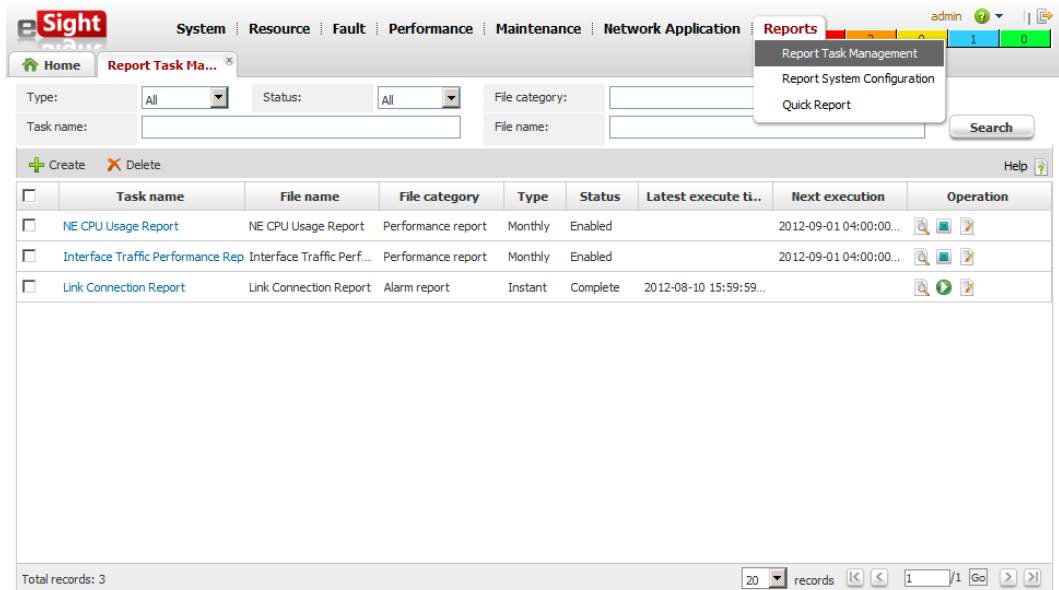
Periodically maintain the report system as required.

### 7.6.1 Modifying a Report Task

Modify a report task as required.

#### Procedure

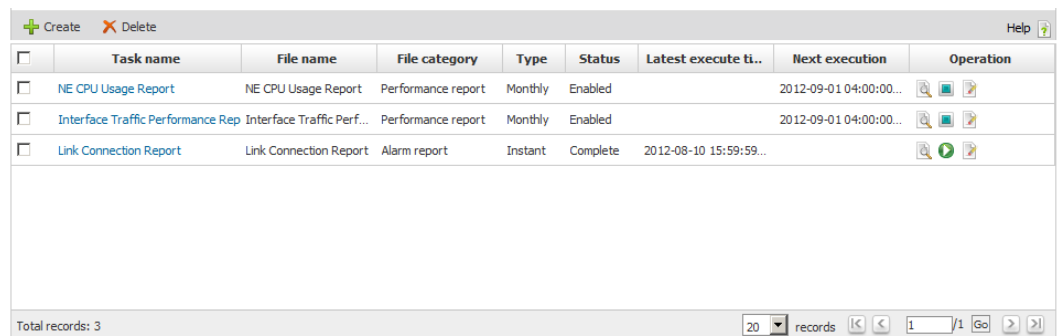
**Step 1** Choose **Reports > Report Task Manager** from main menu.

**Figure 7-16** Report task manager

**Step 2 Optional:** Set the filter conditions of report tasks on the upper part of the window and click **Search** to filter required report tasks.

**Step 3** In **Operation** column, click .

**Step 4** In the **Modify Task** window, modify parameters of the report tasks.

**Figure 7-17** Modifying task

**Step 5** Click **Save**.

----End

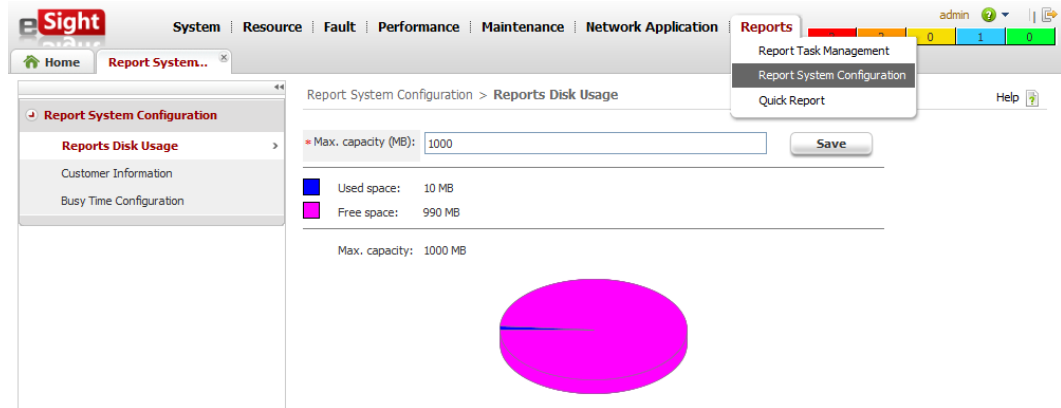
## 7.6.2 Managing Report Storage Space

When the report storage area is full, you should periodically clear the reports in the storage area to release the space.

## Procedure

**Step 1** Choose **Reports > Report System Configuration** from the main menu.

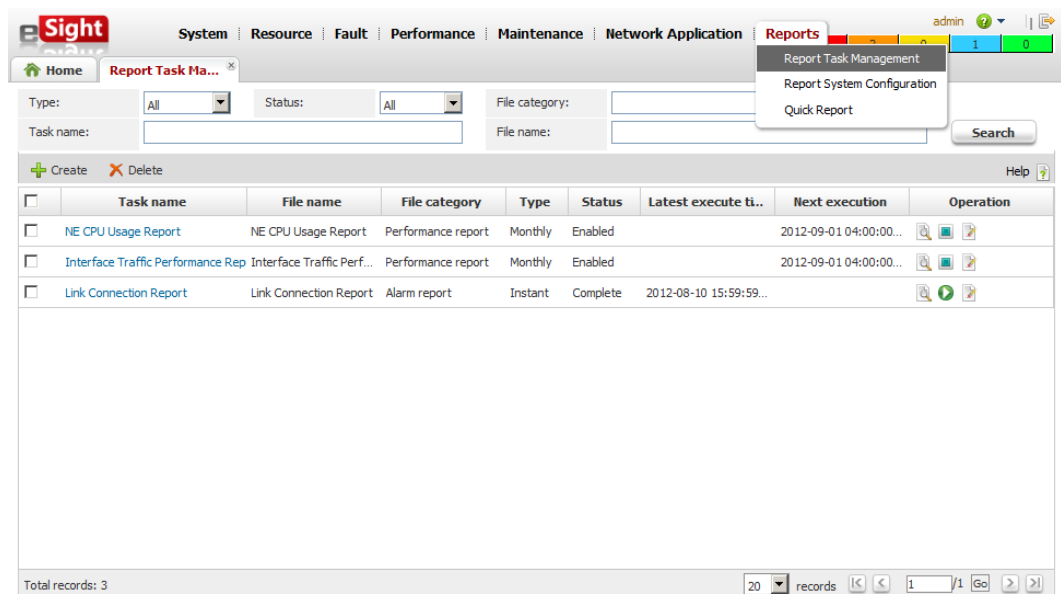
**Figure 7-18** Report system configuration



**Step 2** Select **Reports Disk Usage**, modify **Max.capacity(MB)**, and click **Save**.

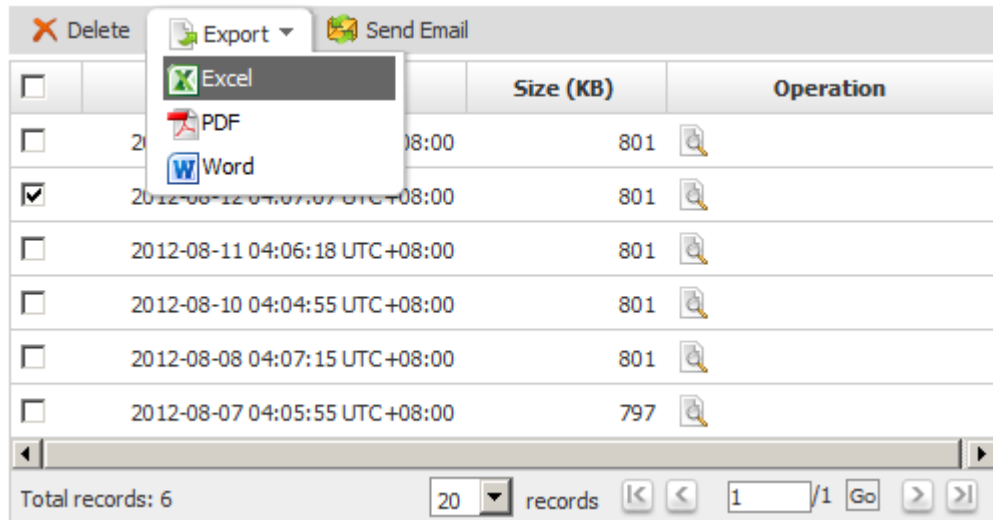
**Step 3** Choose **Reports > Report Task Manager** from main menu.

**Figure 7-19** Report task manager



**Step 4** Export a periodical report.

1. Click .
2. Select the reports to be cleared.
3. Click **Export**, and select the file format of the reports to be exported.

**Figure 7-20** Exporting reports

4. In the window that is displayed, click **OK**.

**NOTE**

An instant report is not saved in the database.

For an instant report, click . In the window that is displayed, click **Export** to export the report.

Reports exported in Excel contain no figures.

- Step 5** Click **Delete** as required to delete the reports in the storage area.

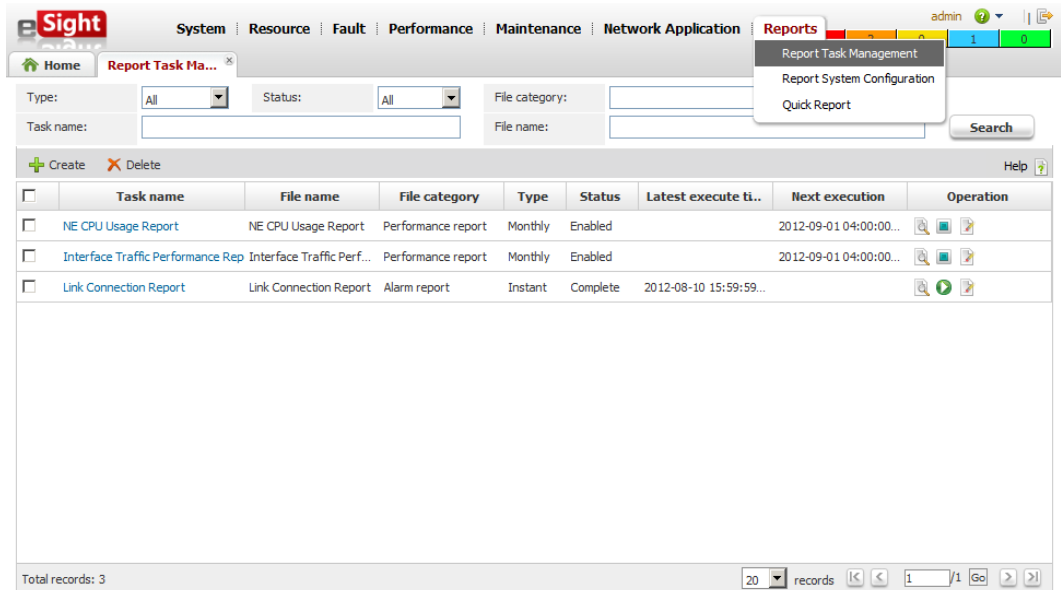
----End

## 7.6.3 Managing Report Task Status

Periodically maintain the report system as required.

### Procedure

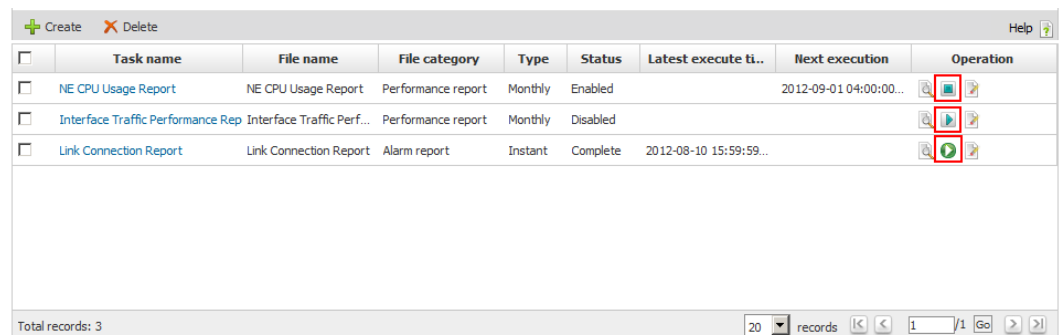
- Step 1** Choose **Reports** > **Report Task Manager** from main menu.

**Figure 7-21** Report Task Manager

**Step 2 Optional:** Set the filter conditions of report tasks on the upper part of the window and click **Search** to filter required report tasks.

**Step 3** View the status information of reports and perform the following operations as required:

- For a periodical report task, click  to enable the task.
- For a periodical report task, click  to disable the task.
- For an instant report task, click  to execute the task immediately.

**Figure 7-22** Managing task status

----End



# 8 NE Management

## About This Chapter

eSight provides the functions such as managing basic device information, viewing device panels, managing device interface information, and viewing IP addresses.

### 8.1 Overview of NE Management Operations

This topic describes the NE management operations.

### 8.2 Querying an NE

This topic describes how to monitor an NE by querying the basic information, panels, and alarm and performance of the NE.

### 8.3 Configuring an NE

NE configuration includes the NE configuration method, protocol parameters, interfaces, and restoration of the NE configuration file.

## 8.1 Overview of NE Management Operations

This topic describes the NE management operations.

### Background

Before performing NE management operations, you must understand basic NE concepts. For details, see [1.2.7 Basic Concepts of Ne Management](#).

### Overview of NE Management Operations

[Figure 8-1](#) shows the overview of NE management operations. For more details, click the operation in the overview.

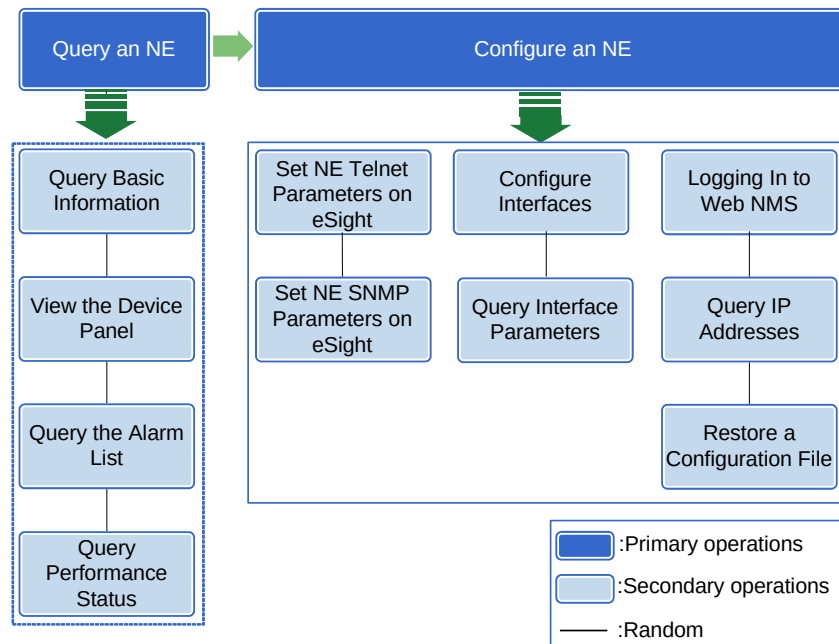
**Figure 8-1** Overview of NE management operations

Table 8-1 describes the NE management operations.

**Table 8-1** Operation description

| Operation                              | Description                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Querying Basic Information             | Queries basic NE information.                                                                                                                  |
| Viewing the Device Panel               | Views slot, board, sub-board, and port parameters on the device panel.                                                                         |
| Querying the Alarm List                | Queries the current alarm information.                                                                                                         |
| Querying Performance Status            | Queries performance data.                                                                                                                      |
| Setting NE Telnet Parameters on eSight | Sets the NE Telnet parameters concurrently on eSight when eSight and an NE communicate over Telnet and the Telnet parameters on the NE change. |
| Setting NE SNMP Parameters on eSight   | Set the NE SNMP parameters concurrently on eSight when eSight and an NE communicate over SNMP and the SNMP parameters on the NE change.        |
| Configuring Interfaces                 | Activates and deactivates interfaces and changes interface aliases.                                                                            |
| Querying Interface Parameters          | Queries interface information including the interface index, description, IP address, type, status, rate, and alias.                           |
| Logging In to Web                      | The eSight provides the link to the web NMS so that you can                                                                                    |

| Operation                      | Description                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------|
| NMS                            | configure the NE conveniently.                                                           |
| Querying IP Addresses          | Queries NE and interface IP addresses during service configuration and network planning. |
| Restoring a Configuration File | Restores an NE configuration file that is corrupted.                                     |

## 8.2 Querying an NE

This topic describes how to monitor an NE by querying the basic information, panels, and alarm and performance of the NE.

### 8.2.1 Querying Basic Information

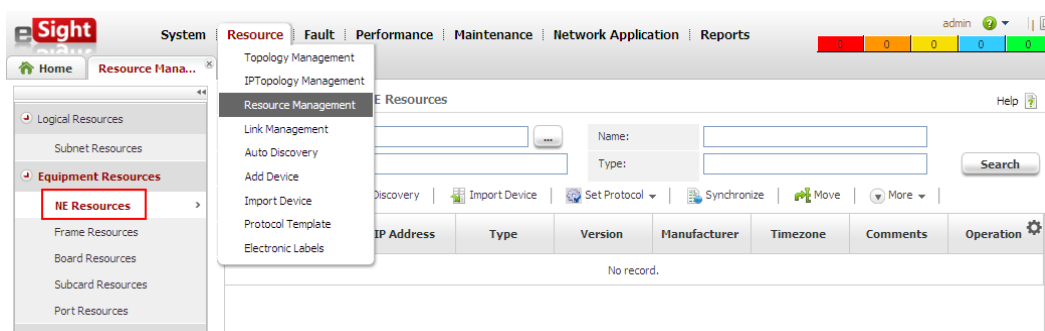
This topic describes how to view basic information about NEs.

#### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-2** Resource Management



**Step 2** Query the basic information of the NE in the **Basic Information** pane on the right.

**Figure 8-3** NE Basic Information

|                                                          |                   |                  |                                 |
|----------------------------------------------------------|-------------------|------------------|---------------------------------|
| Basic Information                                        |                   | Help             |                                 |
| Modify Refresh Telnet Ping Trace Synchronize Device Data |                   |                  |                                 |
| Name:                                                    | S9303_3           | Device location: | nanjing                         |
| Model:                                                   | Switch/S9303      | Version:         | VRP5.11 V200R001C00             |
| Host name:                                               | S9303_3           | System OID:      | 1.3.6.1.4.1.2011.2.170.1        |
| IP address:                                              | 10.137.59.3       | Execute at:      | 10days10hours37minutes56seconds |
| MAC address:                                             | 00-25-9E-16-BC-9F | Last polled at:  | 2012-04-24 02:30:15             |
| KPI                                                      |                   | Configure        | Help                            |
| TOP 10 Alarms                                            |                   |                  |                                 |
| Interface Flow                                           |                   |                  |                                 |

In the pane, you can perform the following operations:

- Click **Modify**. In the window that is displayed, modify the NE basic information and click **OK**.

**NOTE**

If the NE information fails to be modified, the possible causes are as follows: The parameter value length exceeds the maximum allowed by the NE; the SNMP parameters are set incorrectly.

- Click **Refresh**. eSight synchronizes the basic information of the NE and refresh the NE state.
- Click **Telnet** to log in to the device.  
Configure the Telnet parameters before performing this step. For details, see [8.3.2.1 Setting NE Telnet Parameters on eSight](#).
- Click **Ping**. In the window that is displayed, set the ping information. After you click **Ping**, the test result is displayed in the **Ping** window when the ping test is complete. The ping test is intended to verify the connectivity between eSight and the device.
- Click **Trace**. In the displayed dialog box, view the test result. The trace test is intended to verify the connectivity between eSight and the device and trace the route information.
- Click **Synchronize Device Data** to synchronize device data to eSight. In the window that is displayed, you can view the detailed information of the synchronized device.
- In the **KPI** pane, you can view the key performance information of the NE.
- In the **TOP 10 Alarms** pane, you can view the top 10 alarms of the NE.
- In the **Interface Flow** pane, you can view the interface traffic volume of the NE.

----End

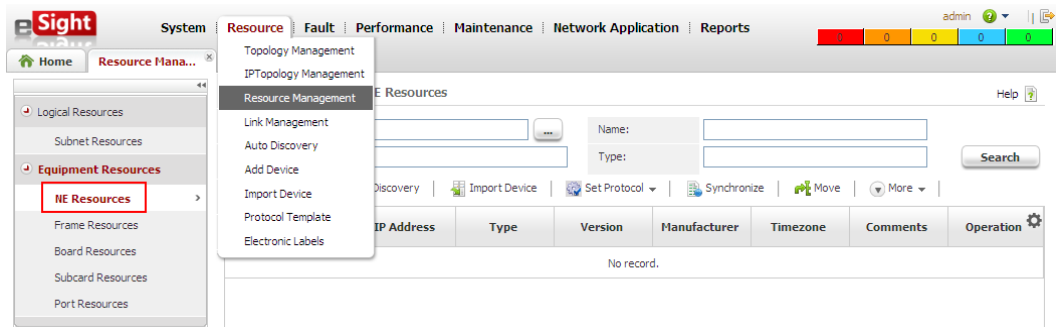
## 8.2.2 Viewing the Device Panel

This topic describes how to view the slot, board, subcard, and port parameters on the device panel.

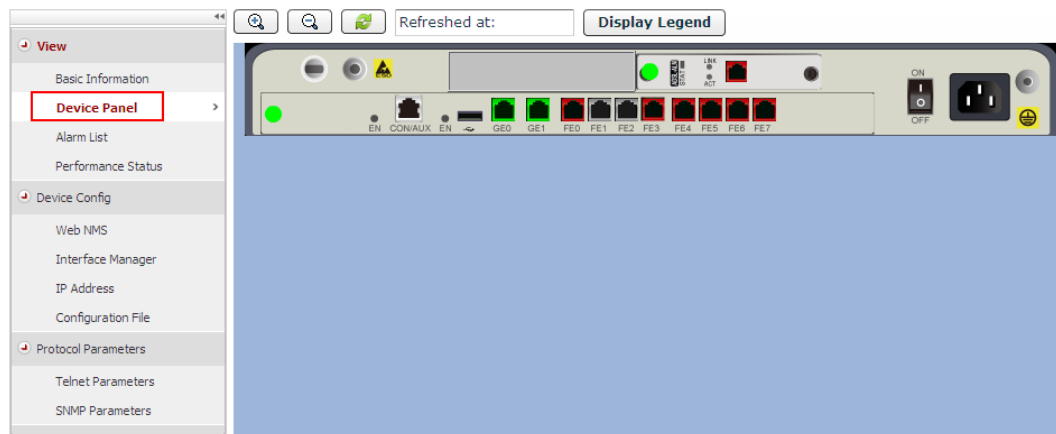
### Procedure

- Step 1** Access the NE manager page.

1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

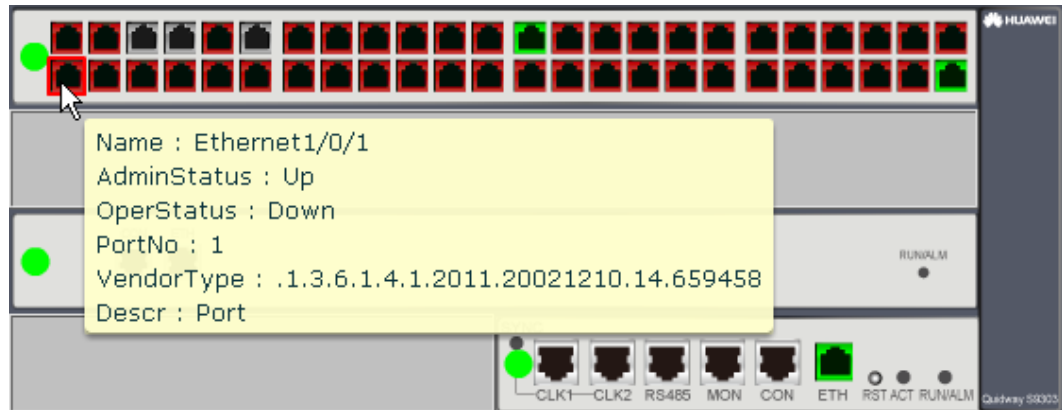
**Figure 8-4** Resource Management

**Step 2** In the navigation tree on the left, choose **View** > **Device Panel**.

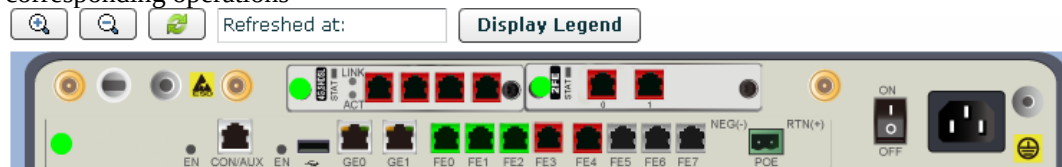
**Figure 8-5** Device Panel

**Step 3** Move the cursor to a board, subcard, or port. eSight displays the parameter information of the board, subcard, or port.

**Figure 8-6** Displaying information



**Step 4 Optional:** Click **Zoom In**, **Zoom Out**, **Refresh**, or **Display Legend** to implement corresponding operations



**Step 5 Optional:** Right-click on the device panel, the following shortcut menus are displayed:

- **Create New Style:** Draw a picture to customize a device panel. For details, see [13.6.4 Customizing the Device Panel](#).
- **Bind Style:** Bind a created device panel with an NE.

**Figure 8-7** Shortcut Menus



----End

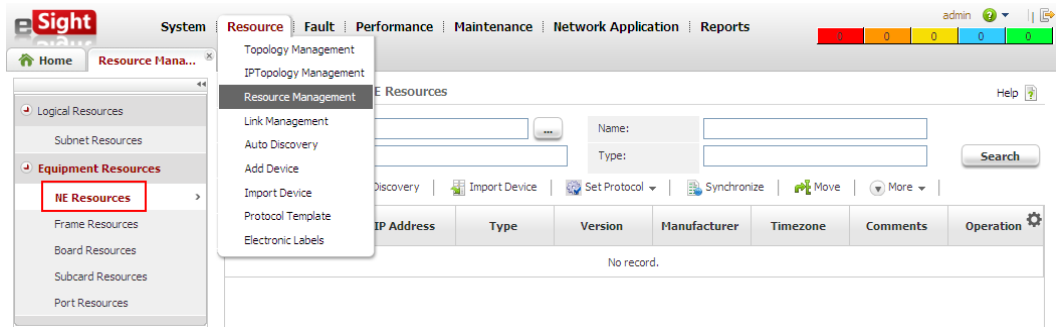
## 8.2.3 Querying the Alarm List

This topic describes how to view the NE alarm list to know the current alarm information.

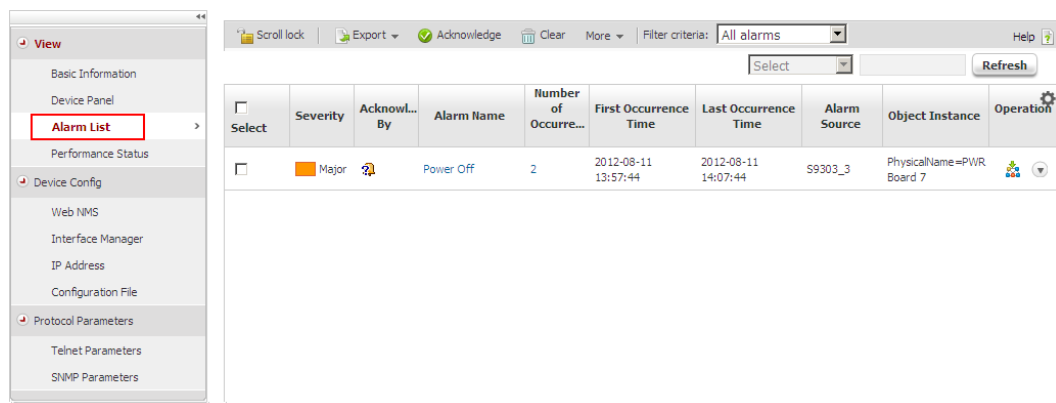
### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-8** Resource Management

**Step 2** In the navigation tree on the left, choose **View > Alarm List**.

**Figure 8-9** Alarm List

**Step 3** In the **Alarm List** window, you can perform the following steps:

**Table 8-2** Operations in Current Alarms window

| Operation Name | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lock           | <p>Click <b>Scroll Lock</b>. The alarms in the current list are locked.</p> <p>If the alarms in the current list are locked, note that:</p> <ul style="list-style-type: none"> <li>Newly reported alarms can be displayed in the current alarm list only after you click <b>Scroll Unlock</b>.</li> <li>When an alarm is available, you can perform operations such as acknowledging or clearing the alarm, or viewing details about the alarm. When an alarm is unavailable, you cannot perform any operations on the alarm.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>If you acknowledge or clear an alarm when you click <b>Scroll Lock</b>, the alarm can be updated to the historical alarm list only when you click <b>Scroll Unlock</b>.</li> <li>If an alarm is available, you can select the alarm.</li> <li>If an alarm is unavailable, you cannot select the alarm because the check box is dimmed.</li> </ul> |

| Operation Name | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unlock         | Click <b>Scroll Unlock</b> . The eSight reports alarms to the alarm list automatically.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Search         | You can perform a search by using either of the following methods: <ul style="list-style-type: none"><li>Click <b>Refresh</b> without setting any search criteria. All alarms are displayed in the current list.</li><li>Select a search scope from <b>Search in</b> when the window is locked, and click <b>Search</b>.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Acknowledge    | Select one or more alarms and click <b>Acknowledge</b> .<br><b>NOTE</b> <ul style="list-style-type: none"><li>If the alarm is acknowledged, <b>Acknowledge User</b> displays the user who acknowledges the alarm.</li><li>If the alarm is unacknowledged, <b>Acknowledge User</b> displays .</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Unacknowledge  | Select one or more alarms and choose <b>More &gt; Unacknowledge</b> .<br><b>NOTE</b> <p>After an alarm is unacknowledged, its status is changed from Acknowledged to Unacknowledged.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Clear          | Select one or more uncleared alarms and click <b>Clear</b> .<br><b>NOTE</b> <ul style="list-style-type: none"><li>The background color of cleared alarms is green.</li><li>The background color of uncleared alarms is white.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Alarm Mask     | <ol style="list-style-type: none"><li>Select an alarm. Then click  in the <b>Operation</b> column and choose  <b>Shield Alarms</b>.</li><li>In the <b>Alarm Mask</b> dialog box, set the rule name, shielding time, masking time, and location information. Click <b>OK</b>.</li></ol><br><b>NOTE</b> <ul style="list-style-type: none"><li>In the current alarm window, the newly created alarm mask rule is in enabled status by default.</li><li>A masking rule is valid only to the alarms reported when the masking rule is enabled and valid. The masking rule does not take effect for the alarms reported before the masking rule is configured.</li><li>You cannot set a mask rule for a performance alarm or cleared alarm.</li></ul> |
| Locate to Topo | Select an alarm and click  .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Alarm Details  | Select an alarm and click <b>Alarm Name</b> .<br>The <b>Alarm Details</b> dialog box displays the name, cause, and solution for the selected alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



| Operation Name | Operation Method                                                                                                                                                               |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarm Logs     | Select an alarm and click <b>Number of Repetitions</b> .<br>The <b>Alarm Logs</b> dialog box displays the alarm log related to this alarm record.                              |
| Export         | Select one or more alarms and choose <b>Export &gt; Selected Records</b> to export the alarm information.<br>If you want to export all alarms, choose <b>Export &gt; All</b> . |

----End

## 8.2.4 Querying Performance Status

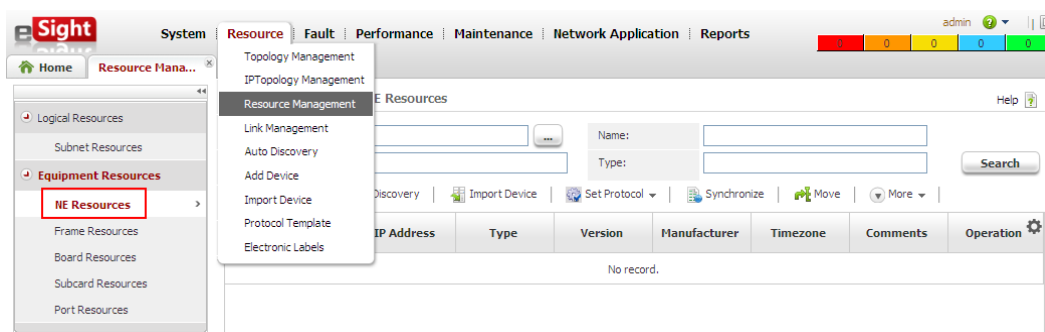
This topic describes how to view NE performance status to know the current performance information.

### Procedure

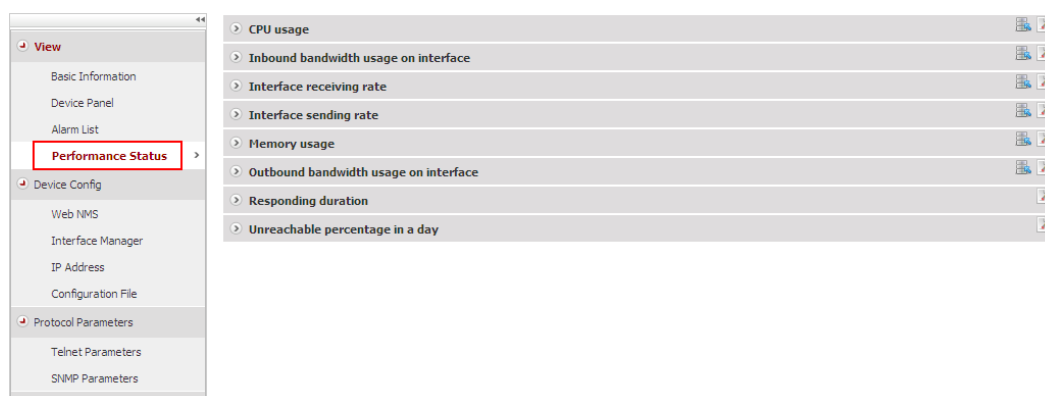
**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-10** Resource Management



**Step 2** In the navigation tree on the left, choose **View > Performance Status**.

**Figure 8-11** Performance Status

**Step 3 Optional:** Click  on the right of a performance title to customize the performance attributes.

----End

## 8.3 Configuring an NE

NE configuration includes the NE configuration method, protocol parameters, interfaces, and restoration of the NE configuration file.

### 8.3.1 Logging In to Web NMS

The eSight provides the link to the web NMS so that you can configure the NE conveniently.

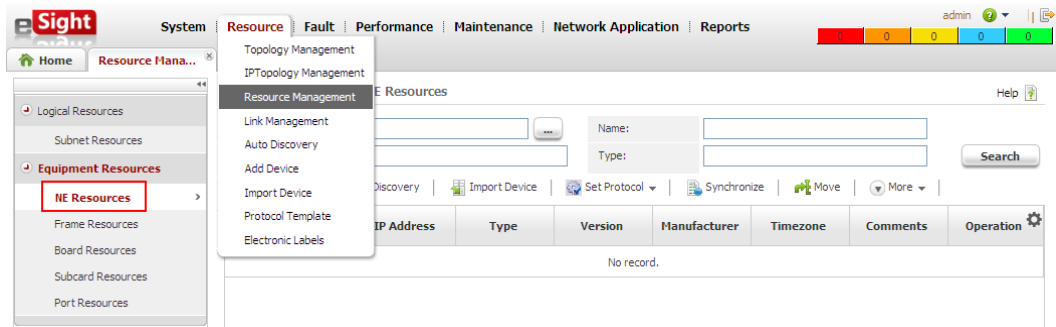
#### Prerequisites

The NE support web NMS.

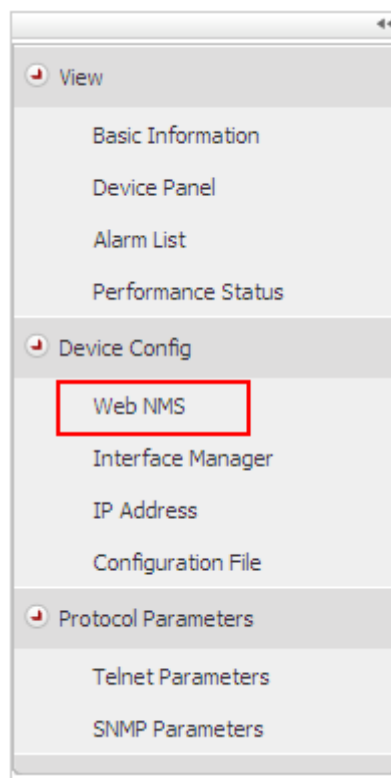
#### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-12 Resource Management**

**Step 2** In the navigation tree on the left, choose **Config > Web NMS**.

**Figure 8-13 Web NMS**

----End

### 8.3.2 Setting Protocol Parameters

To implement normal communication between eSight and an NE, you should set the protocol parameters of eSight.

### 8.3.2.1 Setting NE Telnet Parameters on eSight

When eSight and an NE communicate over Telnet and the Telnet parameters on the NE change, you must set the NE Telnet parameters concurrently on eSight.

#### Prerequisites

The Telnet parameters on eSight and NE are the same.

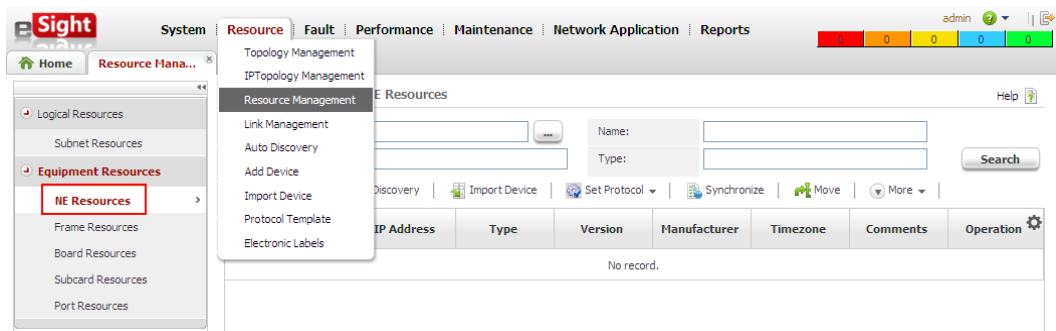
A device is added to eSight.

#### Procedure

**Step 1** Access the NE manager page.

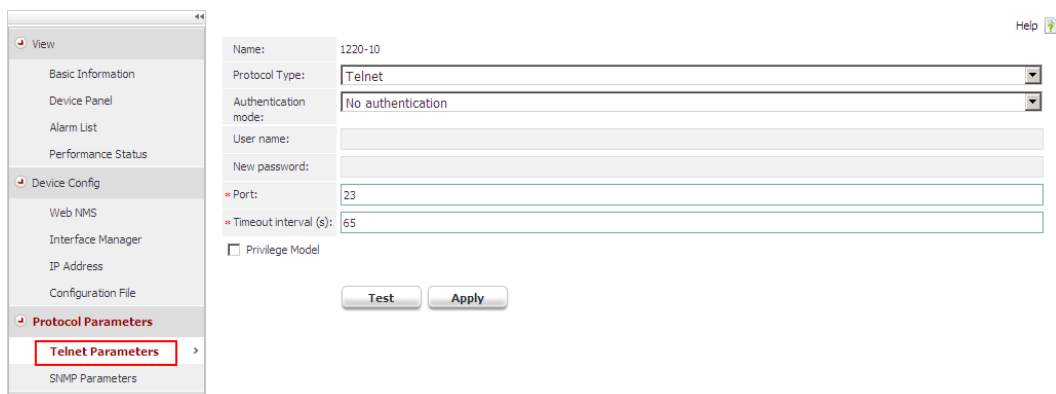
1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-14** Resource Management



**Step 2** In the navigation tree on the left, choose **Protocol Parameters** > **Telnet Parameters**.

**Figure 8-15** Telnet Parameters



**Step 3** On the right of the window, set the Telnet parameters.

- Protocol type: The value can be Telnet or STelnet. STelnet is used in scenarios demanding high security.
- Authentication mode: authentication mode used by eSight to access network elements.
- Port: communication port. BY default, the Telnet port number is 23 and the STelnet port number is 22.
- Timeout interval (s): period for waiting for a response after eSight sends a request to a network element.
- Privilege model: right for eSight to deliver commands to network elements. When you select **Privilege model** and log in to a network element using Telnet or STelnet, eSight switches to the corresponding privilege model.
- Privilege level: A larger value indicates a higher priority. Users can use only the commands at the same or lower level than their own levels.

**NOTE**

Currently, the privilege model can only be set on Huawei devices.

**Figure 8-16** Setting Telnet parameters

|                         |           |
|-------------------------|-----------|
| Name:                   | S9303_3   |
| Protocol Type:          | Telnet    |
| Authentication mode:    | Password  |
| User name:              | client001 |
| * Password:             | *****     |
| * Port:                 | 23        |
| * Timeout interval (s): | 60        |

TestApply

**Step 4** Click **Test**.

**Step 5** After the test, click **Apply**.

----End

### 8.3.2.2 Setting NE SNMP Parameters on eSight

When eSight and an NE communicate over SNMP and the SNMP parameters on the NE change, you must set the NE SNMP parameters concurrently on eSight.

#### Prerequisites

The SNMP parameters on eSight and the NE are the same.

A device is added to eSight.

## Context

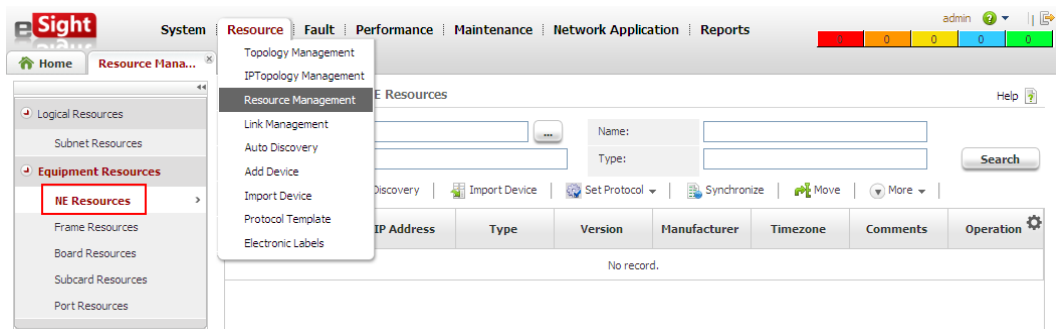
eSight accesses a managed NE over SNMP. When you manually create an SNMP NE or an SNMP NE is automatically created, eSight adapts a specified NE by using the default SNMP profile to determine the SNMP parameters supported by the managed NE. If adaptation is successful, the default profile is the SNMP parameters for the NE configured on eSight. The operations on the NE must be based on the SNMP parameters. When the SNMP parameters for NE access change, the SNMP parameters for a specified NE must be changed accordingly.

## Procedure

**Step 1** Access the NE manager page.

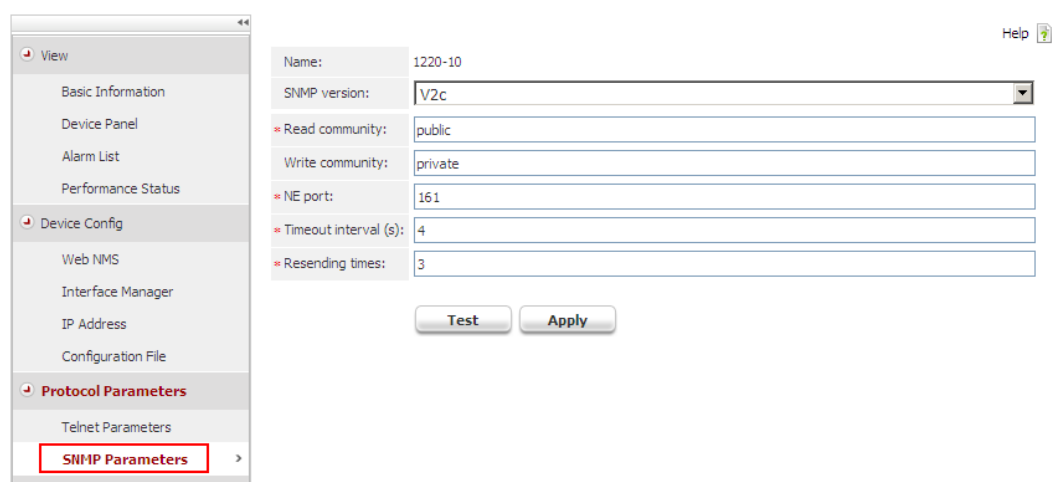
1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-17** Resource Management



**Step 2** In the navigation tree on the left, choose **Protocol Parameters** > **SNMP Parameters**.

**Figure 8-18** SNMP Parameters



**Step 3** On the right of the window, set the SNMP parameters.

- **SNMP version:** Currently, the SNMPv1, SNMPv2c, and SNMPv3 versions are supported. The SNMPv3 version is applied in the scenario requiring high parameter security level.
- **Read community:** The read community name for eSight to send a read request to an NE. The read operation is available when the read community name is the same as that acknowledged by the NE.
- **Write community:** The write community name for eSight to send a write request to an NE. The write operation is available when the write community name is the same as that acknowledged by the NE.
- **Timeout interval(s):** The time when eSight waits for a response for an operation request.
- **Resending times:** The maximum number of times for eSight to resend an operation requests when eSight configures SNMP parameters for an NE in the case that the timer expires. If the actual number of times exceeds this value, operation fails.
- **NE port:** SNMP communication port of the NE.
- **Security name:** NE user name used for accessing the NE.
- **Context name:** Name of the environment engine.
- **Context engine ID:** Uniquely identifies an SNMP engine. The ID must be used with the environment name to uniquely identify an SNMP entity environment. An SNMP packet is processed only when the transmit environment and the receive environment are matching. Otherwise, the SNMP packet is discarded.
- **Authentication protocol:** A protocol used for message verification. You can choose the HMACMD5 or HMACSHA protocol or do not use any protocol. When you use the HMACMD5 or HMACSHA protocol, you must set an authentication password.
- **Privacy protocol:** Encryption protocol used for data encapsulation. You can choose the DES or AES encryption protocol or do not use encryption. When you use the DES or AES encryption protocol, you must set an encryption password.

**Step 4** Click **Test**.

**Step 5** After the test, click **Apply**.

----End

## 8.3.3 Managing Interfaces

To manage a device, a user must know the basic information and state of the interfaces on the device.

### 8.3.3.1 Understanding an Interface

This topic describes important parameters related to an interface.

| Attribute         | Description                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Rate(bit/s)       | Processing rate of the data packet passing through an interface.                                                                        |
| If Admin Status   | Physical state of an interface. Whether a user disables the interface.                                                                  |
| If Operate Status | Logical state of an interface, the integration of the management state and protocol state of an interface. When either of the states is |

| Attribute | Description                                       |
|-----------|---------------------------------------------------|
|           | down, the running state of the interface is down. |

### 8.3.3.2 Configuring Interfaces

This topic describes how to activate, deactivate an interface, and modify the alias of the interface.

#### Prerequisites

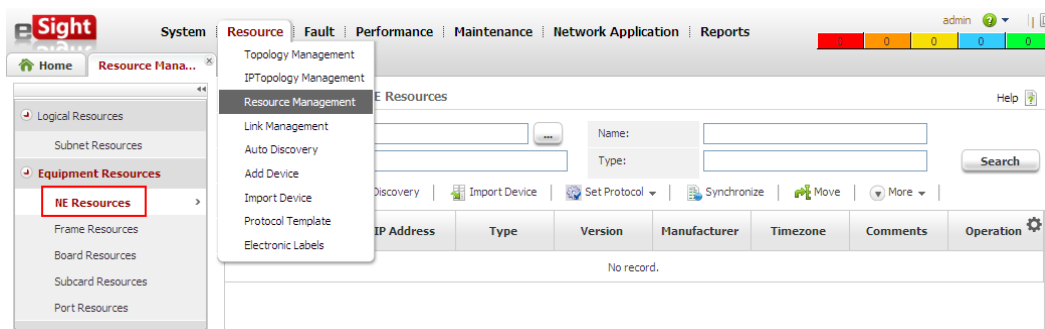
SNMP write permission is set.

#### Procedure

**Step 1** Access the NE manager page.

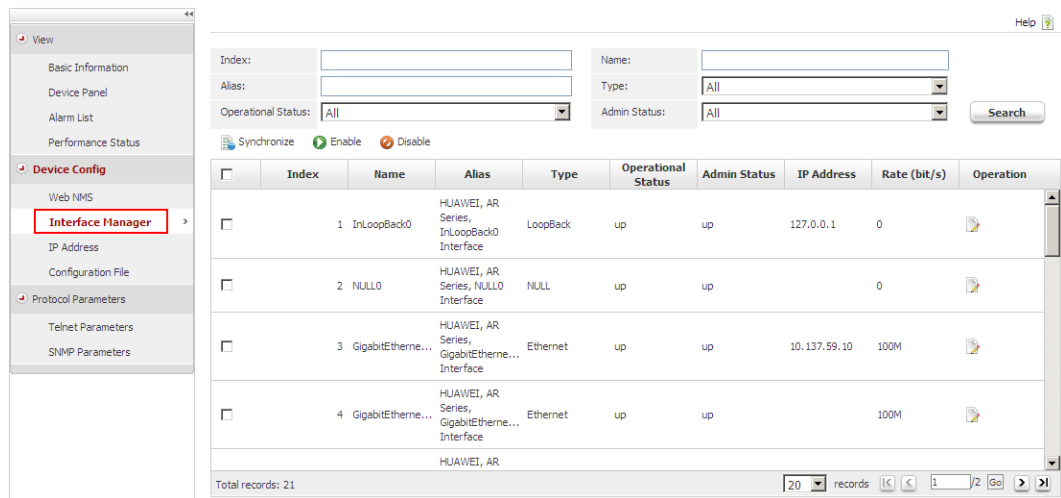
1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-19** Resource Management

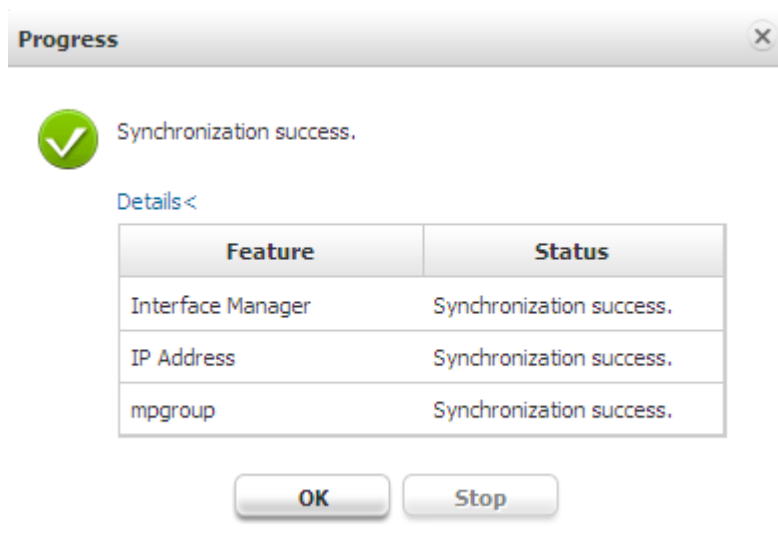


**Step 2** In the navigation tree on the left, choose **Device Config** > **Interface Manager**.



**Figure 8-20** Interface Manager

**Step 3** Click **Synchronize**. The **Progress** dialog box is displayed. After the synchronization task is complete, click **OK**.

**Figure 8-21** Progress

**Step 4** Click  to set parameters related to an interface.

**Figure 8-22 Parameters**

|                     |                                          |
|---------------------|------------------------------------------|
| Index:              | 1                                        |
| Name:               | InLoopBack0                              |
| Alias:              | HUAWEI, AR Series, InLoopBack0 Interface |
| Type:               | LoopBack                                 |
| MTU:                | 1500                                     |
| Operational Status: | up                                       |
| Admin Status:       | up                                       |
| IP Address:         | 127.0.0.1                                |
| Rate (bit/s):       | 0                                        |

OK Cancel

**NOTE**

The interface alias is mandatory for some NEs.

**Step 5** Select multiple interfaces, and click **Enable**, **Disable**, **Enable Alarm Shielding**, or **Disable Alarm Shielding** to implement operations in batches.

**NOTE**

If an interface is configured with disabling alarm reporting, the interface does not report alarms monitored by the interface to eSight.

Only switches of the S series support the enabling and disabling of alarm reporting.

----End

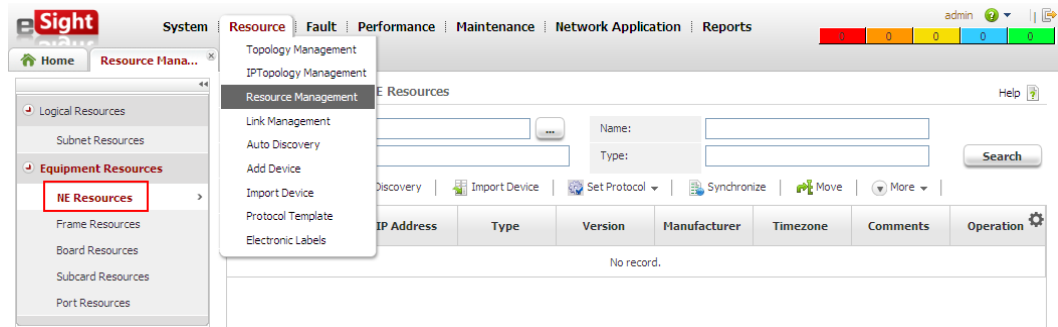
### 8.3.3.3 Querying Interface Parameters

eSight allows users to query interface information.

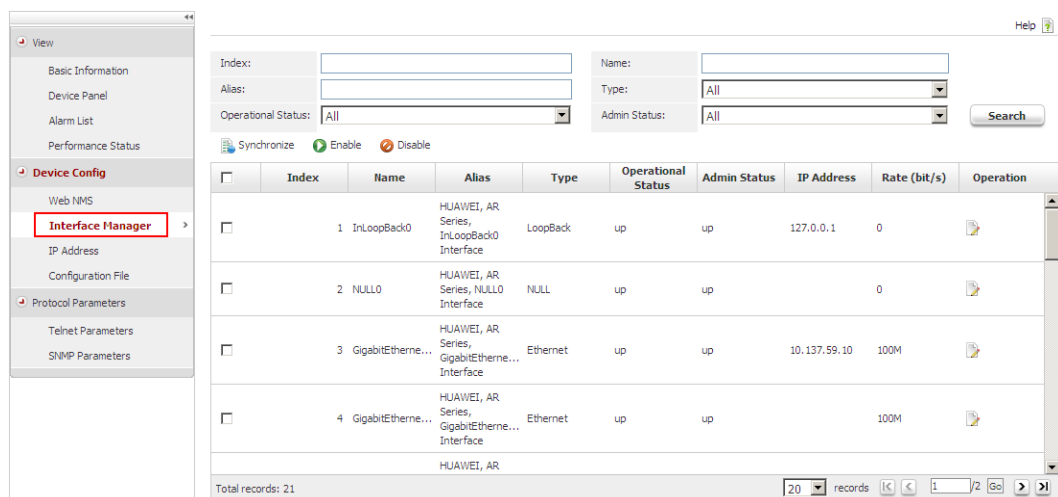
#### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-23 Resource Management**

**Step 2** In the navigation tree on the left, choose **Device Config** > **Interface Manager**.

**Figure 8-24 Interface Manager**

**Step 3** Set filter parameters at the top of the pane and click **Search**.

**Step 4** On the lower part of the right pane of the window, view the interface parameters.

----End

### 8.3.4 Querying IP Addresses

When performing service configuration and network planning, you must query the IP addresses of an NE and the interface. eSight supports query of IP addresses of an NE and the interface.

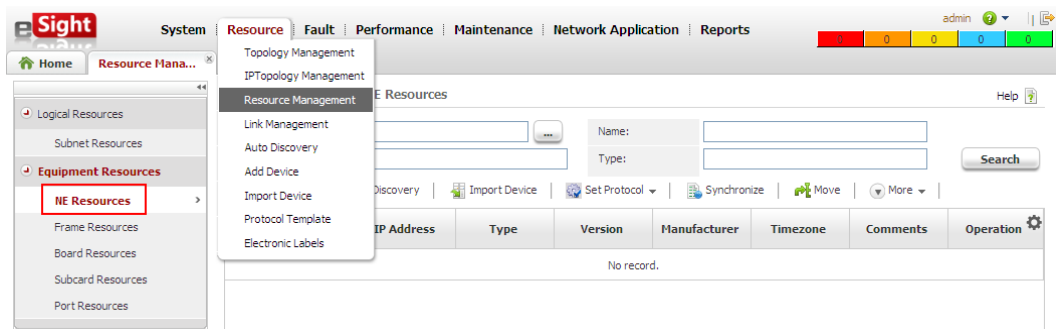
#### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.

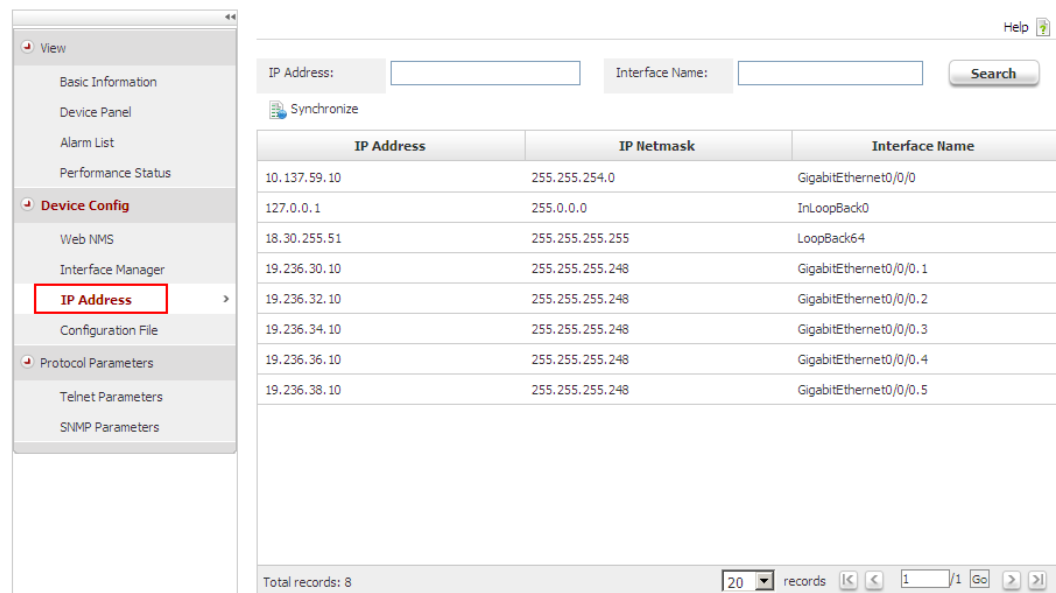
3. Click the NE name.

**Figure 8-25 Resource Management**

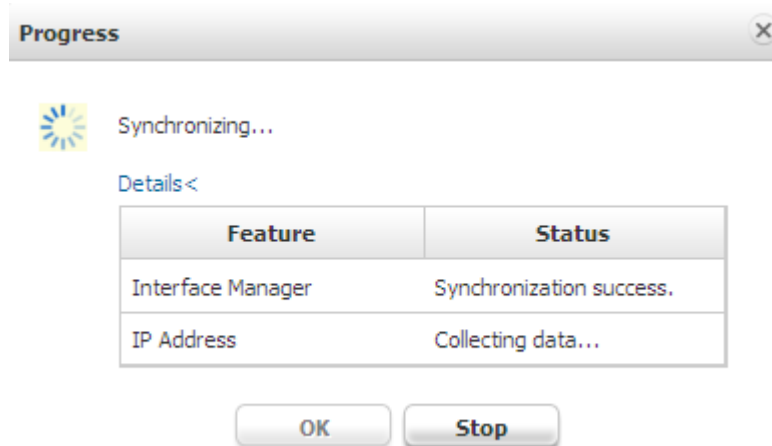


**Step 2** In the navigation tree on the left, choose **Device Config > IP Address**.

**Figure 8-26 IP Address**



**Step 3** Click **Synchronize**. After the synchronization, in the displayed **Progress** window, view the detailed information, and click **OK** to synchronize the IP address of the NE to eSight.

**Figure 8-27** Progress

**Step 4** Set filter parameters at the top of the pane and click **Search**. On the lower part of the right pane of the window, view the IP address parameters of the interface.

----End

## 8.3.5 Restoring a Configuration File

eSight supports restoration of the configuration file of an NE. When data in the configuration file is corrupted, you can protect the file by means of data restoration.

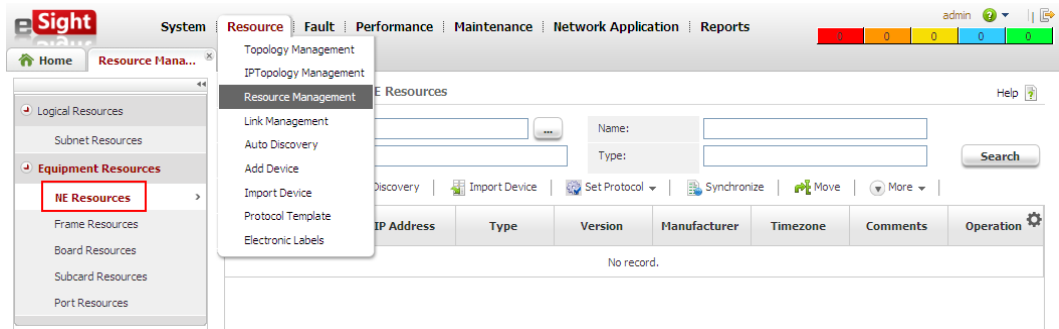
### Prerequisites

SNMP write permission is set.

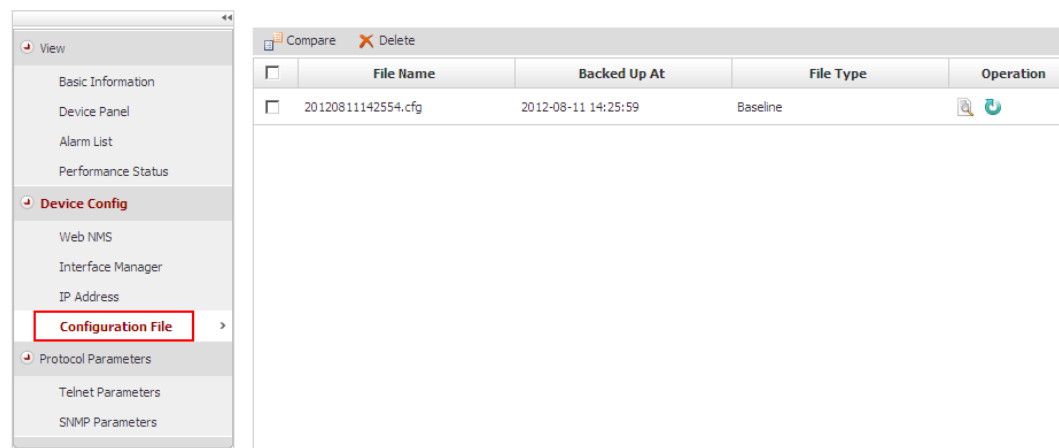
### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 8-28 Resource Management**

**Step 2** In the navigation tree on the left, choose **Device Config** > **Configuration File**.

**Figure 8-29 Configuration File**

**Step 3** Click  in **Operation**.

----End

## Follow-up Procedure

Backing Up NE Configuration Files, refer to [12.3.2 Backing Up NE Configuration Files Manually](#).

---

# 9 Network Traffic Analysis

---

## About This Chapter

The eSight NTA management tools provide a reliable and an efficient traffic analysis solution. NTA monitors the whole network traffic and provides multidimensional traffic analysis reports. It helps users detect traffic exceptions in a timely manner and know network bandwidth usage and traffic distribution. The eSight NTA allows visual traffic management, timely fault location, and reasonable network planning.

### 9.1 NTA Panorama

This topic describes the NTA operations. You can perform the operations based on the actual requirements.

### 9.2 NTA Overview

eSight network traffic analyzer (NTA) allows devices to monitor whole network traffic without using hardware probes, which reduces user investment. eSight NTA collects and analyzes NetFlow, NetStream, and sFLOW packets and provides analysis reports that meet customer requirements. eSight NTA is a good choice for enterprises to monitor the whole network traffic in real time.

### 9.3 NTA Overview and Configuration Prerequisites

eSight NTA provides a method to quickly monitor and analyze network traffic. It analyzes the whole network traffic based on information provided by network devices that support the NetFlow, NetStream, and sFLOW technologies, and provides traffic analysis reports in real time. eSight NTA shows analysis reports in various types of graphs, to allow users to quickly detect abnormal traffic and know the traffic distribution on the network.

### 9.4 Monitoring Network Traffic

NTA provides a dashboard and traffic analysis functions. It analyzes and displays network traffic from multiple dimensions to locate network fault in a timely manner.

### 9.5 Creating a Traffic Report

You can create traffic report tasks to generate traffic reports. In this way, you can obtain network traffic statistics. This ensures guaranteed bandwidth for key services.

### 9.6 Creating Traffic Forensics Tasks

You can create traffic forensics tasks to view traffic data in detail. This helps locate network fault.

## 9.7 Configuring NTA

This section describes how NTA collects traffic from monitored objects.

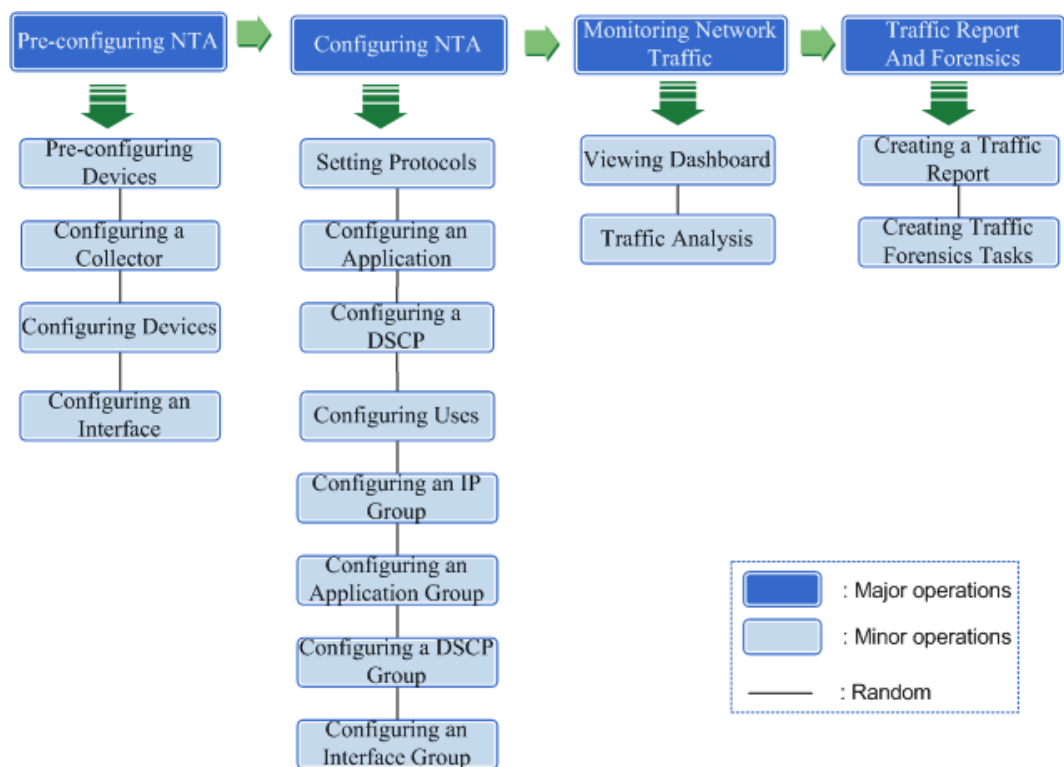
# 9.1 NTA Panorama

This topic describes the NTA operations. You can perform the operations based on the actual requirements.

Figure 9-1 shows the NTA panorama. For more details, click the operation in the overview.

## Overview of NTA Management Operations

Figure 9-1 Overview of NTA management operations



## 9.2 NTA Overview

eSight network traffic analyzer (NTA) allows devices to monitor whole network traffic without using hardware probes, which reduces user investment. eSight NTA collects and analyzes NetFlow, NetStream, and sFLOW packets and provides analysis reports that meet customer requirements. eSight NTA is a good choice for enterprises to monitor the whole network traffic in real time.



**Table 9-1** Basic concepts

| Concept   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDE       | Network data exporter (NDE) is a network device that supports the Flow technology including Netstream, Netflow, and sFlow. An NDE can be a Huawei or H3C router or switch, or a Cisco switch. NDE classifies packets coming into and going out of each port based on a traffic classifier and exports packets in packages.                                                                                                                                                                                                                                          |
| NTC       | Network traffic collector (NTC) collects packets from multiple NDEs, provides traffic listening, package parsing, and raw packet statistics functions, and forwards the aggregated packets to NMC.                                                                                                                                                                                                                                                                                                                                                                  |
| NMC       | Network management console (NMC) provides network traffic analysis, report analysis and network linkage management to fulfill centralized storage, data extraction, and analysis of network traffic. Based on the B/S architecture, NMC allows users to view graphical and explicit analysis results on the management analysis page using a Web browser.                                                                                                                                                                                                           |
| NetStream | NetStream is a technology of collecting and releasing statistics about network traffic. It classifies the statistics about traffic flows and resource usage on the network. NetStream also manages the network and conducts charging based on types of services and QoS. Based on the destination IP address, source IP address, destination port number, source port number, protocol number, Type of Service (ToS), and inbound and outbound interfaces of packets, NetStream identifies different streams and collects independent statistics for these streams. |
| sFlow     | Sampled Flow (sFlow) is a traffic monitoring technology that collects and analyzes traffic statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| DSCP      | Differentiate Services Code Point (DSCP) uses the ToS field in the IP header of each data packet to identify service priority. The ToS field consists of six standard bytes and two user-defined bytes.                                                                                                                                                                                                                                                                                                                                                             |

## 9.3 NTA Overview and Configuration Prerequisites

eSight NTA provides a method to quickly monitor and analyze network traffic. It analyzes the whole network traffic based on information provided by network devices that support the NetFlow, NetStream, and sFLOW technologies, and provides traffic analysis reports in real time. eSight NTA shows analysis reports in various types of graphs, to allow users to quickly detect abnormal traffic and know the traffic distribution on the network.

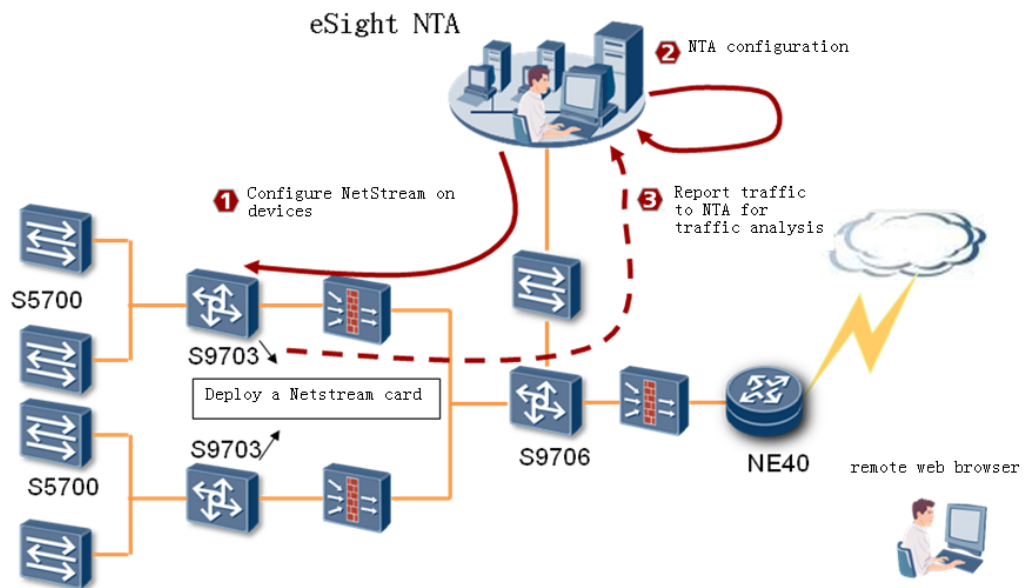
### NTA Features

- **Visible traffic:** NTA provides real time traffic monitoring and displays traffic trends, so that administrators can find and process abnormality in time.
- **Fault location:** The network traffic analyzer component analyzes the raw flows to facilitate the administrators to perform traffic auditing.
- **Reasonable planning:** NTA provides the trend analysis and user-defined report functions to offer reference for network capacity planning.

## NTA Solution

**Figure 9-2** NTA management process

eSight NTA collects and analyzes traffic information sent by NDEs to monitor the whole network traffic. Users can deploy NTCs on routers at the aggregation layer, core layer or the egress. After the configuration is complete, traffic logs on NDEs are sent to eSight NTA, analyzed by NTA, and summarized to the database. After the data is summarized, NTA analyzes the traffic on interfaces, hosts, of sessions, applications, and protocols, and shows the result to users.



shows the detailed process. On a typical campus network, traffic on different layers can be monitored separately. You can deploy NTCs on different positions to meet different monitoring requirements. For example, NTCs can be deployed on an Internet egress to monitor users' online behaviors. NTCs can be deployed on a DMZ ingress to identify users (internal users or external users). NTCs can be deployed at the core layer to monitor important services and applications. NTCs can be deployed at the aggregation layer to monitor the bandwidth usage of a specified branch.

### Prerequisites:

To use NTA to manage networks, complete the following tasks:

- Configuring an IP address to which network traffic is exported: **ip netstream export source ip-address**



#### NOTE

The NetStream-enabled NMS identifies the source of NetStream data according to the source IP address of NetStream flows. The **ip netstream export source** command is used to configure the source IP address for the output NetStream flows. The IP address of LoopBack interface is suggested.

- Configuring an IP address for the NTC: **ip netstream export host ip-address port-number**

**NOTE**

The NDE samples data traffic and sends the sampled data to the NSC for further processing. The **ip netstream export host** command configures the IP address of the NSC as the destination IP address of the sampled data to be output by the NDE.

- Configuring an interval at which an active flow times out: **ip netstream timeout active active-interval**

**NOTE**

Indicates the active aging time of NetStream original flows. When the active time of a flow (from the time when the flow is created to the current time) exceeds the set aging time, the flow is aged and output to the specified destination. The duration of an active flow in the buffer is determined by the active time set for the flow. To enable the NMS to rapidly detect the status of an active flow, you can set the active time to a smaller value to increase the frequency at which NetStream packets are sent. To increase the statistics efficiency, you can set the active time to a greater value to reduce the frequency at which NetStream packets are sent. You are advised to set this parameter value to 1 minute.

- Configuring an interval at which an inactive flow times out: **ip netstream timeout inactive inactive-interval**

**NOTE**

Indicates the inactive aging time set for NetStream original flows. When the inactive time of a flow (from the time when the last packet is added to the flow to the current time) exceeds the set aging time, the flow is aged and sent to the specified destination. The duration of an inactive flow in the buffer is determined by the inactive time set for the flow. If the volume of the traffic is large, you can reduce the inactive time set for the inactive flows, improving the statistics efficiency. You are advised to set this parameter value between 30 to 60 seconds.

- Configuring the Netstream direction on an interface: **ip netstream { inbound | outbound }**

**NOTE**

After NetStream is enabled to collect statistics about incoming or outgoing data flows, statistics about unicast and multicast packets are collected.

- Configuring an interval at which Netstream flows are sampled on an interface: **ip netstream sampler fix-packets packet-interval { inbound | outbound }**
- Users can run the **display netstream all** command to display Netstream configuration information.

Perform the following operations on eSight:

- Choose **Configuration > Collector Configuration** from the main menu. Configure the traffic sending port on the device to be monitored by NTA.
- Choose **Configuration > Device Configuration** from the main menu, enter an **IP address**, select the interfaces, and add them to interfaces monitored by NTA.

**NOTE**

It is recommended that you add all interfaces of the device to the NTA. When the traffic forensics function is enabled, the NTA collects session information passing through all interfaces added to the NTA. If the outbound or inbound interface in the session information is not monitored by the NTA, its corresponding traffic forensics information is displayed as empty.

- Restart the collector manually after you change the listening port of the collector.

## 9.4 Monitoring Network Traffic

NTA provides a dashboard and traffic analysis functions. It analyzes and displays network traffic from multiple dimensions to locate network fault in a timely manner.

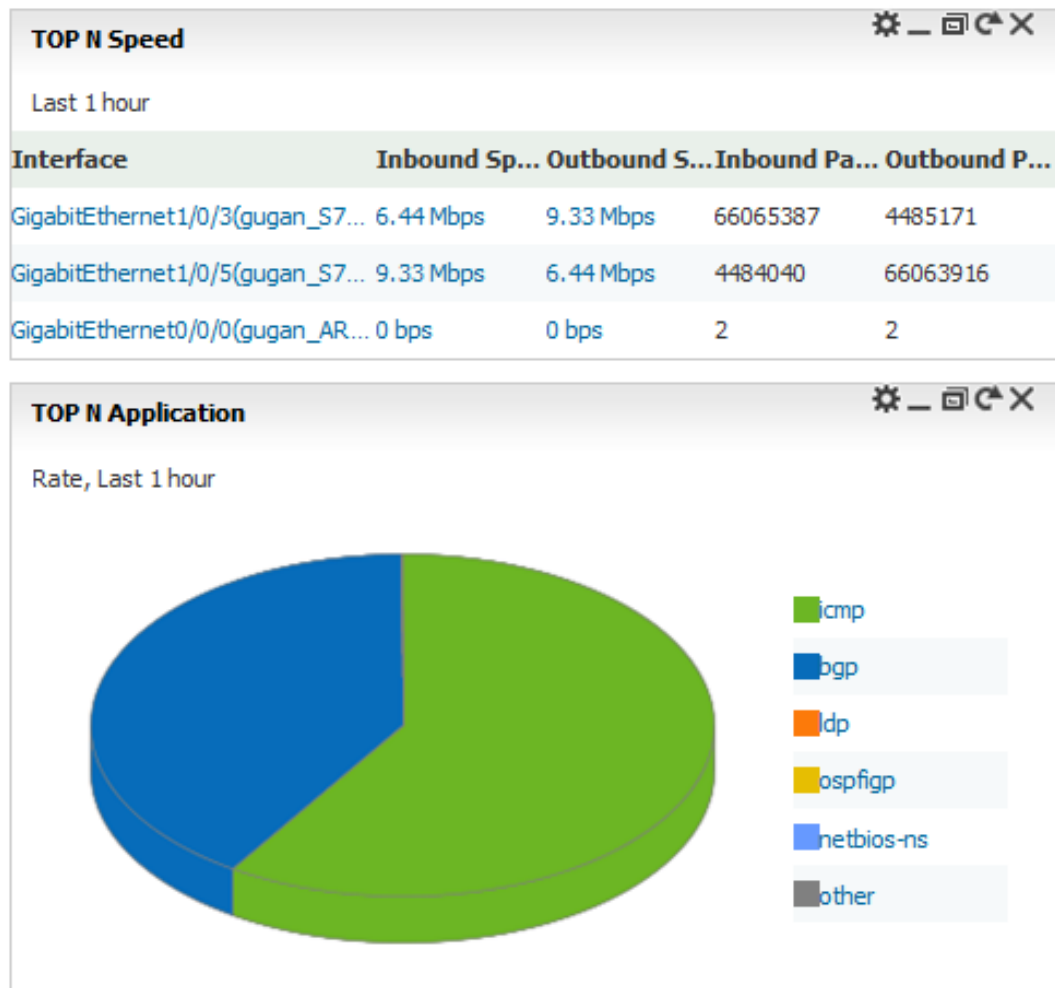
## 9.4.1 Viewing Dashboard

Dashboard displays the inbound/outbound utilization of an interface, Top N applications, and Top N hosts, which helps you learn about the network running status.

### Main Functions

1. Customized content display
  - By default, Dashboard provides eight types of Top N ranking the interface, interface usage, application, DSCP, source host, destination host, session, and protocol.
  - Click  on the top right corner of the page to add the other five types of Top N ranking: application group traffic ranking, IP group traffic ranking, interface group traffic ranking, and DSCP group traffic ranking.
  - Click  on the top right corner of a Top N ranking area to close this Top N ranking. Dashboard allows you to minimize and maximize a wedge.

Figure 9-3 Dashboard traffic analysis



2. Customized format display

- Click  on the top right corner of a Top N ranking area to set **Title**, **Automatically refresh interval**, **Time range**, and **Maximum number of lines displayed**.
  - Click  on the top right corner to refresh all the content on the page or click  to refresh data in the area. The system refreshes the page every 10 minutes by default.
3. Data association
- Click a piece of data on the Top N area to view the traffic trend relevant to the data in the last 1 hour.

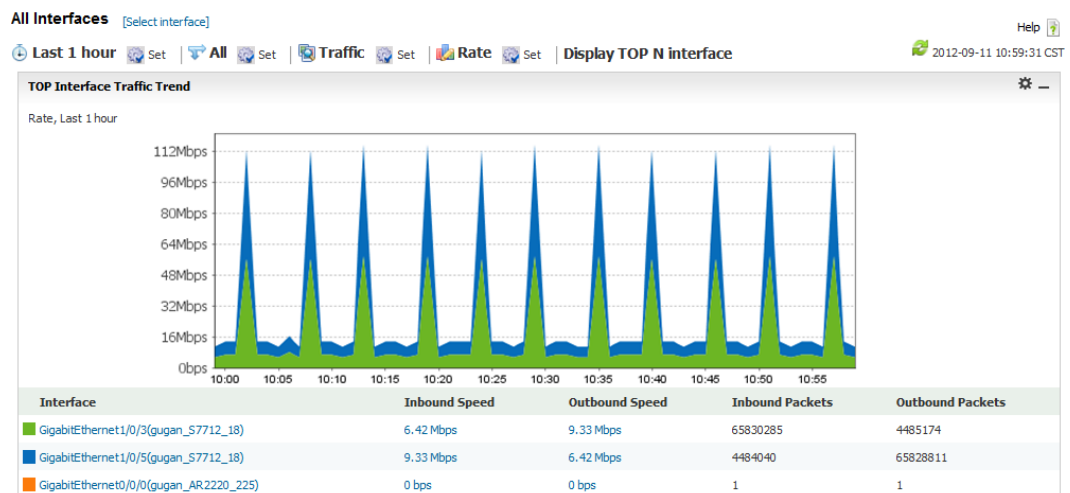
## 9.4.2 Traffic Analysis

Through traffic analysis, NTA displays the traffic trend and traffic ranking from multiple dimensions.

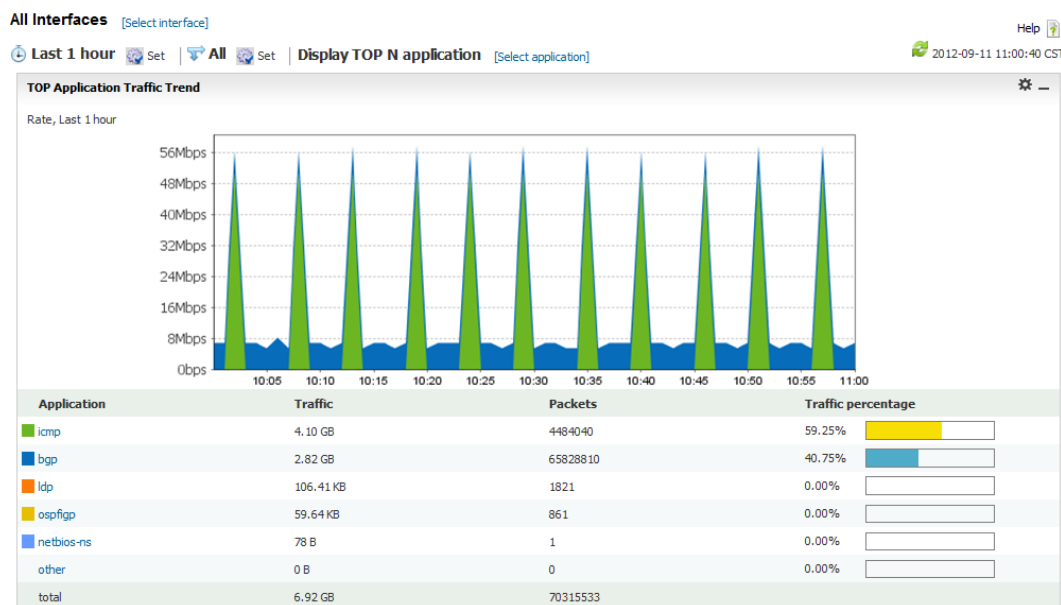
### Main Functions

1. Interface traffic analysis
  - The system provides the rate trend of traffic on Top N interfaces among monitored interfaces in the recent 1 hour.
  - You can also select one interface to view traffic and traffic trend on an interface, Top N source host traffic ranking, Top N destination host traffic ranking, Top N application traffic ranking, and Top N DSCP traffic.

**Figure 9-4** Interface traffic analysis



2. Application traffic analysis
  - Displaying top N traffic list of all applications.
  - Displaying traffic types and traffic trend of a single application, and Top N source and destination hosts of the application traffic.

**Figure 9-5** Application traffic analysis

3. Source host traffic analysis
  - Displaying the Top N source host traffic list.
  - Displaying traffic types and traffic trend of a single host among Top N source hosts, Top N application traffic, and Top N DSCP traffic.
4. Destination host traffic analysis
  - Displaying the Top N destination host traffic list.
  - Displaying traffic types and traffic trend of a single host among Top N destination hosts, Top N application traffic, and Top N DSCP traffic.
5. DSCP traffic analysis
  - Displaying the Top N DSCP traffic list.
  - Displaying the trend of a single DSCP traffic.
  - Displaying Top N source hosts and destination hosts of DSCP traffic.
6. Session traffic analysis
  - Displaying the traffic trend of Top N sessions, including source hosts, destination hosts, applications, traffic, data packet quantity, and traffic percentage.
7. Interface group traffic analysis
  - Displaying Top N traffic interface groups.
  - Inbound rate, outbound rate, number of incoming packets, and number of outgoing packets of Top N interface groups.
8. Application group traffic analysis
  - Displaying Top N traffic application groups.
  - Displaying traffic and data packet quantity of Top N traffic application groups.
9. IP group traffic analysis
  - Displaying Top N traffic IP groups.
  - Displaying traffic and data packet quantity of Top N traffic IP groups.
10. DSCP group traffic analysis

- Displaying Top N traffic DSCP groups.
- Displaying traffic and data packet quantity of Top N traffic DSCP groups.
- Displaying the traffic trend, Top N source hosts, Top N destination hosts of a single DSNP group among Top N DSCP groups.

**NOTE**

- The system provides powerful filtering capabilities. You can set filtering conditions as: traffic time, traffic direction, analysis type and statistics index.
- Click **Set** at the upper right corner of the traffic trend chart, you can modify **Title** and **Maximum number of lines displayed**.
- Select part-time with the left mouse button in the traffic trend chart, and double-click the area, you can view traffic trends in detail at that period.

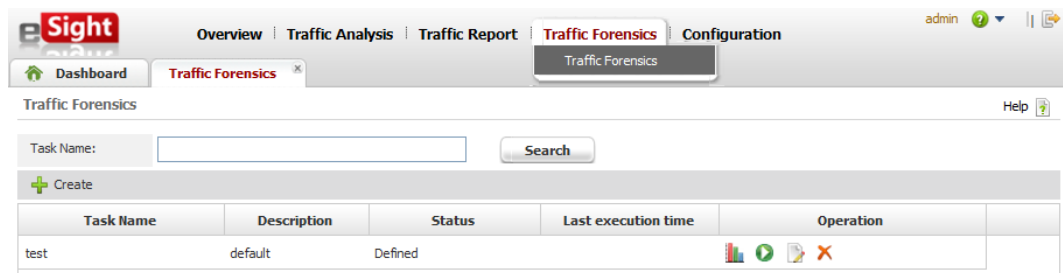
## 9.5 Creating a Traffic Report

You can create traffic report tasks to generate traffic reports. In this way, you can obtain network traffic statistics. This ensures guaranteed bandwidth for key services.

### Procedure

**Step 1** Choose **Traffic Report > Traffic Report**.

**Figure 9-6** Traffic report



**Step 2** Click **Create**. The navigation page for creating traffic reports is displayed.

**Step 3** Set the **General** option.

1. Enter a name in **Name**, select a report category in **Report Category**, and enter descriptions in **Description**.

**NOTE**

- A report group is similar to a file. You can place multiple reports in a file. This facilitates report filtering and querying on the report query page.
  - You can choose a report group on the NMS or create a new report group.
  - You can select report groups from the drop-down list box. Report groups on the NMS can be deleted.
2. Select **Interface** to select a monitored object.
  3. Click **Next**.

**Figure 9-7** General option

Traffic Report > Create

General Filter Layout Schedule Abstract

\* Name: DSCP\_report

Report Category: DSCP

Add

Delete

Description:

Select the object to be monitored.

+ Select Interface

| Device Name      | Selected interface   | Interface Description                  | Operation |
|------------------|----------------------|----------------------------------------|-----------|
| Huawei S9300     | GigabitEthernet3/0/0 | GigabitEthernet3/0/0                   | ✗         |
| Huawei S9300     | GigabitEthernet3/0/1 | GigabitEthernet3/0/1                   | ✗         |
| gugan_AR3260_222 | GigabitEthernet0/0/0 | HUAWEI, AR Series, GigabitEthernet0... | ✗         |
| gugan_AR3260_222 | Ethernet6/0/0        | HUAWEI, AR Series, Ethernet6/0/0 In... | ✗         |
| gugan_AR3260_222 | Ethernet6/0/1        | HUAWEI, AR Series, Ethernet6/0/1 #...  | ✗         |

Next Cancel

**Step 4** Set the **Filter** option.

1. Select **Summary Type** to choose one or multiple summary types. The system supports six summary types: **Application summary**, **Session summary**, **DSCP summary**, **DSCP summary**, **Destination host summary**, and **Interface summary**.
2. After the report filtering conditions are specified, click **Add** to add filtering conditions to the following list.

You can set more than one filtering conditions. The added filtering conditions can be removed from the list.

3. Click **Next**.

**Figure 9-8** Filter option

Traffic Report > Create

General Filter Layout Schedule Abstract

Summary Type

☐ Application Summary

☐ Conversation Summary

☒ DSCP Summary

☐ Source Host Summary

☐ Destination Host Summary

☐ Interface Summary

Filter: DSCP Equal to AF13

Add

| Filter             | Operation |
|--------------------|-----------|
| DSCP Equal to AF12 | ✗         |
| DSCP Equal to AF13 | ✗         |

Previous Next Cancel



**Step 5** Set the **Layout** option.

1. Select **Summary Type** and **Details** to add the report display model to the following list.



### NOTE

- **Summary Type** is one option of **Filter**. If the **Layout** option of a summary type is not selected, statistics about this report is not collected.
- You can delete a layout type or adjust the layout sequence in the **Operation** column.

2. Click **Next**.

**Figure 9-9** Layout option

Traffic Report > Create Help 

General **Filter** Layout Schedule Abstract

**Layout**

Summary Type: DSCP Summary Details: Pie Chart Add

Delete

|                          |   | Details                  | Operation                                                                                                                                                                                                                                                   |
|--------------------------|---|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 1 | DSCP Summary - Table     |    |
| <input type="checkbox"/> | 2 | DSCP Summary - Pie Chart |    |

Previous Next Cancel

**Step 6** Set the **Time Frame** option.

1. Set the **Time Range**. You can choose an absolute time range or a cycle time range. If you select **Current time**, **Recurrence** can be set.
2. Click **Next**.

**Figure 9-10** Time frame option

Traffic Report > Create Help

---

General **Filter** Layout Schedule Abstract

**Period Type**

Time Range:  Last

**Periodic Task**

☐ Periodic Task

☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Execution Time:

Previous Next Cancel

- Step 7** Click **Abstract** to browse summary about the previous configurations. Click **Save and Execute** to save the report to the report list and execute the task.

**Figure 9-11** Abstract

**Abstract**

|                  |                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name:            | DSCP_report                                                                                                                                                     |
| Report Category: | Default                                                                                                                                                         |
| Description:     |                                                                                                                                                                 |
| Interface:       | NULL0<br>GigabitEthernet0/0/2<br>Cellular0/0/0<br>Cellular0/0/1<br>GigabitEthernet5/0/1<br>GigabitEthernet5/0/2<br>GigabitEthernet5/0/3<br>GigabitEthernet5/0/6 |
| Filter:          | DSCP Equal to AF12<br>DSCP Equal to AF13                                                                                                                        |
| Summary Type:    | DSCP Summary                                                                                                                                                    |
| Layout:          | DSCP Summary - Table<br>DSCP Summary - Pie Chart                                                                                                                |
| Time Range:      | Last 1 Day(s)                                                                                                                                                   |

[Previous](#) [Save](#) [Save and Execute](#) [Cancel](#)

You can click **Previous** to modify previous configurations, click **Save** to save the previous configurations to the report list for later execution, or click **Cancel** to clear all inputted contents and exit from the report creation.

----End

## Follow-up Procedure

The created report is displayed on the homepage. You can click **Operation**  to view details about the data trend on the report, click  to view the defined filtering conditions and report layout, click  to execute the saved report task that has not been executed, or click  to delete the report task.

## 9.6 Creating Traffic Forensics Tasks

You can create traffic forensics tasks to view traffic data in detail. This helps locate network fault.

## Procedure

**Step 1** Choose **Traffic Forensics** > **Traffic Forensics**.

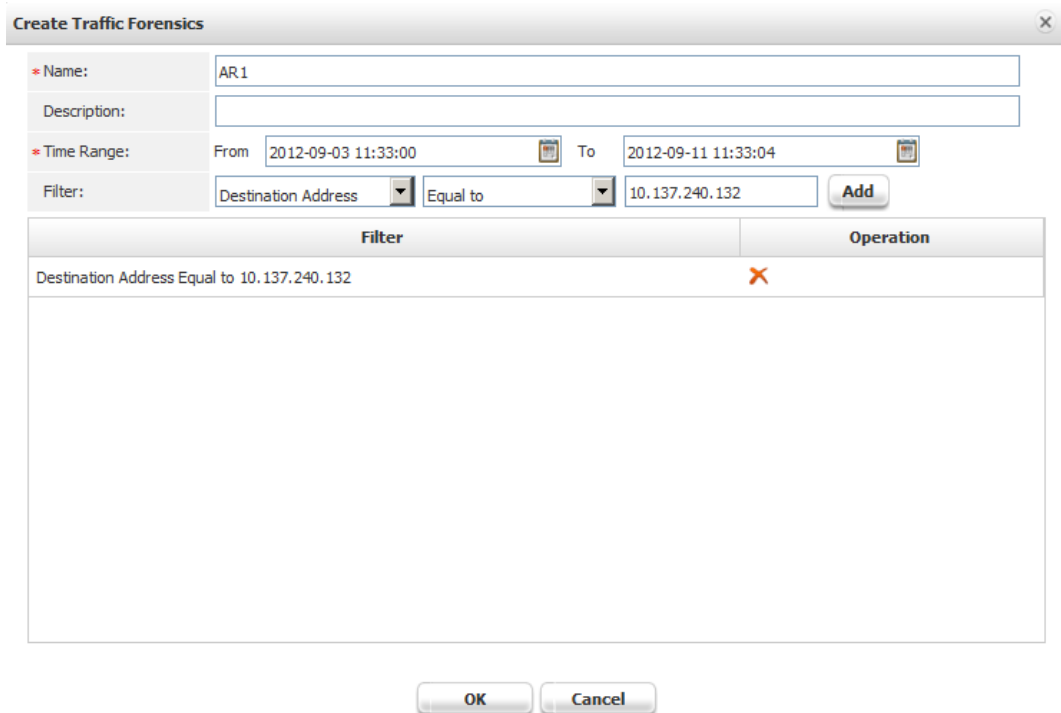
**Figure 9-12** Traffic forensics



**Step 2** Click **Create**. The page for creating traffic forensics tasks is displayed.

**Step 3** Enter a name in **Name** and descriptions in **Description** for the traffic forensics task. Enter a time range in **Time Range**.

**Figure 9-13** Create Traffic forensics



**Step 4** Set the **Filter** option and click **Add** to add filtering conditions to the filtering list. You can set more than one filtering conditions.

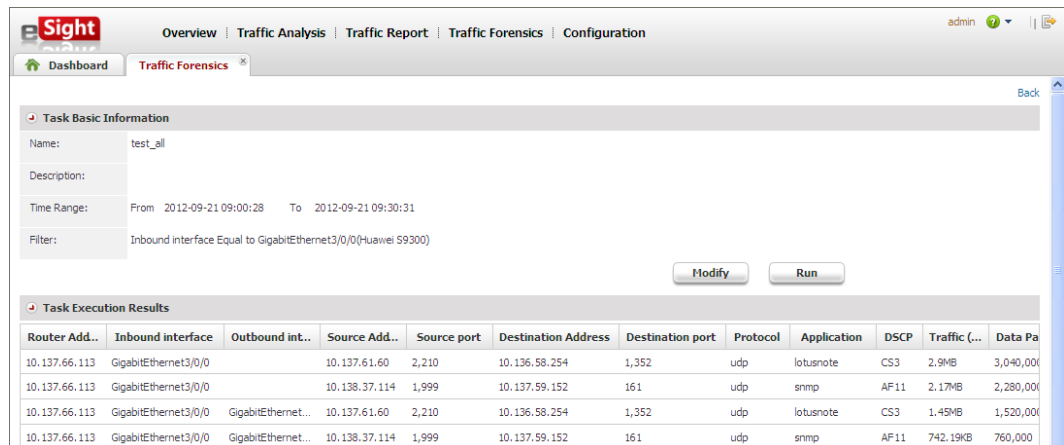
**Step 5** Click **OK**. A traffic forensics task is created.

 **NOTE**

The created task is not executed immediately. You need to click  in the traffic forensics list to manually execute it.

**Step 6** On the main page of traffic forensics, click  of **Operation** area to see traffic data information in details.

**Figure 9-14** Traffic forensics detail



The screenshot shows the 'Traffic Forensics' page in the eSight interface. It includes a navigation bar with 'Overview', 'Traffic Analysis', 'Traffic Report', 'Traffic Forensics', and 'Configuration'. The 'Traffic Forensics' tab is active. Below the navigation bar, there's a 'Task Basic Information' section with fields for Name (test\_all), Description, Time Range (From 2012-09-21 09:00:28 To 2012-09-21 09:30:31), and Filter (Inbound interface Equal to GigabitEthernet3/0/0(Huawei S9300)). There are 'Modify' and 'Run' buttons. Below this is the 'Task Execution Results' section, which contains a table with 12 columns: Router Addr., Inbound interface, Outbound int., Source Addr., Source port, Destination Address, Destination port, Protocol, Application, DSCP, Traffic (...), and Data Pa.

| Router Addr.  | Inbound interface    | Outbound int.      | Source Addr.  | Source port | Destination Address | Destination port | Protocol | Application | DSCP | Traffic (...) | Data Pa   |
|---------------|----------------------|--------------------|---------------|-------------|---------------------|------------------|----------|-------------|------|---------------|-----------|
| 10.137.66.113 | GigabitEthernet3/0/0 |                    | 10.137.61.60  | 2,210       | 10.136.58.254       | 1,352            | udp      | lotusnote   | CS3  | 2.9MB         | 3,040,000 |
| 10.137.66.113 | GigabitEthernet3/0/0 |                    | 10.138.37.114 | 1,999       | 10.137.59.152       | 161              | udp      | snmp        | AF11 | 2.17MB        | 2,280,000 |
| 10.137.66.113 | GigabitEthernet3/0/0 | GigabitEthernet... | 10.137.61.60  | 2,210       | 10.136.58.254       | 1,352            | udp      | lotusnote   | CS3  | 1.45MB        | 1,520,000 |
| 10.137.66.113 | GigabitEthernet3/0/0 | GigabitEthernet... | 10.138.37.114 | 1,999       | 10.137.59.152       | 161              | udp      | snmp        | AF11 | 742.19KB      | 760,000   |

 **NOTE**

- If more forensics results are displayed than required, you can click **Modify** on the page, change filtering conditions for traffic forensics tasks, and click **Execute** to get streamlined information.
- If the inbound interface or outbound interface is empty, it indicates a broadcast packet or the interface is not monitored by the NTA.

----End

## Follow-up Procedure

The created traffic forensics task is displayed on the home page of the traffic forensics. You can click **Operation**  to view traffic data details, click  to modify the traffic forensics task, click  to execute the task, or click  to delete the created task.

## 9.7 Configuring NTA

This section describes how NTA collects traffic from monitored objects.

### 9.7.1 Configuring a Collector

This section describes how to configure the listening port on the collector and the receiving port on the analyzer.

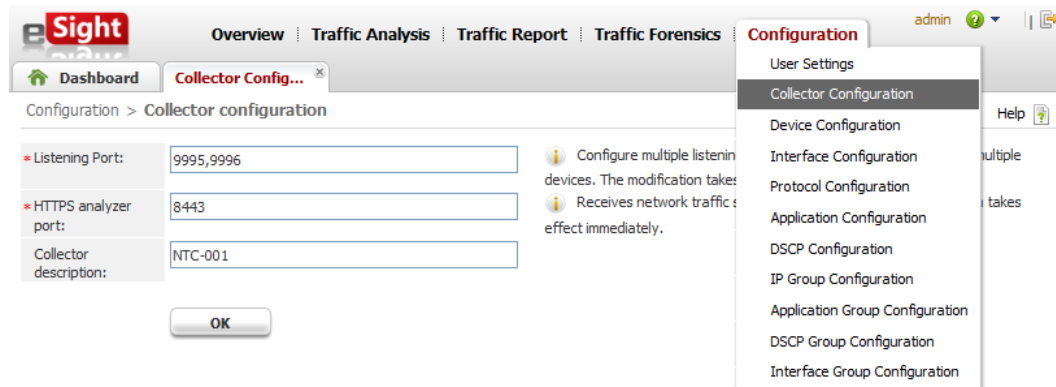
#### Context

Currently, only one collector can be configured.

## Procedure

**Step 1** Choose **Configuration > Collector configuration** from the main menu.

**Figure 9-15** Collector configuration



**Step 2** Enter a port number in **Listening Port**. To monitor network traffic of multiple devices, configure multiple listening ports.

**Step 3** Enter a port number in **HTTPS analyzer port**.

**Step 4** Click **OK**.

----End

## 9.7.2 Setting Protocols

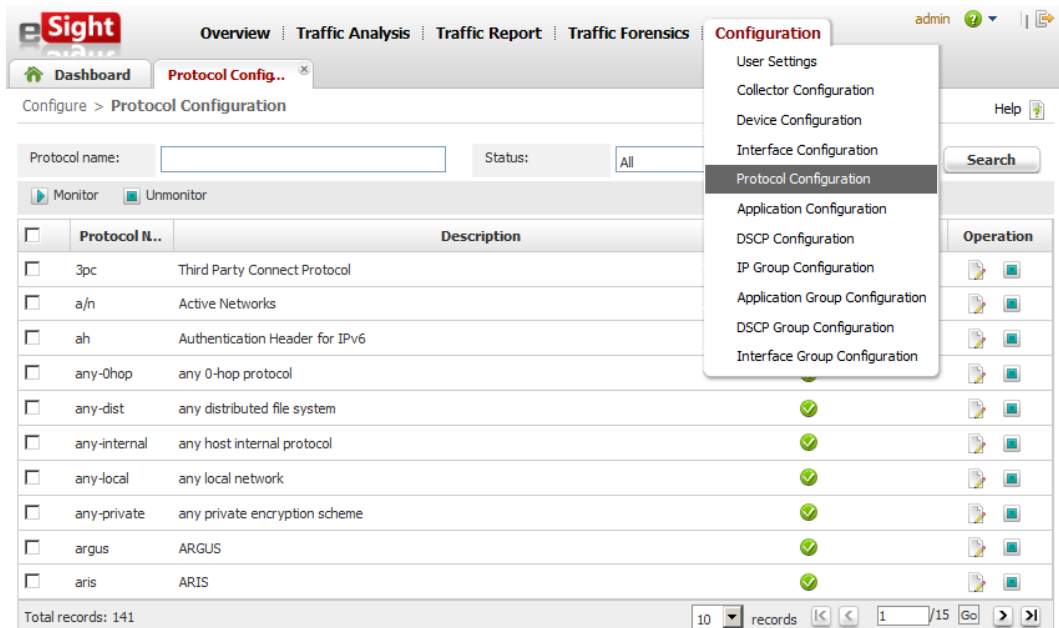
This section describes how to set protocols.

### Context

- Protocols have a higher priority than applications. When a protocol is disabled, the application cannot be monitored.
- The system provides 141 protocols and the commonly used protocols are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Simple Mail Transfer Protocol (SMTP).

## Procedure

**Step 1** Choose **Configure > Protocol Configuration** from the main menu. The page that shows protocols supported by eSight is displayed.

**Figure 9-16** Protocol configuration

**Step 2** Select multiple protocols and click **Monitor** or **Unmonitor** to display the modification result.

**Step 3** Click **Modify** in the **Operation** column to modify the protocol description. The protocol description after modification is displayed on the page.

----End

## 9.7.3 Configuring Application

This section describes how to configure applications and the scopes.

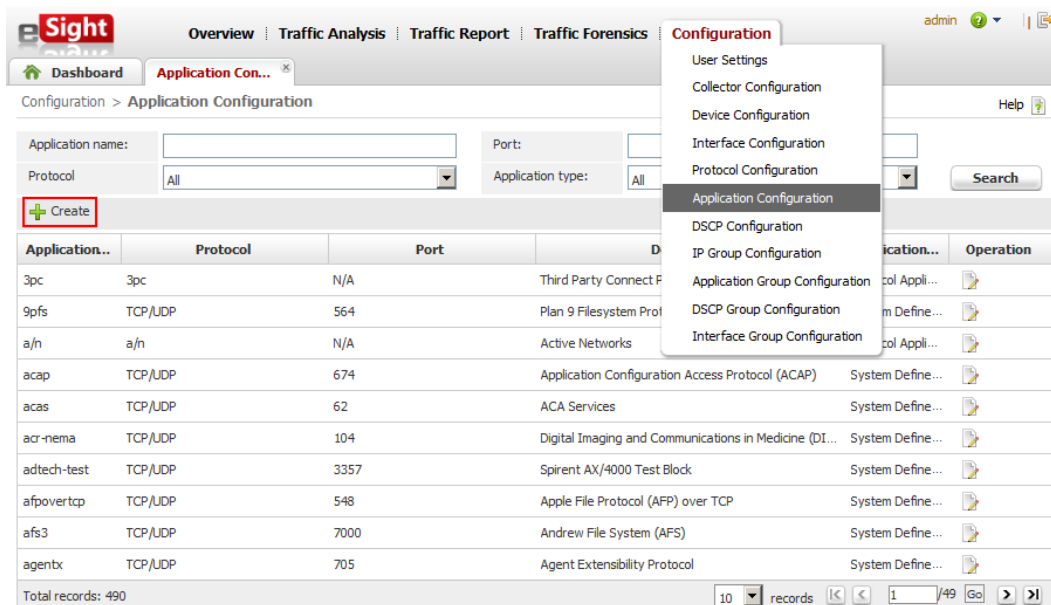
### Context

- System-defined applications: the system provides more than 300 pre-defined applications, which are named in the format of protocol name-port number.
- Protocol applications: refer to the protocols with the monitoring port number of 0, such as ICMP and IGMP.
- User-defined applications: refer to the applications created by users. For example, TCP-443 represents the HTTPS application. However, the mail system of a company uses the port 443. In this case, the network administrator can create an imail application based on the IP address range of the mail system. After receiving TCP-443 packets, the system parses data within the IP address range into the imail application and data beyond the IP address range into the HTTPS application.
- System-added applications: when a collector receives flow statistics information from a device, the TCP-port or UDP-port contained in the flow is unknown. In this case, this application is not a system-defined application. The system automatically adds the application and names this application in the format of TCP-XXX or UDP-XXX, where XXX represents the port number.

## Procedure

- Step 1** Choose **Configuration > Application Configuration** from the main menu. The page that shows the system-defined and user-defined application list is displayed.

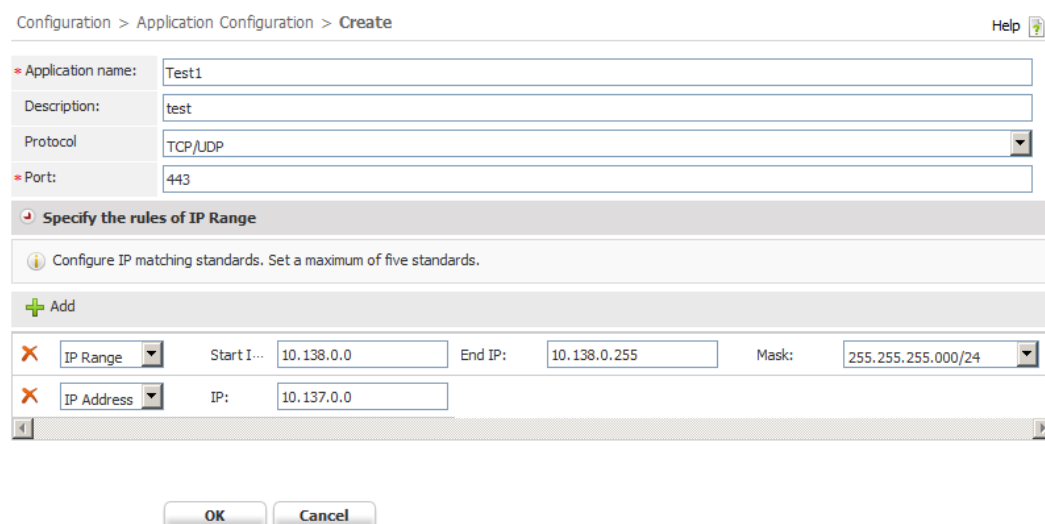
**Figure 9-17** Application configuration



- Step 2** Click **Create** to display the **Create Application** page.

- Step 3** Set **Application name**, **Description**, **Protocol**, and **Port**.

**Figure 9-18** Create



- Step 4** Click **Add** in the **Specify the rules of IP Range** area to set an IP address, range, or network.

- Step 5** Click **OK**.

----End

## Follow-up Procedure

- The system allows you modify **Application name, Description, Protocol, Port** and **Specify the rules of IP Range to User-defined applications**. The system only allows you modify **Description** to other applications.
- The system allows you delete **User-defined applications**.

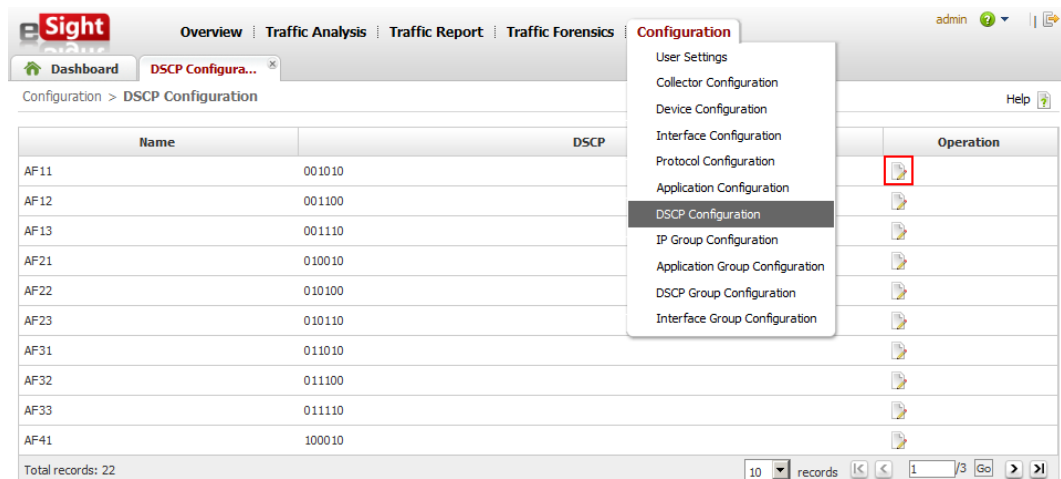
## 9.7.4 Configuring DSCP

This section describes how to configure DSCP monitored by eSight.

### Procedure

- Step 1** Choose **Configuration > DSCP Configuration** from the main menu. The page that shows DSCP supported by eSight is displayed.

**Figure 9-19** DSCP configuration



- Step 2** Click **Modify** in the **Operation** column to modify the DSCP name.

----End

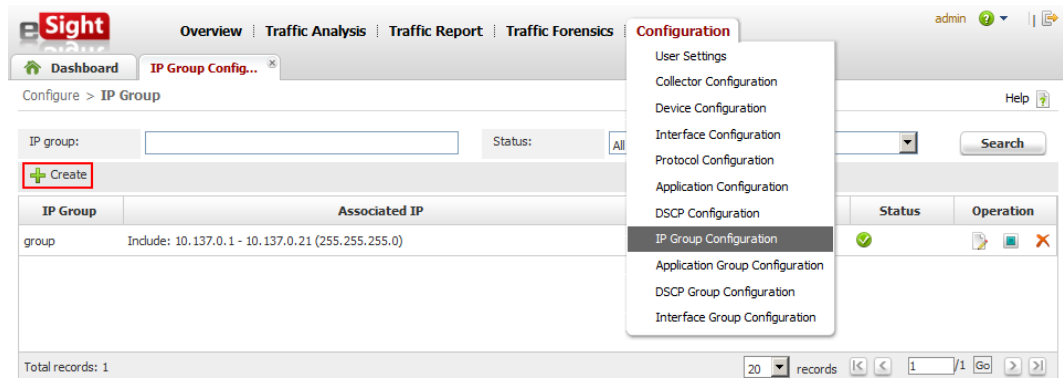
## 9.7.5 Configuring an IP Group

This section describes how to configure an IP group.

### Procedure

- Step 1** Choose **Configuration > IP Group Configuration** from the main menu.



**Figure 9-20** IP group configuration

**Step 2** Click **Create**.

**Step 3** Set **IP group** and **Description**.

**Figure 9-21** Create

Configure > IP Group > Create

\* IP group:

Description:

**Specify the rules of IP Range**

Configure IP matching standards. Set a maximum of five standards.

**Add**

☐ IP Address IP:

☐ IP Range Start IP:  End IP:  Mask:

**Step 4** Click **Add** in the **Specify the rules of IP Range** area to set an IP address, range, or network.

**Step 5** Click **OK**.

----End

## Follow-up Procedure

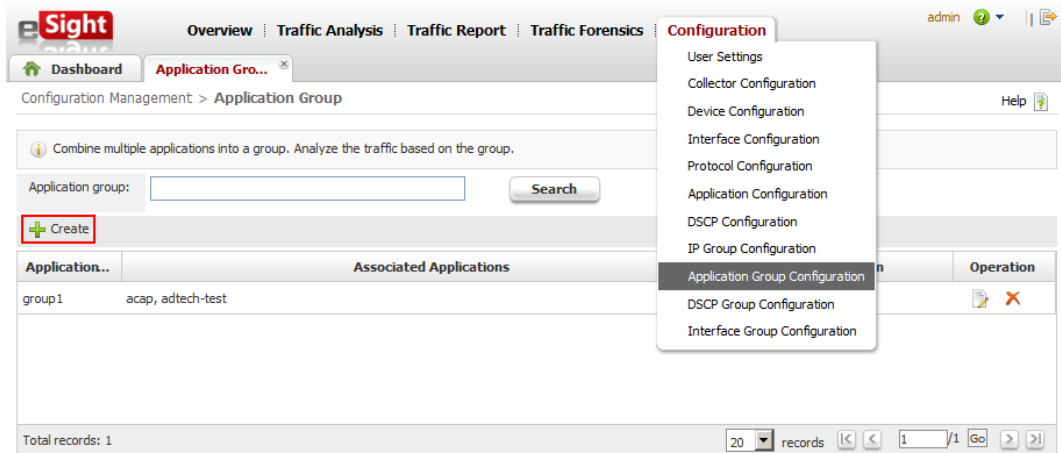
The system allows you modify **IP Group**.

## 9.7.6 Configuring an Application Group

This section describes how to configure an application group.

### Procedure

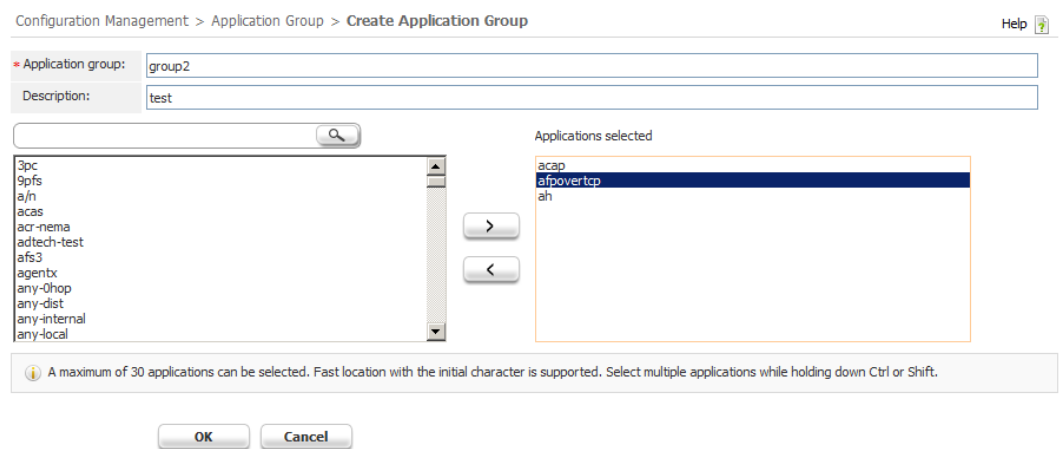
**Step 1** Choose **Configuration > Application Group Configuration** from the main menu.

**Figure 9-22** Application group configuration

**Step 2** Click **Create**.

**Step 3** Set **Application group** and **Description**, and select **Application**.

A maximum of 30 applications can be selected. You can quickly locate the applications with the first character. Press **Ctrl** or **Shift** to select multiple applications.

**Figure 9-23** Create application group

**Step 4** Click **OK**.

----End

## Follow-up Procedure

The system allows you modify **Application Group**.

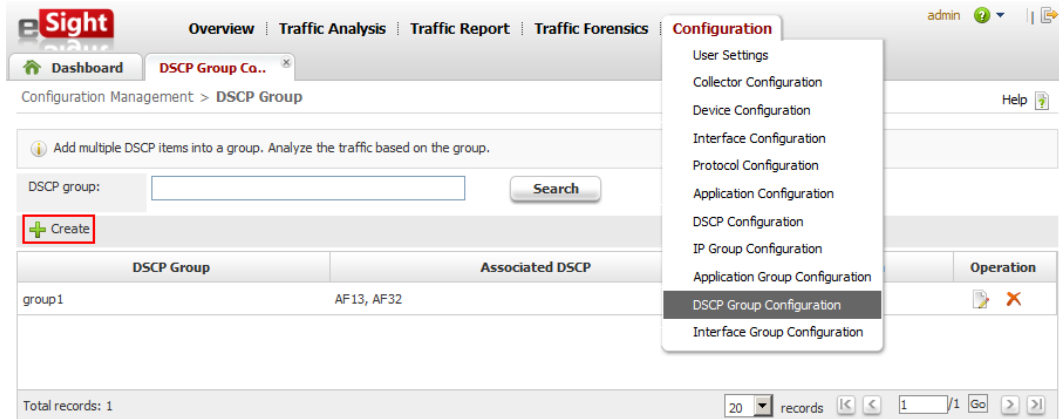
### 9.7.7 Configuring a DSCP Group

This section describes how to configure a DSCP group.

## Procedure

**Step 1** Choose **Configuration > DSCP Group Configuration** from the main menu.

**Figure 9-24** DSCP group configuration

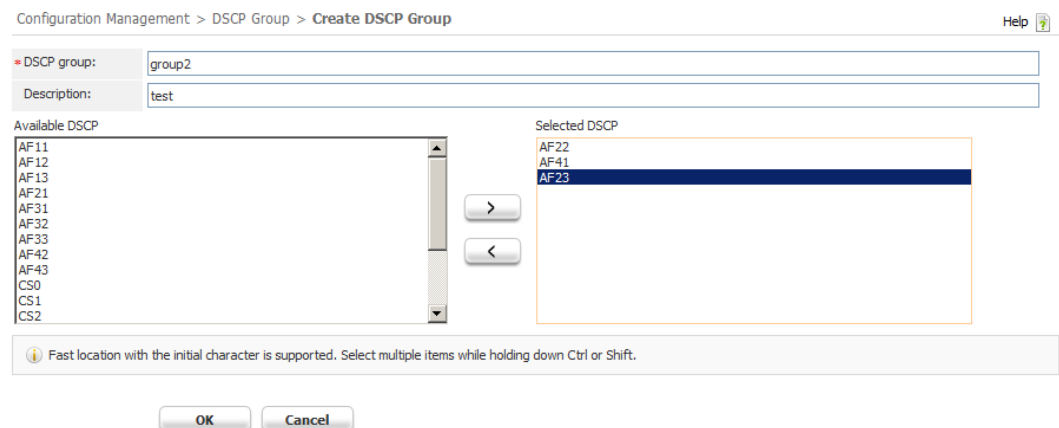


**Step 2** Click **Create**.

**Step 3** Set **DSCP group** and **Description**, and select **Available DSCP**.

Press **Ctrl** or **Shift** to select multiple DSCP.

**Figure 9-25** Create DSCP group



**Step 4** Click **OK**.

----End

## Follow-up Procedure

The system allows you modify **DSCP Group**.

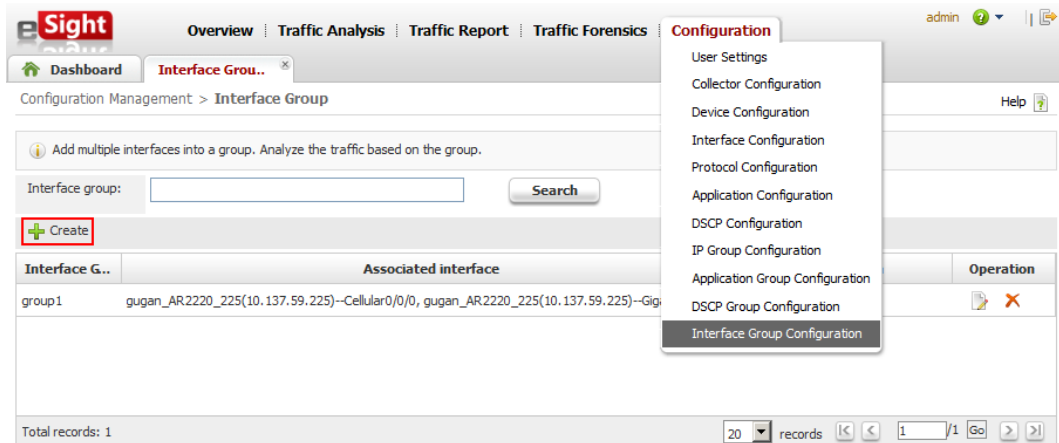
## 9.7.8 Configuring an Interface Group

This section describes how to configure an interface group. After an interface group is configured, multiple sub-interfaces can be treated as a logical entity.

### Procedure

**Step 1** Choose **Configuration > Interface Group Configuration** from the main menu.

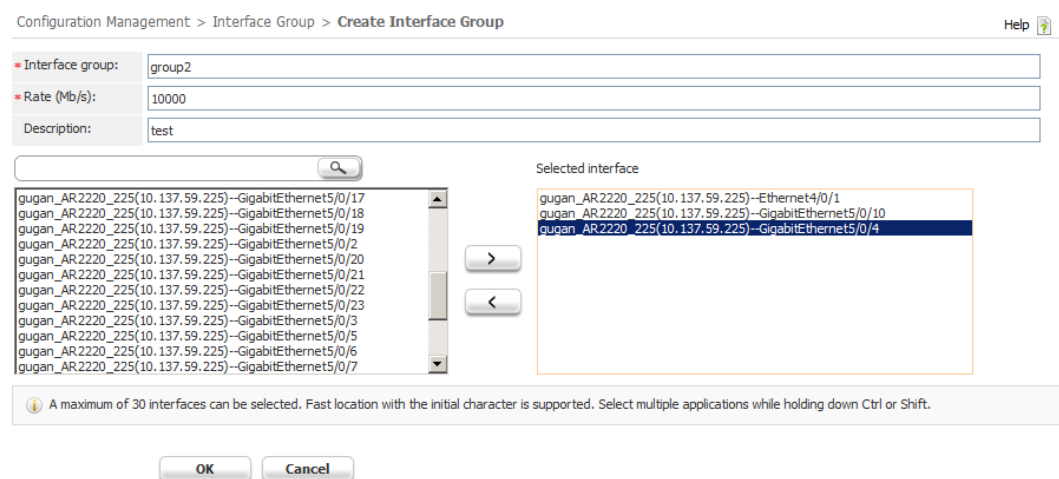
**Figure 9-26** Interface group configuration



**Step 2** Click **Create**.

**Step 3** Set **Interface group**, **Rate**, and **Description**, and select **Available interface**.

**Figure 9-27** Create interface group



**Step 4** Click **OK**.

----End

## Follow-up Procedure

The system allows you modify **Interface Group**.

---

# 10 Service Management

---

## About This Chapter

### 10.1 IPsec VPN Service Monitoring and Management

eSight monitors and manages the IPsecVPN service and provides the functions such as synchronizing a network domain tunnel and viewing network domain details, such as the tunnel list and network domain topology.

### 10.2 WLAN Management

This topic describes the basic concepts and configuration methods of the WLAN.

### 10.3 BGP/MPLS VPN Management

This topic describes terms, functions, and typical configuration examples of BGP/MPLS VPN management provided by eSight.

### 10.4 SLA Management

eSight provides the service level agreement (SLA) monitoring and management functions, including SLA Overview, SLA services, SLA tasks, and quick diagnosis.

## 10.1 IPsec VPN Service Monitoring and Management

eSight monitors and manages the IPsecVPN service and provides the functions such as synchronizing a network domain tunnel and viewing network domain details, such as the tunnel list and network domain topology.

### 10.1.1 IPsec VPN Application

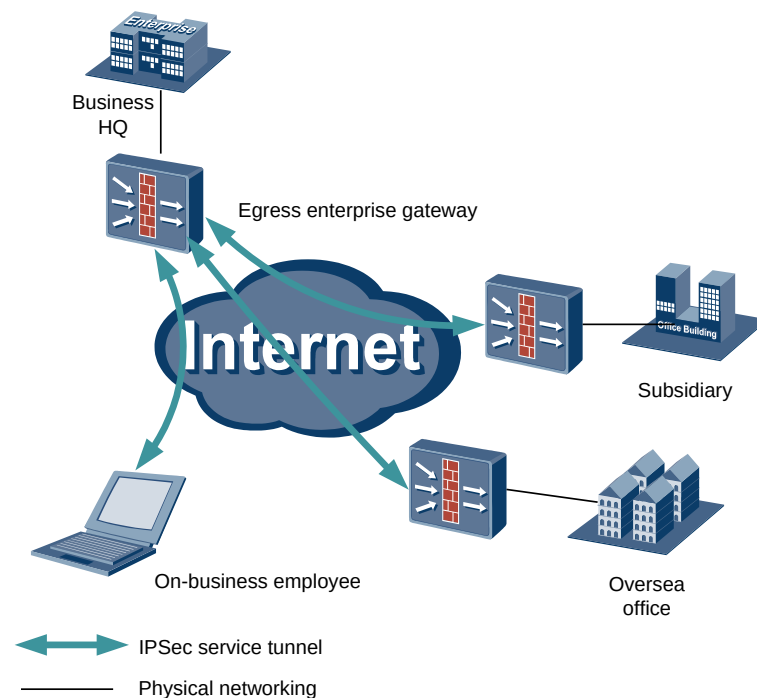
IPsec VPN establishes secure communication tunnels for enterprises and users in different geographic areas. This helps prevent data from being illegally viewed or tampered with during transmission on the public network.

With the rapid development of the Internet, more and more enterprises and individuals communicate over the Internet. When enterprises or individuals in different geographic areas communicate with each other over the Internet, most communication traffic is transmitted on an unknown network over the Internet. Therefore, security of sending and receiving data on the network cannot be ensured. IPsec provides the function of establishing and managing secure tunnels. By encrypting and authenticating data packets that are to be transmitted on the

public network, data are prevented from being illegally viewed or tempered with. That is, IPSec establishes secure communication tunnels for users in different geographic areas.

See [Figure 10-1](#). The head office, branch office, and regional office of an enterprise are connected to each other over the Internet. An IPSec VPN tunnel can be established respectively between the breakout gateways of the head office and the branch office and between the breakout gateways of the head office and the regional office. To access the breakout gateway of the head office, staff on a business trip can also directly send a request for establishing an IPSec VPN tunnel by using a PC. Remote interaction data flows of all users in the enterprise are carried by secure IPSec VPN tunnels. Data flows are still transmitted on the public network; however, the data flows are encrypted and authenticated. Therefore, the data transmission security is ensured.

**Figure 10-1** Typical application scenario of IPSec VPN



## 10.1.2 Overview of IPSec VPN Management Operations

The overview of IPSec VPN management operations helps to learn about report management operations. In the overview of report management operations, you are perform operations as required.

[Figure 10-2](#) shows the overview of IPSec VPN management operations. For details, click operations in the overview.

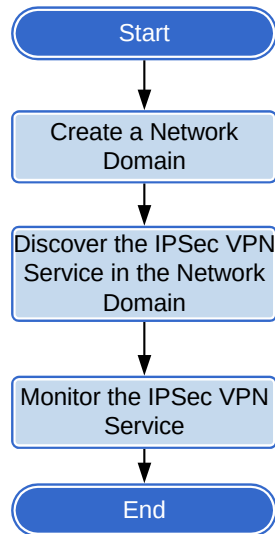
**Figure 10-2** Overview of IPSec VPN Management Operations

Table 10-1 describes the IPSec VPN management operations.

**Table 10-1** Operation description

| Operation                                            |                                                  | Description                                                                                                                                                                |
|------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a Network Domain                              |                                                  | To manage the IPSec service in an area in a centralized way, a user must create a network domain and add devices to the domain according to the management requirement.    |
| Discover the IPSec VPN Service in the Network Domain |                                                  | After creating a network domain, a user must synchronize the tunnel information of the device added to the domain to eSight. eSight monitors the tunnel connectivity.      |
| Monitor the IPSec VPN Service                        | View the Topology Structure of the IPSec Service | When querying the topology structure of the network domain, a user can view the tunnels of nodes in the network domain and tunnel status information in the topology view. |
|                                                      | Query the Running State of the IPSec VPN Service | When maintaining the IPSec service, you must query the running status periodically.                                                                                        |

### 10.1.3 Creating a Network Domain

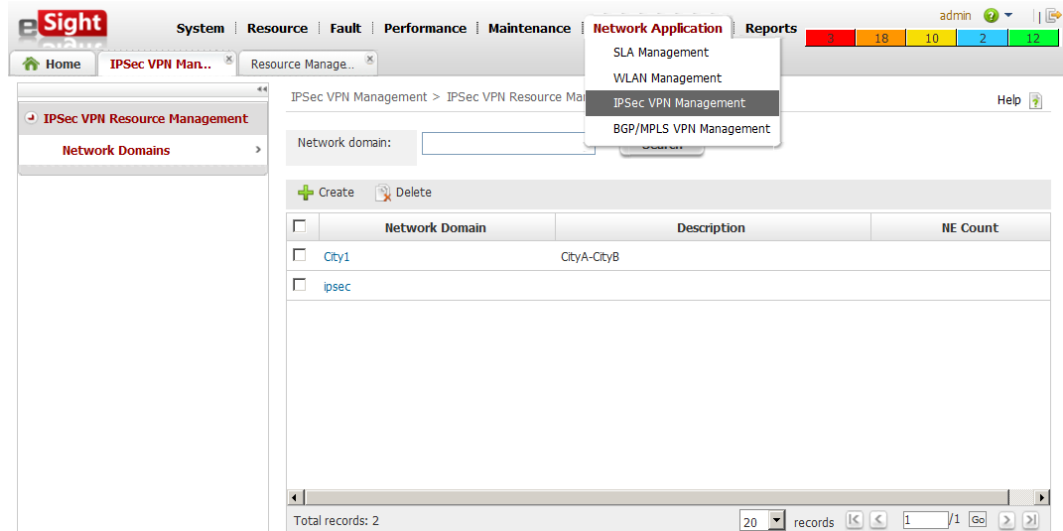
To manage the IPSec service in an area in a centralized way, a user must create a network domain and add devices to the domain according to the management requirement.



## Procedure

**Step 1** Choose **Network Application > IPsec VPN Management** from the main menu.

**Figure 10-3** IPsec VPN management



**Step 2** In the basic information pane, click **Create**.

**Step 3** In the window that is displayed, set **Network Domain** and **Description**.

**Figure 10-4** Create network domain

| * Network domain:        | City                                                                                                                                                                                                                                   |                          |         |            |         |            |  |  |  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|---------|------------|---------|------------|--|--|--|
| Description:             | CityA-CityB                                                                                                                                                                                                                            |                          |         |            |         |            |  |  |  |
| NE list:                 | <div><span>+</span> Add <span>-</span> Delete</div> <table><thead><tr><th><input type="checkbox"/></th><th>NE Name</th><th>IP Address</th><th>Ne Type</th></tr></thead><tbody><tr><td colspan="4">No record.</td></tr></tbody></table> | <input type="checkbox"/> | NE Name | IP Address | Ne Type | No record. |  |  |  |
| <input type="checkbox"/> | NE Name                                                                                                                                                                                                                                | IP Address               | Ne Type |            |         |            |  |  |  |
| No record.               |                                                                                                                                                                                                                                        |                          |         |            |         |            |  |  |  |

**Step 4** Click **Add**.

**Step 5** Select an NE or multiple NEs from the NE list, and click **OK**.

**Step 6** Click **OK**.

----End

### 10.1.4 Discovering the IPsec VPN Service in the Network Domain

After creating a network domain, a user must synchronize the tunnel information of the device added to the domain to eSight. eSight monitors the tunnel connectivity.

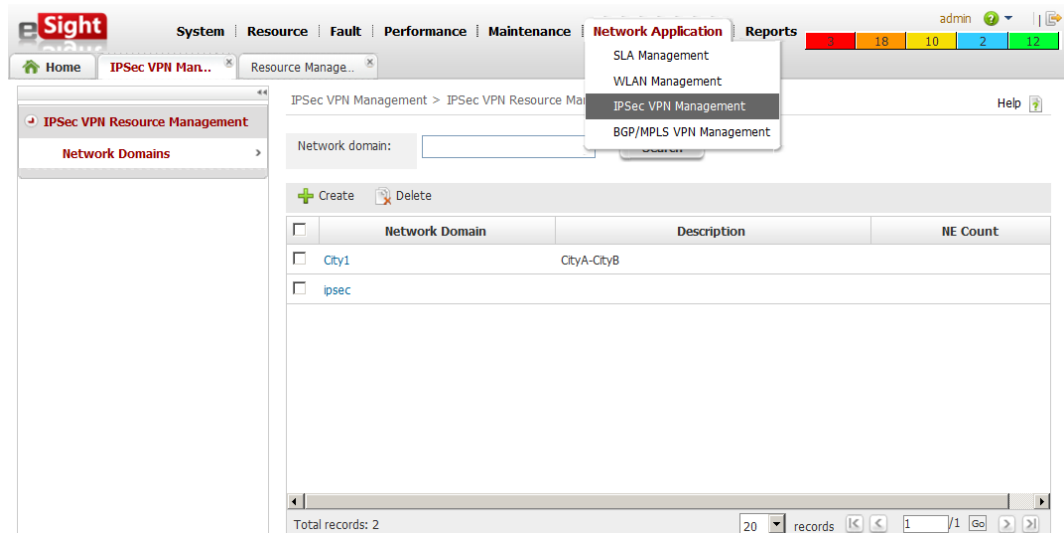
## Prerequisites

The Telnet parameters on eSight and the NE are set.

## Procedure

**Step 1** Choose **Network Application > IPsec VPN Management** from the main menu.

**Figure 10-5** IPsec VPN management



**Step 2** In the navigation tree on the left, choose **IPSec VPN Resource Management > Network Domains**. On the right, click the name of network domain to access the network domain of the IPsec VPN service.

**Step 3** Click **Synchronize** to synchronize the tunnel of the device to eSight.

**Figure 10-6** Discovering service

| Synchronize |                 |                      |         |                |                      |               |           |
|-------------|-----------------|----------------------|---------|----------------|----------------------|---------------|-----------|
| Local SN    | Local Device IP | Local Port           | Peer SN | Peer Device IP | Peer Port            | Tunnel Status | Operation |
| 10          | 10.137.59.208   | GigabitEthernet0/0/1 | 10      | 10.137.59.206  | GigabitEthernet0/0/1 | Connected     |           |

----End

## 10.1.5 Monitoring the IPsec Service

This topic describes how to monitor the performance of the IPsec network domain.

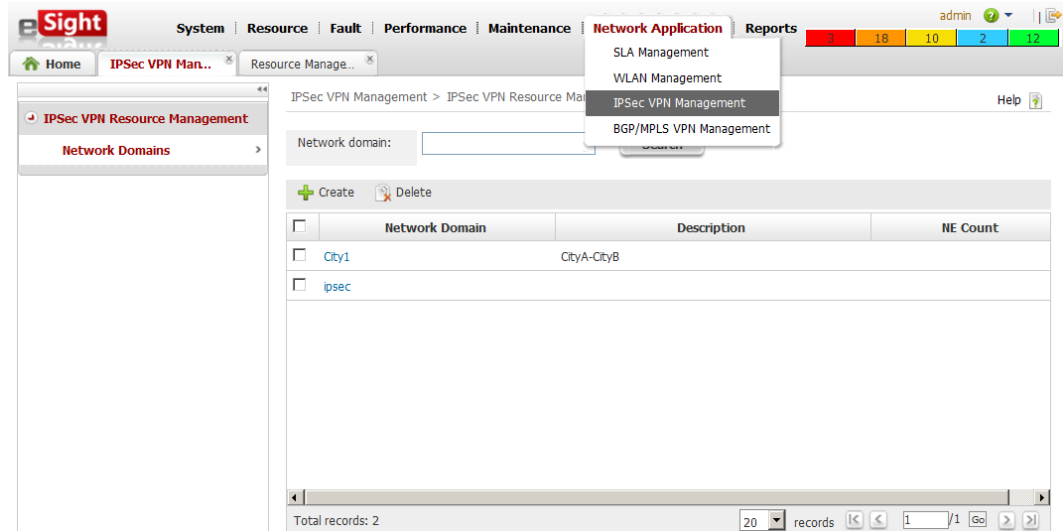
### 10.1.5.1 Viewing the Topology Structure of the IPsec Service

When querying the topology structure of the network domain, a user can view the tunnels of nodes in the network domain and tunnel status information in the topology view.

## Procedure

**Step 1** Choose **Network Application** > **IPSec VPN Management** from the main menu.

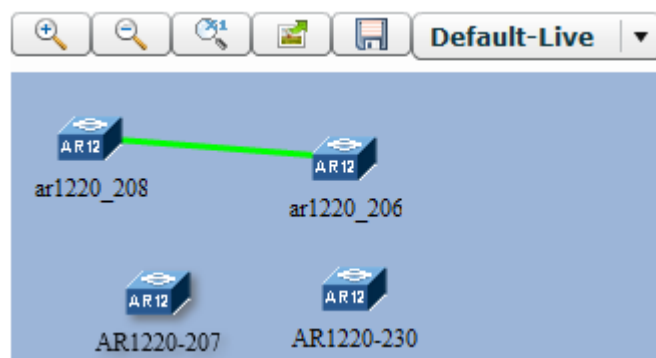
**Figure 10-7** IPsec VPN management



**Step 2** In the navigation tree on the left, choose **IPSec VPN Resource Management** > **Network Domains**. On the right, click the name of network domain to access the network domain of the IPsec VPN service.

**Step 3** In the **Tunnel Topology** pane, view the topology information of the IPsec service.

**Figure 10-8** Tunnel topology



Tunnel status in the topology view:

- Green: up
- Red: down

----End

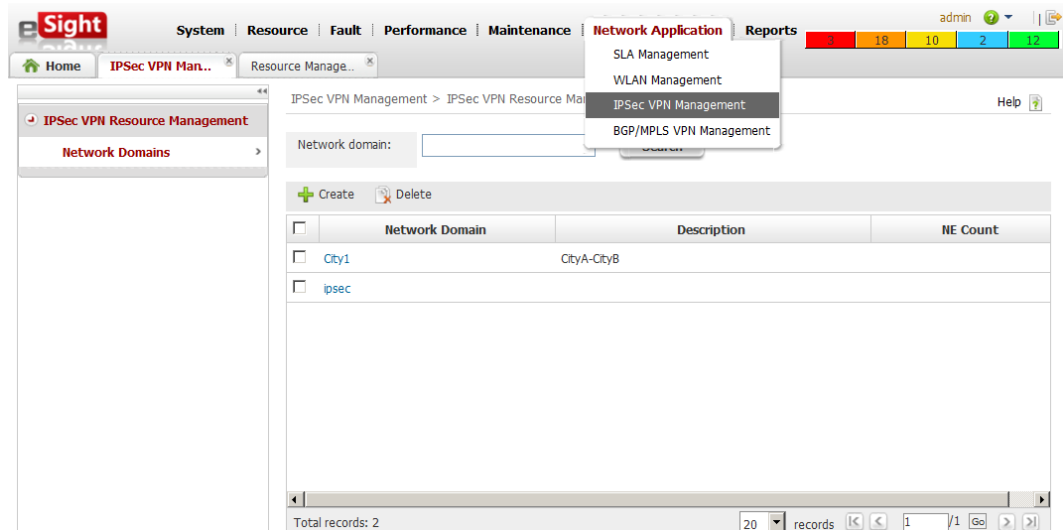
### 10.1.5.2 Querying the Running State of the IPsec VPN Service

When maintaining the IPsec service, you must query the running status periodically.

#### Procedure

**Step 1** Choose **Network Application** > **IPSec VPN Management** from the main menu.

**Figure 10-9** IPsec VPN management



**Step 2** In the navigation tree on the left, choose **IPSec VPN Resource Management** > **Network Domains**. On the right, click the name of network domain to access the network domain of the IPsec VPN service.

**Step 3** Click **Synchronize** to synchronize the tunnel of the device to eSight.

**Step 4** In **Tunnel List**, check the value of **Tunnel Status**.

**Figure 10-10** Tunnel status

| Synchronize |                 |                      |         |                |                      |               |           |
|-------------|-----------------|----------------------|---------|----------------|----------------------|---------------|-----------|
| Local SN    | Local Device IP | Local Port           | Peer SN | Peer Device IP | Peer Port            | Tunnel Status | Operation |
| 10          | 10.137.59.208   | GigabitEthernet0/0/1 | 10      | 10.137.59.206  | GigabitEthernet0/0/1 | Connected     |           |

----End

## 10.2 WLAN Management

This topic describes the basic concepts and configuration methods of the WLAN.

## 10.2.1 Basic Concepts

A WLAN is a network system that connects computers in wireless mode for communication and resource sharing.

The essential feature of a WLAN is that computers are connected to the network in wireless mode and no communication cables are required. Therefore, the network construction is more flexible and the terminal mobility is improved. Compared with the traditional wired access, the initiation and implementation of the WLAN is easier, and the maintenance cost is lower. Generally, you only need to deploy one or more access points (APs) to establish a Local Area Network (LAN) covering the whole building or area.

A WLAN uses wireless multiple access channels as the transmission media to provide traditional wired LAN services. Data is transmitted by radio waves on the WLAN. The WLAN technology is widely used in business districts, universities, airports, and other public areas.

**Table 10-2** Related Concepts of the WLAN

| Concept                                                    | Description                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP(Access Point)                                           | Connects wireless workstations to a LAN and converts frames transmitted between a WLAN and a wired LAN.                                                                          |
| FIT AP                                                     | Also referred to as a centralized control AP. The FIT AP cannot work independently, and needs to work with the AP Controller (AC) to implement the WLAN service access function. |
| AC(Access Controller)                                      | Controls and manages all APs on a WLAN, and provides authentication services for WLAN users by interacting with an authentication server.                                        |
| CAPWAP(Control And Provisioning of Wireless Access Points) | Transmits management packets and data packets between APs and ACs.                                                                                                               |
| SSID(Service Set Identifier)                               | The wireless terminal can scan all the networks and then selects a specified SSID to access a specified wireless network.                                                        |
| VAP(virtual Access Point)                                  | Service function entity on an AP. Users can create different VAPs for each radio frequency (RF) of an AP. A VAP is created by binding a service set to a specified RF of the AP. |

## 10.2.2 Network Scheme and Principle

The WLAN network schemes mainly include direct connection network and hung beside network.

### Direct Connection Network

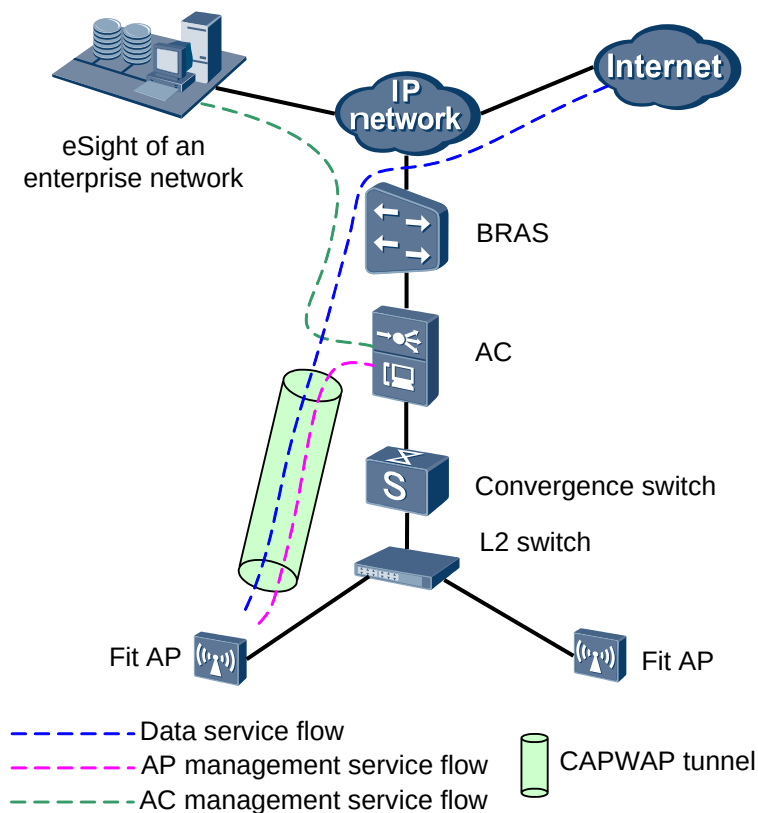
On a direct connection network, ACs are directly connected to the broadband remote access server (BRAS). ACs forward and process AP data services and AP management services uniformly. ACs on a direct connection network must have strong forwarding capabilities to function as the convergence layer. The direct connection network mode is applicable to a large scale and centralized WLAN and can simplify the network architecture.

In the direct connection network scheme, each AP establishes a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel with an AC. Management services must be encapsulated in CAPWAP tunnels. Data services can be encapsulated in CAPWAP tunnels.

Two configuration scenarios exist based on whether data services are encapsulated in CAPWAP tunnels.

- Scenario 1: Data services encapsulated in CAPWAP tunnels  
All the management services and data services are encapsulated in CAPWAP tunnels, including all the AP management services and end user data services. See [Figure 10-11](#). All the data services and AP management services are encapsulated in CAPWAP tunnels. Different Virtual Local Area Networks (VLANs) distinguish different services.

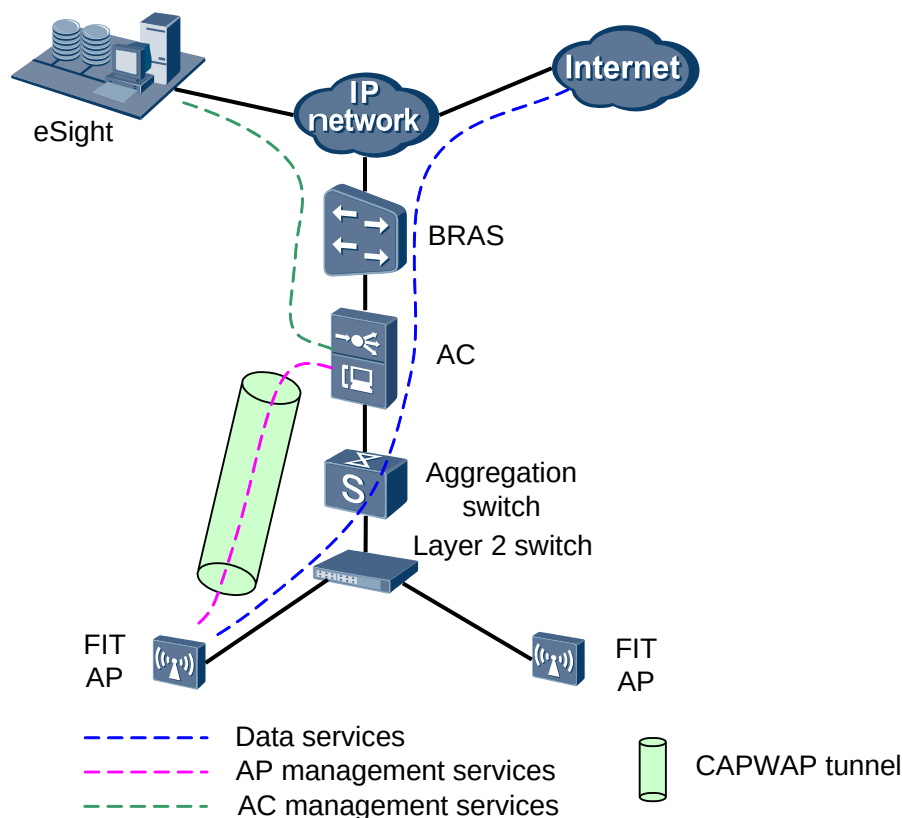
**Figure 10-11** Data services encapsulated in CAPWAP tunnels



In this mode, you only need to configure management VLANs on switches in advance. You do not need to configure data VLANs. The AP management VLANs connect APs to ACs.

- Scenario 2: Data services not encapsulated in CAPWAP tunnels  
The AP management services are encapsulated in CAPWAP tunnels; however, the AP data services are not encapsulated in CAPWAP tunnels. APs directly send data services to ACs, and then ACs forward the data services to the upper-layer devices. See [Figure 10-12](#). No data service is encapsulated in CAPWAP tunnels. Data services are forwarded from the AC to the upper-layer device. The AP management services are encapsulated by CAPWAP tunnels. Different VLANs distinguish different services.

**Figure 10-12** Data services not encapsulated in CAPWAP tunnels



In this mode, you need to configure management VLANs and data VLANs on switches in advance to distinguish different WLAN services.

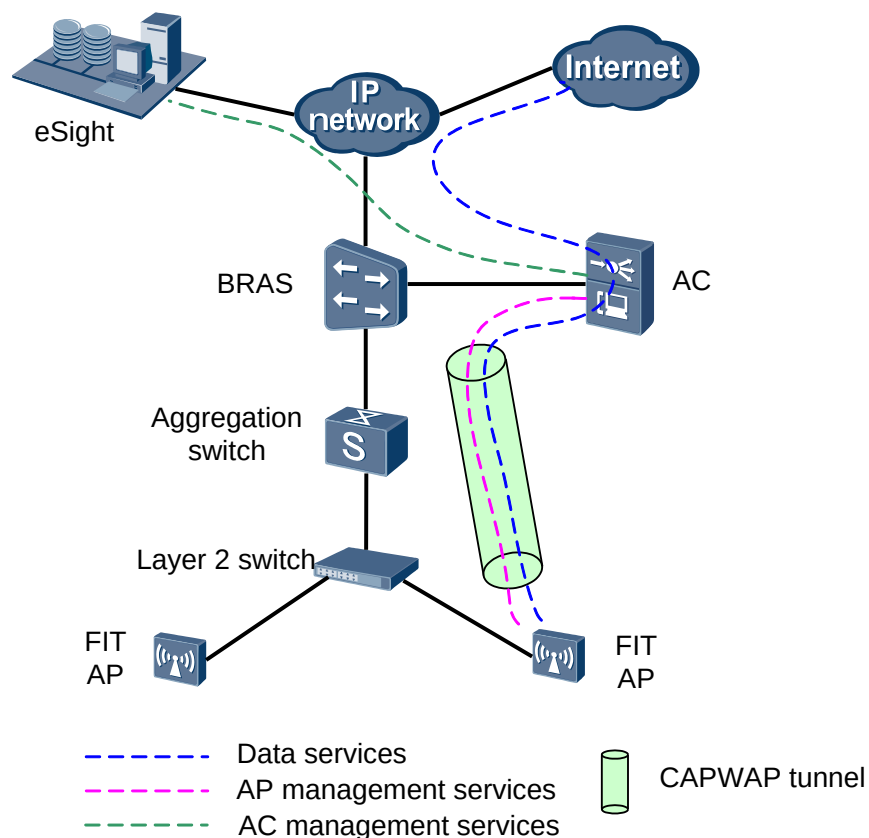
- On switches between APs and ACs, configure the AP management VLANs to connect APs to ACs.
- On switches between ACs and upper-layer devices, configure the data VLANs of users to distinguish different WLAN services.

## Hung Beside Network

In a hung beside network, ACs are hung beside the BRAS to manage the WLAN service of APs. In the hung beside network mode, ACs that are hung beside the BRAS manages all the APs that are deployed within the management area of the BRAS, and AC deployment is quite centralized. The hung beside network mode is applicable to scenarios in which APs are scattered throughout an entire area.

Two configuration scenarios exist based on whether data services are encapsulated in CAPWAP tunnels.

- **Scenario 1: Data services encapsulated in CAPWAP tunnels**  
All the management services and data services are encapsulated in CAPWAP tunnels, including all the AP management services and end user data services. See [Figure 10-13](#). All the data services and AP management services are encapsulated in CAPWAP tunnels. Different VLANs distinguish different services.

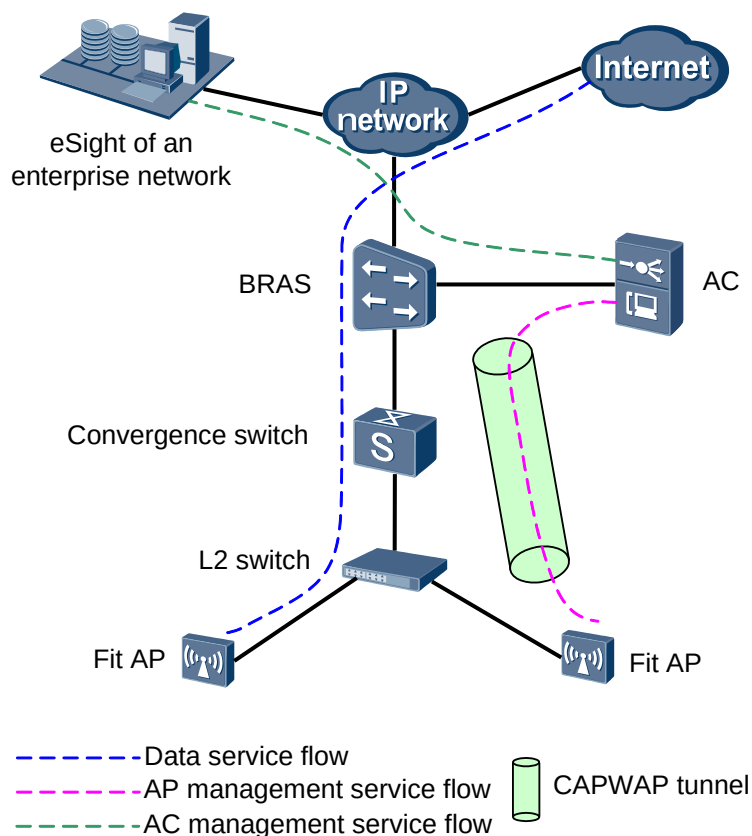
**Figure 10-13** Data services encapsulated in CAPWAP tunnels

In this mode, you only need to configure management VLANs on switches in advance. You do not need to configure data VLANs. The AP management VLANs connect APs to ACs.

- Scenario 2: Data services not encapsulated in CAPWAP tunnels

ACs only manage APs. Management services are encapsulated in CAPWAP tunnels. Data services are directly forwarded to the layer 2 switch, aggregation switch, and are transmitted to the upper-layer network by the BRAS. [Figure 10-14](#) shows the networking diagram.



**Figure 10-14** Data services not encapsulated in CAPWAP tunnels

- ACs are hung beside the BRAS to manage APs. All the AP management services are transmitted to ACs.

The BRAS enables the Dynamic Host Configuration Protocol (DHCP) server function to allocate IP addresses for APs. APs find ACs by using the Domain Name Service (DNS) or DHCP Option43/option60. Or, an AC functions as the DHCP server of APs and directly allocates IP addresses for the APs. The VLANIF corresponding to the VLAN accessed by the AP enables the DHCP server function.

- The AP data services are forwarded on the local host without passing through ACs.

End users can configure various service VLANs based on various SSIDs and configure a Layer 2 switch and an aggregation switch to identify the service VLANs. The service VLANs are forwarded to and terminated by the upper-layer BRAS. The BRAS controls end user access and allocates IP addresses for end users. The BRAS authenticates the user identity based on the authentication manner. After the authentication is successful, packets of the user can access the network.

## Comparison Between the Direct Connection Network and the Hung Beside Network

ACs can be directly connected to the BRAS or hung beside the BRAS. [Table 10-3](#) compares the direct connection network with the hung beside network.

**Table 10-3** Comparison between the direct connection network and the hung beside network

| Item                 | Direct Connection Network                                                                                                                                                                                       | Hung Beside Network                                                                                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Implementation       | ACs are directly connected to the BRAS. ACs forward and process AP data services and AP management services uniformly.                                                                                          | ACs are hung beside the BRAS to manage the WLAN service of APs.                                                                                                                                                                                                       |
| Application scenario | ACs have strong forwarding capabilities to function as the convergence layer. The direct connection network mode is applicable to a large scale and centralized WLAN and can simplify the network architecture. | ACs that are hung beside the BRAS manages all the APs that are deployed within the management area of the BRAS, and AC deployment is quite centralized. The hung beside network mode is applicable to scenarios in which APs are scattered throughout an entire area. |

### 10.2.3 Overview

This topic describes the WLAN configuration operations.

[Figure 10-15](#) shows the overview of WLAN configuration operations.

Figure 10-15 Overview of WLAN configuration operations

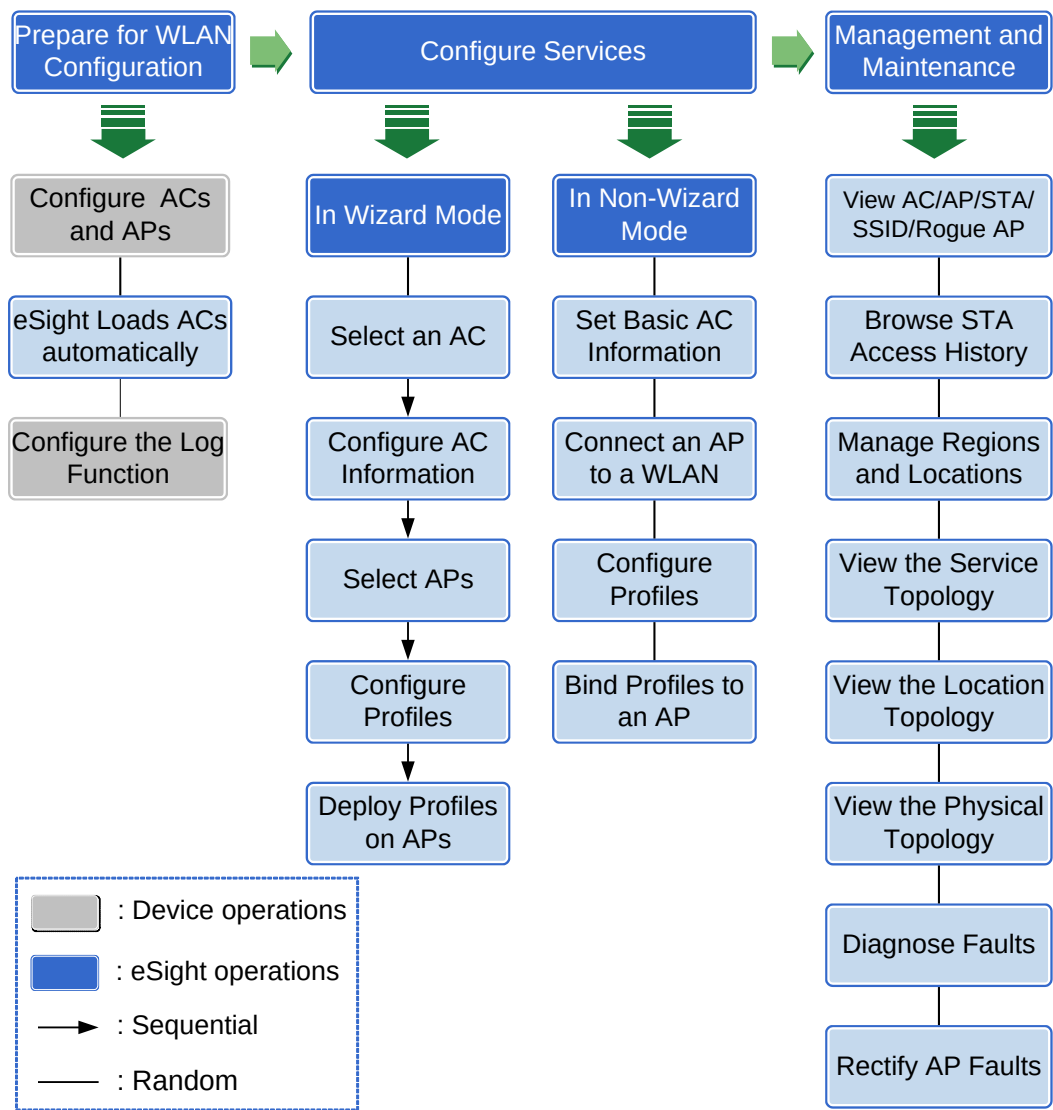


Table 10-4 lists the WLAN configuration operations.

Table 10-4 WLAN configuration operations

| Stage                          | Operation Description                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prepare for WLAN configuration | Prepare for WLAN configuration and management. <ul style="list-style-type: none"><li>Configure ACs and APs, and verify that the management channels and service channels between ACs and APs function properly.</li><li>eSight loads ACs automatically.</li><li>Before the log function is configured on a device, the device cannot record the STA access history, top N user login fail rate statistics, and top N user login count statistics.</li></ul> |
| Configure services             | <a href="#">10.2.5.1 Configuring the WLAN Service in Wizard Mode</a>                                                                                                                                                                                                                                                                                                                                                                                        |

| Stage                      | Operation Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <p>describes the detailed procedure for configuring the WLAN service.</p> <p>To configure the WLAN service in non-wizard mode, proceed as follows:</p> <ol style="list-style-type: none"><li>1. Configure AC basic information: Create an AC, and set the AC source interface, authentication mode, and forwarding type.</li><li>2. Bring APs online.</li><li>3. Configure profiles: Configure the AP profile, radio profile, and ESS profile.</li><li>4. Bind profiles to APs: Bind profiles to APs to complete the service configuration for APs.</li></ol> <p><b>NOTE</b></p> <p>You can use predefined system templates in the smart configuration tool to batch configure basic WLAN services for multiple devices. For details, see "Delivering a Template" in "Smart Configuration Tool".</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Management and maintenance | <ul style="list-style-type: none"><li>• View AC/AP/STA/SSID/Rogue AP: eSight allows you to browse the detailed information about ACs, APs, stations(STAs), SSIDs, and rogue APs on the entire network.</li><li>• Manage Regions and Locations: You can simulate the existing network to construct a virtual network architecture and add APs to the architecture, which makes it easy for you to view APs and facilitates operation and maintenance.</li><li>• View the service topology: You can view ACs, APs, rogue APs, STAs, and the logical relationship between them in the service topology.</li><li>• View the location topology: You can view the current signal coverage scope and current device status, and simulate actual networks in the location topology to facilitate daily maintenance.</li><li>• View the physical topology: The eSight supports integrated wired and wireless topology management. The physical topology shows AP alarms, states, links, and network structure, which help you rapidly locate faults. For details, see "Browsing a Physics View" in "Topology Management".</li><li>• Diagnose faults: eSight provides the fault diagnosis function for you to locate service faults.</li><li>• Rectify AP faults: eSight allows you to restore APs to factory settings, restart APs, or replace APs based on the site scenario to quickly rectify faults.</li></ul> |

## 10.2.4 Configuring the Log Function

Before the log function is configured on a device, the device cannot record the STA access history, top N user login fail rate statistics, and top N user login count statistics.

## Prerequisites

- eSight has installed on the Linux server.
- The type of the AC is **ACU** or **AC6605**.
- IP addresses and routing protocols are configured to ensure reachable routes between the AC and the Linux server.

## Context

During the daily maintenance, technical support personnel need to deal with STA access problems. eSight provides user login fail rate statistics and logs about user login fails. The statistics and logs provide evidence for technical support personnel to judge whether the network is robust and can easily locate user login failures.

After the log function is configured, the AC records the access history of STAs to the WLAN in the logs, and sends the logs to the Linux server. eSight periodically parses the logs and saves STA access information. Therefore, the log function must be configured on both the AC and the Linux server.

## Procedure

- Configure the log function on the AC.

The configuration process is as follows:

1. Enable the information center.
2. Name the tunnel.
3. Configure the channel for outputting logs.



### NOTE

Set the name of the module that outputs logs to **CM**.

4. Configure the source interface that sends logs.
5. Configure the log host.



### NOTE

Set the IP address of the log host to the IP address of the Linux server. Configure the same channel as that is configured in the preceding process.

Configuration Example:

```
<Huawei> system-view
[Huawei] info-center enable
[Huawei] info-center channel 0 name channel0
[Huawei] info-center source CM channel channel0 log level notifications
[Huawei] info-center loghost source Ethernet0/0/0
[Huawei] info-center loghost 192.168.1.10 channel channel0 facility local0
[Huawei] quit
```



### NOTE

You can configure the log function by using command lines or the intelligent configuration tool. Using the system template **Configure WLAN Syslog** predefined in the intelligent configuration tool can easily configure the log function.

- Configure the log function on the Linux server.
  1. Log in to the server as the **root** user.
  2. Change the configuration file **/etc/syslog-ng/syslog.conf**.
    - a. Open the configuration file **/etc/syslog-ng/syslog.conf** in the vi editor.

```
vi /etc/syslog-ng/syslog.conf
```

- b. Move the cursor to the bottom and press **a** to enter the editing mode.
- c. Enter the following contents:

```
filter f_wlansta { match("[\\s\\S]*WLAN_STA_INFO[\\s\\S]*"); };

Destination wlanstadst{file("/var/log/wlan/$YEAR.$MONTH.$DAY.$hour.stalog"
template("$UNIXTIME#$HOST [$LEVEL] $MSG\n")
template_escape(no)
frac_digits(3)
create_dirs(yes));};

log {source(src);filter(f_wlansta);destination(wlanstadst);};
```



## CAUTION

The source **source(src)** uses the default configuration **udp(ip("0.0.0.0") port(514))** of the log server. Ensure that the # at the beginning of the sentence has been deleted.

---

- d. Press **Esc** to exit the editing mode.
  - e. Enter **:wq!** and press **Enter** to save and close the editing page.
3. Restart the log service for the settings to take effect.
  - a. Run the following command to check the **syslog** process status.

```
ps -ef|grep syslog
```

If information similar to the following is displayed, the **syslog** process is running properly.

```
root 5367 3019 0 10:36 pts/1 00:00:00 grep syslog
root 23212 1 0 Mar23 ? 00:00:01 /sbin/syslog-ng
```

- b. Run the following command to stop the **syslog** service.

```
service syslog stop
```

If information similar to the following is displayed, the command to stop the **syslog** process is executed.

```
Shutting down syslog services done
```

- c. Wait for five seconds and run the following command to check whether the **syslog** process stops.

```
ps -ef|grep syslog
```

If information similar to the following is displayed (the **/sbin/syslog-ng** information is not displayed), the **syslog** process stops.

```
root 5967 3019 0 11:18 pts/1 00:00:00 grep syslog
```

- d. Confirm that the **syslog** process stops. Run the following command to restart the **syslog** process.

```
service syslog start
```

If information similar to the following is displayed, the command to restart the **syslog** process is executed.

```
Starting syslog services done
```

- e. Wait for five seconds and run the following command to check whether the **syslog** process restarts.

```
ps -ef|grep syslog
```

If information similar to the following is displayed, the **syslog** process restarts.

```
root 5367 3019 0 10:36 pts/1 00:00:00 grep syslog
root 23212 1 0 Mar23 ? 00:00:01 /sbin/syslog-ng
```

----End

## 10.2.5 Configuring Services

This topic describes how to configure the WLAN service.

### 10.2.5.1 Configuring the WLAN Service in Wizard Mode

This topic describes how to configure the WLAN service in wizard mode.

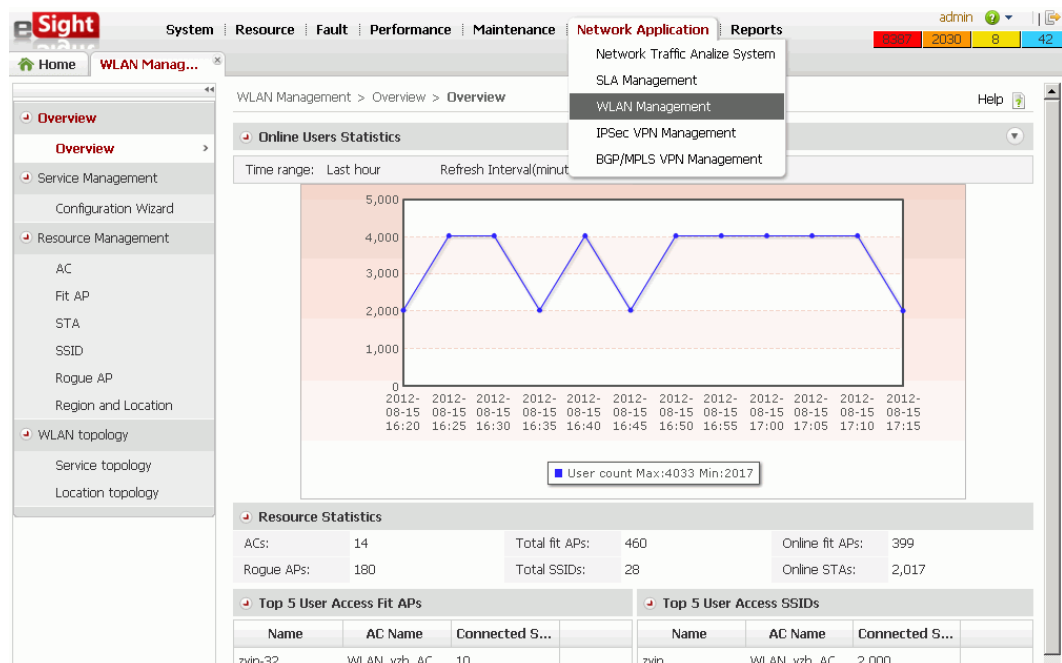
#### Prerequisites

- ACs have been created in eSight.
- APs and ACs are connected properly.
- The SNMP read and write permissions have been configured.

#### Procedure

**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-16 Overview



**Step 2** In the navigation tree, choose **Service Management > Configuration Wizard**.

**Figure 10-17** Configuration wizard

WLAN Management > Service Management > Configuration Wizard

You can use an AP profile to import APs. [Download an AP profile](#)

Progress: Select an AC (Current) | Configure AC information | Select APs | Configure profiles | Deploy profiles on APs

Name:  Type:   
IP address:

| Status  | Name            | IP Address    | Type      | AP Authentication | Forwarding Type | Country...    |
|---------|-----------------|---------------|-----------|-------------------|-----------------|---------------|
| Online  | WLAN_ACU_1      | 13.0.0.1      | SPU       | No authentication | AP              | CN(CHINA)     |
| Offline | AC6605-master   | 10.136.12.88  | AC6605-AC | No authentication | ESS             | CN(CHINA)     |
| Online  | WS6603_184      | 10.137.59.184 | WS6603    | SN                | ESS             |               |
| Online  | VASP_204        | 10.137.59.204 | SPU       | No authentication | ESS             | CN(CHINA)     |
| Online  | WS6605_AC_54_23 | 10.136.54.235 | AC6605-AC | No authentication | ESS             | AE(UNITED...) |
| Online  | WLAN_ACU_2      | 13.0.0.2      | AC6605-AC | No authentication | AP              | CN(CHINA)     |
| Online  | WLAN_58         | 10.137.59.58  | SPU       | No authentication | AP              | IN(INDIA)     |
| Online  | V2R1_SPU_1      | 10.138.35.66  | AC6605-AC | No authentication | AP              | CN(CHINA)     |
| Online  | SPU_V2R2_SPU_1  | 10.137.58.210 | SPU       | SN                | ESS             | CN(CHINA)     |
| Online  | wlan119         | 10.137.61.119 | SPU       | SN                | ESS             |               |

Total records: 11  records  / 1

**Step 3** Select an AC, and click **Next**.



**NOTE**

- Click **Synchronize** to synchronize the WLAN service in eSight with that on the live network.
- To add APs to eSight in batches, click **Download an AP profile** to import AP information to a plan sheet.

**Step 4** Set the AC basic attributes, including **Interface name**, **AP authentication mode**, **Forward type** and **Country Code**.

- When **Forwarding type** is set to **ESS**, APs forward data in the forwarding mode set in the bound ESS profile.
- When **Forwarding type** is set to **AP**, APs forward data in the forwarding mode set when APs are created.
- Country Code**: The AC of the SPU type support this parameter.

**Figure 10-18** Configure AC information

Progress: Select an AC | **Configure AC information** (Current) | Select APs | Configure profiles | Deploy profiles on APs

\*Interface name:

AP authentication mode:

Forwarding type:

Country Code:



**NOTE**

If an AP whose identity is confirmed exists in eSight, the AC attributes cannot be changed.

**Step 5** Click **Add AP**, select required APs, and click **OK**. Then click **Next**.

**Figure 10-19** Select APs

**Select APs**

Name:  Status:  IP address:  Location:

**+ Add AP**

| <input type="checkbox"/>            | Stat... | Name   | Alias | SN    | MAC        | IP Addr... | Location |
|-------------------------------------|---------|--------|-------|-------|------------|------------|----------|
| <input checked="" type="checkbox"/> | ● O...  | zyin-4 |       | zyin4 | 09-33-3... | 192.168... |          |
| <input checked="" type="checkbox"/> | ● O...  | zyin-3 |       | zyin3 | 09-33-3... | 192.168... |          |
| <input type="checkbox"/>            | ● O...  | zyin-2 |       | zyin2 | 09-33-3... | 192.168... |          |
| <input type="checkbox"/>            | ● O...  | zyin-1 |       | zyin1 | 09-33-3... | 192.168... |          |
| <input type="checkbox"/>            | ● O...  | zyin-0 |       | zyin0 | 09-33-3... | 192.168... |          |

Total records: 5  records /1

**NOTE**

You can add APs in either of the following ways:

- Choose **Add AP > Create Manually**, and create APs offline.
- Choose **Add AP > Batch Import**, and import an AP plan sheet to create APs in batches.

**Step 6** Configure an AP profile, a radio profile, and an ESS profile, bind them to APs, and click **Next**.

**Figure 10-20** Configure profile

Select an AC    Configure AC inform...    Select APs    **Configure profiles**    Deploy profiles on A...

AP profile:  ...

**Configure radio:**

+ Create

**Radio Configuration 1** X Delete

\*Radio ID:

\*RF profile:  ...

Working status:

Bandwidth:

Channel value:

Transmit power level:

Available antennas:

\*ESS profile:  + Add  
X Clear

**NOTE**

You can bind multiple ESS profiles to an AP.

**Step 7 Optional:** Select **Add to whitelist**.

**Figure 10-21** Deploy profiles on APs

Select an AC   Configure AC inform...   Select APs   Configure profiles   Deploy profiles on A...

⚠ If you close the page or switch to another page, the deployment still continues on the eSight server. But you can not view the deployment results.

| Name   | Type    | SN    | MAC               | IP Address  | Deploy Status | Result |
|--------|---------|-------|-------------------|-------------|---------------|--------|
| zyin-4 | WA633DN | zyin4 | 09-33-33-34-01-05 | 192.168.0.6 |               |        |
| zyin-3 | WA633DN | zyin3 | 09-33-33-34-01-04 | 192.168.0.5 |               |        |

Total records: 2   20 records   1/1   Go

☒ Add to whiteList

Previous   Deploy   Cancel

**Step 8** Click **Deploy**.

**Step 9** When the service is deployed, click **Finish**.

----End

### 10.2.5.2 Setting Basic AC Information

Set the basic AC information that will be used by eSight to load APs.

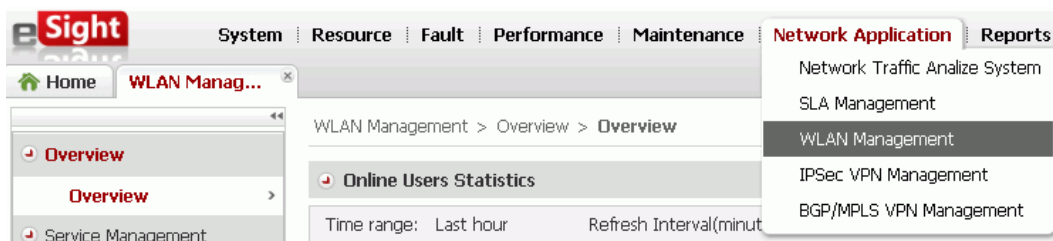
#### Prerequisites

SNMP write permission is set.

#### Procedure

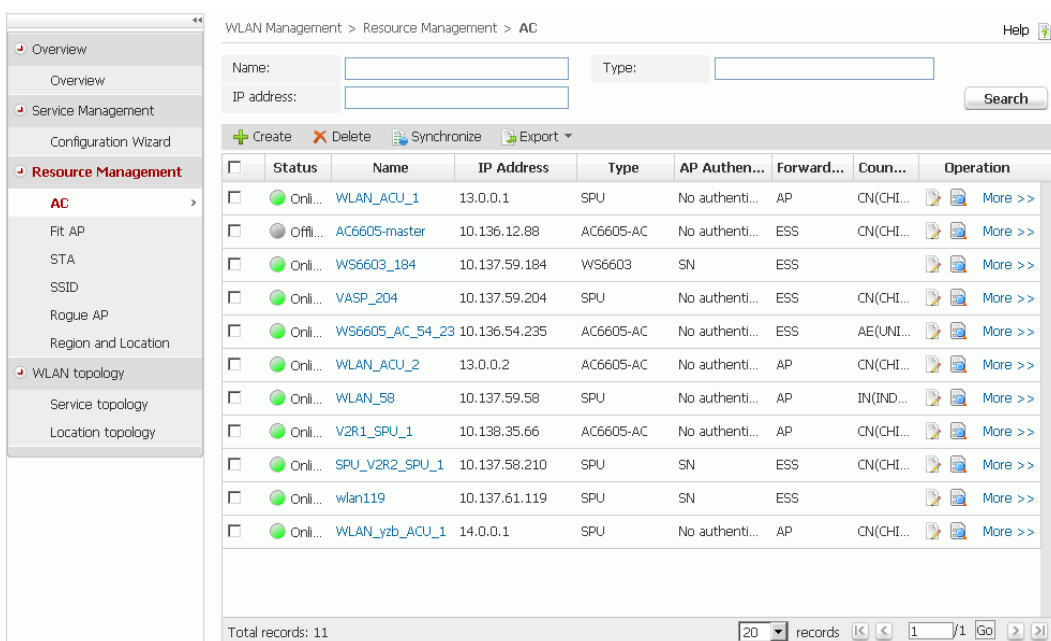
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-22 WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management > AC**.

Figure 10-23 AC list



**Step 3** In the pane on the right, click **Create**.

**Step 4** In the displayed **Create AC** window, click **Select**. In the window that is displayed, select an AC and click **OK** to create an AC.

Figure 10-24 Creating AC

**NOTE**

To create an AC of the SPU type, ensure that the AC runs WLAN services.

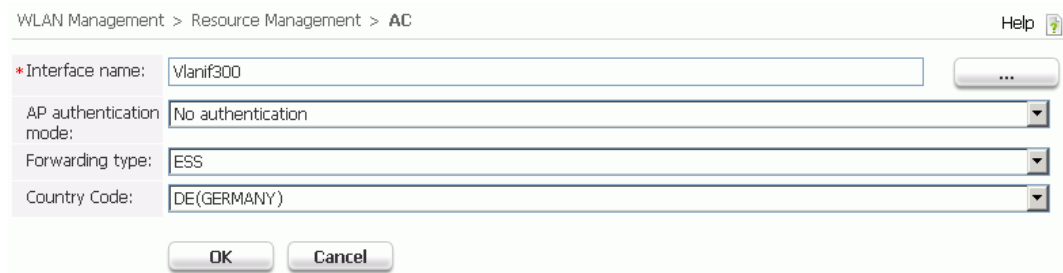
**Step 5** Click  to set the basic parameters of the AC.

**Step 6** After **Interface name**, click **Select**, select an interface, and click **OK**.

**NOTE**

On the WS6603, no interface parameter can be selected.

**Figure 10-25** AC basic parameters



**Step 7** Set **AP authentication mode**, **Forward type** and **Country Code**.

**Table 10-5** AC basic parameters

| Parameter              | Description                                                                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP authentication mode | <ul style="list-style-type: none"><li><b>No authentication:</b> The AP is automatically connected to the AC.</li><li><b>MAC or SN:</b> A user must manually create the AP in offline mode, or add the AP MAC or SN to the whitelist, or determine the rogue AP in online mode.</li></ul> |
| Forwarding type        | <ul style="list-style-type: none"><li><b>ESS:</b> The AP forwards user data in the mode specified by the ESS profile bound to the AP.</li><li><b>AP:</b> The AP forwards user data in the mode set by the AP.</li></ul>                                                                  |
| Country Code           | The AC of the SPU type support this parameter.                                                                                                                                                                                                                                           |

----End

## Follow-up Procedure

After the AC is configured, click **Name** and view the AC information in the **AC Information** window that is displayed.

### 10.2.5.3 Connecting an AP to a WLAN

To connect an AP managed by an AC to a WLAN, you can add the AP in offline mode, add the AP to the whitelist, or manually identify a rogue AP.

## Prerequisites

A VLAN is configured.

The basic functions of the AC are configured.

The AP is connected to an AC.

The AC is set to report alarms to the eSight server.

SNMP write permission is set.

## Context

The process of connecting an AP to a WLAN is as follow:

- If an AP is added in offline mode, this AP can be directly connected to a WLAN.
- If an AP is not added in offline mode, but **AP authentication mode** is set to **No authentication**, or AP MAC or SN is in the set **Whitelist**, the AP is automatically added and connected to the WLAN.
- If an AP does not exist in the whitelist or AP list, and **AP authentication mode** is not set to **No authentication**, the AP is in the unauthorized AP list. You can identify the AP in the unauthorized AP list to determine whether to add the AP to the WLAN.

## Procedure

**Step 1** Choose **Network Application > WLAN Management**.

**Figure 10-26** WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management > AC**.

**Figure 10-27** AC list

WLAN Management > Resource Management > AC

Name:  Type:

IP address:

| <input type="checkbox"/> | Status   | Name            | IP Address    | Type      | AP Authen...   | Forward... | Coun...   | Operation |
|--------------------------|----------|-----------------|---------------|-----------|----------------|------------|-----------|-----------|
| <input type="checkbox"/> | Onli...  | WLAN_ACU_1      | 13.0.0.1      | SPU       | No authenti... | AP         | CN(CHI... | More >>   |
| <input type="checkbox"/> | Offli... | AC6605-master   | 10.136.12.98  | AC6605-AC | No authenti... | ESS        | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | WS6603_184      | 10.137.59.184 | WS6603    | SN             | ESS        |           | More >>   |
| <input type="checkbox"/> | Onli...  | VASP_204        | 10.137.59.204 | SPU       | No authenti... | ESS        | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | WS6605_AC_54_23 | 10.136.54.235 | AC6605-AC | No authenti... | ESS        | AE(UNI... | More >>   |
| <input type="checkbox"/> | Onli...  | WLAN_ACU_2      | 13.0.0.2      | AC6605-AC | No authenti... | AP         | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | WLAN_58         | 10.137.59.58  | SPU       | No authenti... | AP         | IN(IND... | More >>   |
| <input type="checkbox"/> | Onli...  | V2R1_SPU_1      | 10.138.35.66  | AC6605-AC | No authenti... | AP         | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | SPU_V2R2_SPU_1  | 10.137.58.210 | SPU       | SN             | ESS        | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | wlan119         | 10.137.61.119 | SPU       | SN             | ESS        |           | More >>   |
| <input type="checkbox"/> | Onli...  | WLAN_yzb_ACU_1  | 14.0.0.1      | SPU       | No authenti... | AP         | CN(CHI... | More >>   |

Total records: 11  records  / 1

Select the AP connecting mode according to the actual networking. See [Add an AP in offline mode](#), [Add an AP to the whitelist](#), and [Add a unauthorized AP](#).

**Step 3** Add an AP in offline mode.

1. In the pane on the right, click in **Operation**.

**Figure 10-28** AP list

WLAN Management > Resource Management > AC > **AP** [Back](#) [Help](#)

Name:  Status:

Type:  IP address:

Location:

Create Delete Bind Profile Synchronize Restart Restore Factory Settings

| <input type="checkbox"/> | Status | Name  | Alias | Type    | SN    | MAC         | IP Address   | AP R... | Location | Operati... |
|--------------------------|--------|-------|-------|---------|-------|-------------|--------------|---------|----------|------------|
| <input type="checkbox"/> | Onl... | zyin5 |       | WA63... | zyin5 | D8-01-01... | 193.168.0.12 | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin4 |       | WA63... | zyin4 | D8-01-01... | 193.168.0.11 | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin3 |       | WA63... | zyin3 | D8-01-01... | 193.168.0.4  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin2 |       | WA63... | zyin2 | D8-01-01... | 193.168.0.3  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin1 |       | WA63... | zyin1 | D8-01-01... | 193.168.0.2  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin0 |       | WA63... | zyin0 | D8-01-01... | 193.168.0.1  | zyin    |          |            |

Total records: 6 20 records 1 / 1

2. Click **Create**.
3. Set AP parameters.



**Figure 10-29** Creating AP

WLAN Management > Resource Management > AC > AP > Create Help

|                       |                   |            |       |
|-----------------------|-------------------|------------|-------|
| *Name:                | AP1002            | Alias:     |       |
| SN:                   | AP1002            | MAC:       |       |
| Location:             |                   | Type:      | WA601 |
| Type:                 |                   | Antenna:   |       |
| Data forwarding mode: | Direct forwarding | AP region: | zyin  |
| AP profile:           | ap-profile-0      |            |       |

RF profile: + Bind ✗ Unbind

| <input type="checkbox"/> | Radi... | Radi... | Work... | Band... | Chan... | Operati... | Transmi... | Operatin... | Availabl... |
|--------------------------|---------|---------|---------|---------|---------|------------|------------|-------------|-------------|
| <input type="checkbox"/> | 1       | zyin    | Open    | 20MHz   | 1       |            | 1          |             | All         |

ESS profile: + Bind ✗ Unbind

| <input type="checkbox"/> | Radio ID | ESS Profile Name | SSID | ESS Type |
|--------------------------|----------|------------------|------|----------|
| <input type="checkbox"/> | 1        | zyin             | zyin | Service  |

OK Cancel

- After **AP region** or **AP profile**, click **Select** and set the parameters.
- After **RF profile** and **ESS profile**, click **Bind** to bind corresponding profiles.
- Click **OK**.

**Step 4** Add an AP to the whitelist.

1. In the pane on the right, choose **More > AP Whitelist**.

**Figure 10-30** AC operation

Create

Delete

Synchronize

Export

| <input type="checkbox"/> | Status                                   | Name     | IP Address    | Type | AP Authen...   | Forward... | Coun...   | Operation                                                 |
|--------------------------|------------------------------------------|----------|---------------|------|----------------|------------|-----------|-----------------------------------------------------------|
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> | WLAN_58  | 10.137.59.58  | SPU  | MAC            | AP         | IN(IND... | <div><div></div><div></div><div>More &gt;&gt;</div></div> |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> | WLAN_106 | 10.137.66.106 | SPU  | No authenti... | AP         | C         | <div><div></div><div>AP Profile</div></div>               |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> | WLAN_35  | 10.137.66.106 | SPU  | No authenti... | AP         | C         | <div><div></div><div>RF Profile</div></div>               |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> |          |               |      |                |            |           | <div><div></div><div>ESS Profile</div></div>              |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> |          |               |      |                |            |           | <div><div></div><div>AP Region</div></div>                |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> |          |               |      |                |            |           | <div><div></div><div>Unauthorized AP</div></div>          |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> |          |               |      |                |            |           | <div><div></div><div>AP Whitelist</div></div>             |
| <input type="checkbox"/> | <div><div></div><div>Onli...</div></div> |          |               |      |                |            |           | <div><div></div><div>View Service Topology</div></div>    |

**Figure 10-31** Creating AP whitelist

WLAN Management > Resource Management > AC > AP Whitelist > Create Help

|      |                   |
|------|-------------------|
| MAC: | 01-02-23-15-10-01 |
| SN:  |                   |

4. Click **OK**.

**Figure 10-32** AP whitelist list

WLAN Management > Resource Management > AC > AP Whitelist Back Help

|     |  |      |  |                                       |
|-----|--|------|--|---------------------------------------|
| SN: |  | MAC: |  | <input type="button" value="Search"/> |
|-----|--|------|--|---------------------------------------|

| <input type="checkbox"/> | SN    | MAC               |
|--------------------------|-------|-------------------|
| <input type="checkbox"/> |       | 01-02-23-15-10-01 |
| <input type="checkbox"/> |       | C9-01-01-01-01-04 |
| <input type="checkbox"/> | zyin0 |                   |

**Step 5** Add a unauthorized AP.

1. In the pane on the right, choose **More > Unauthorized AP** and click **Synchronize**.
2. Click a unauthorized AP and click **Confirm AP identities**.

**Figure 10-33** Unauthorized AP list

WLAN Management > Resource Management > AC > Unauthorized AP Back Help

|             |  |       |  |
|-------------|--|-------|--|
| SN:         |  | MAC:  |  |
| IP Address: |  | Type: |  |

| <input type="checkbox"/> | Detected At        | SN         | MAC               | IP Address     | Type    |
|--------------------------|--------------------|------------|-------------------|----------------|---------|
| <input type="checkbox"/> | 2011-4-13 21:36:31 | AB26002913 | 5C-4C-A9-07-FF-51 | 192.168.58.254 | WA603SN |

----End

## 10.2.5.4 Configuring an AP Profile

An AP profile integrates AP configuration. By default, eSight automatically binds an AP profile to an AP. A user can modify the bound AP profile as required.

### Prerequisites

SNMP write permission is set.

## Procedure

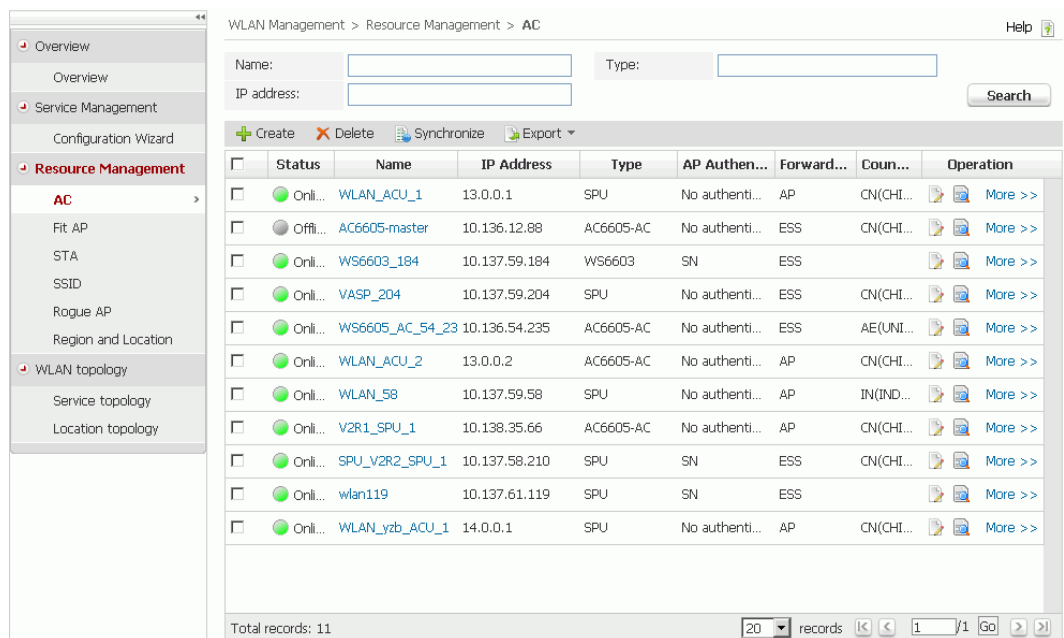
**Step 1** Choose **Network Application** > **WLAN Management**.

**Figure 10-34** WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management** > **AC**.

**Figure 10-35** AC list



**Step 3** In the pane on the right, choose **More** > **AP Profile**.

**Figure 10-36** AC operation

| Create  Delete  Synchronize  Export ▾ |         |          |               |      |                |            |           |           |
|---------------------------------------|---------|----------|---------------|------|----------------|------------|-----------|-----------|
| <input type="checkbox"/>              | Status  | Name     | IP Address    | Type | AP Authen...   | Forward... | Coun...   | Operation |
| <input type="checkbox"/>              | Onli... | WLAN_58  | 10.137.59.58  | SPU  | MAC            | AP         | IN(IND... | More >>   |
| <input type="checkbox"/>              | Onli... | WLAN_106 | 10.137.66.106 | SPU  | No authenti... | AP         | C         | More >>   |
| <input type="checkbox"/>              | Onli... | WLAN_35  | 10.137.66.106 | SPU  | No authenti... | AP         | C         | More >>   |

AP Profile  
 RF Profile  
 ESS Profile  
 AP Region  
 Unauthorized AP  
 AP Whitelist  
 View Service Topology

**Step 4** Click **Create**. In the window that is displayed, set AP profile parameters.

**Figure 10-37** Creating AP profile

WLAN Management > Resource Management > AC > AP Profile > **Create** Help

|                       |                                               |
|-----------------------|-----------------------------------------------|
| *Name:                | <input type="text" value="APProfile1"/>       |
| MTU:                  | <input type="text" value="1500"/>             |
| Log Backup Mode:      | <input type="text" value="Automatic backup"/> |
| Log Backup Server IP: | <input type="text" value="192.168.1.10"/>     |

**Step 5** Click **OK**. The new AP profile is displayed in the list.

**Figure 10-38** AP profile list

WLAN Management > Resource Management > AC > **AP Profile** Back Help

Name:

Create Delete Synchronize

| <input type="checkbox"/> | Name       | MTU  | Log Backup ...   | Log Backup ... | Operation |
|--------------------------|------------|------|------------------|----------------|-----------|
| <input type="checkbox"/> | APProfile1 | 1500 | Automatic bac... | 192.168.1.10   |           |
| <input type="checkbox"/> | zyin       | 1500 | Automatic bac... |                |           |

**NOTE**

Click to modify AP profile parameters.

----End

## 10.2.5.5 Configuring a RF Profile

An AP communicates with a terminal through radio channels. Configure the AP with a RF profile to make the AP runs properly.

### Prerequisites

SNMP write permission is set.

### Procedure

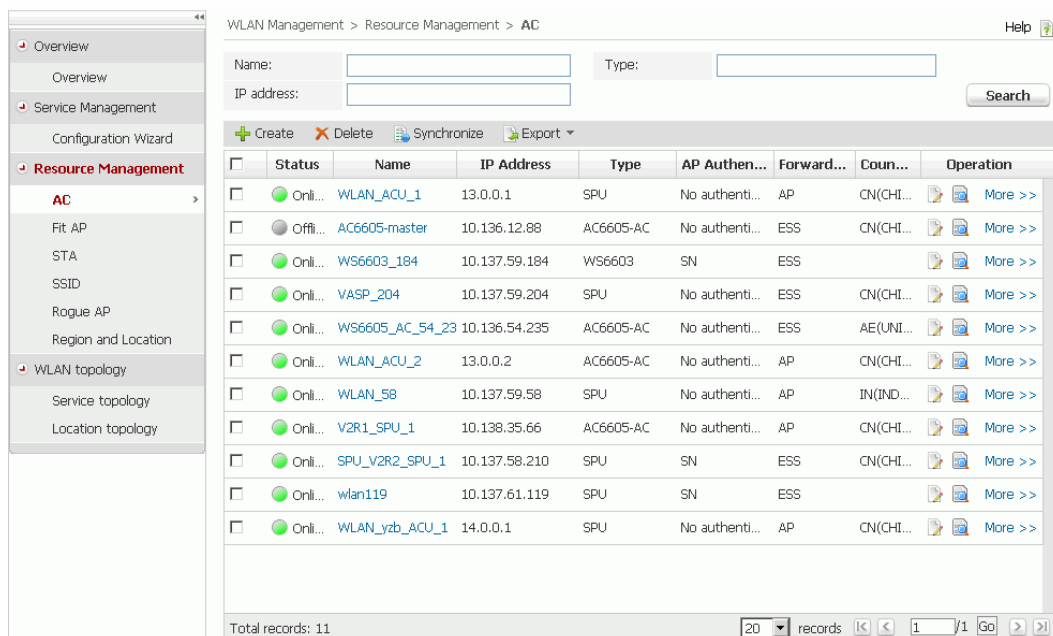
**Step 1** Choose **Network Application > WLAN Management**.

**Figure 10-39** WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management > AC**.

**Figure 10-40** AC list



**Step 3** In the pane on the right, choose **More > RF Profile**.

**Figure 10-41** AC operation

| + Create   X Delete   Synchronize   Export ▾ |         |          |               |      |                |            |           |           |
|----------------------------------------------|---------|----------|---------------|------|----------------|------------|-----------|-----------|
| <input type="checkbox"/>                     | Status  | Name     | IP Address    | Type | AP Authen...   | Forward... | Coun...   | Operation |
| <input type="checkbox"/>                     | Onli... | WLAN_58  | 10.137.59.58  | SPU  | MAC            | AP         | IN(IND... | More >>   |
| <input type="checkbox"/>                     | Onli... | WLAN_106 | 10.137.66.106 | SPU  | No authenti... | AP         | C         |           |
| <input type="checkbox"/>                     | Onli... | WLAN_35  | 10.137.66.106 | SPU  | No authenti... | AP         | C         |           |

**Step 4** Click **Create**. In the window that is displayed, set RF profile parameters.

**Figure 10-42** Creating RF profile

WLAN Management > Resource Management > AC > RF Profile > Create Help ?

|                |            |
|----------------|------------|
| *Name:         | RFProfile1 |
| RF Type:       | 802.11bg   |
| Rate Mode:     | Automatic  |
| Rate (Mbit/s): | 54         |
| Channel Mode:  | Automatic  |
| Power Mode:    | Automatic  |

- When **Channel Mode** is set to **Automatic**, the AP automatically selects an unused channel. When multiple APs are available in a region, channels set for the adjacent nodes must be five channels away from each other.
- When **Power Mode** is set to **Automatic**, the AP automatically selects transmit power. The greater the transmit power, the longer the transmission distance. Power selection not only involves power coverage and maximum number of clients but also impacts on other devices in the same region.
- **Rate**: Maximum bit rate that can be supported by an AP. Transmission distance varies with the bit rate. The lower the bit rate, the longer the transmission distance.

**Step 5** Click **OK**. The new RF profile is displayed in the list.

**Figure 10-43** RF profile list

WLAN Management > Resource Management > AC > RF Profile [Back](#) [Help](#)

Name:  RF Type:

Create Delete Synchronize

| <input type="checkbox"/> | Name       | RF Type  | Rate M... | Rate (M... | Channel... | Power ... | Operation |
|--------------------------|------------|----------|-----------|------------|------------|-----------|-----------|
| <input type="checkbox"/> | aaan       | 802.11a  | Automatic | 48         | Automatic  | Automatic |           |
| <input type="checkbox"/> | ABCD       | 802.11bg | Automatic | 54         | Automatic  | Automatic |           |
| <input type="checkbox"/> | an         | 802.11a  | Automatic | 54         | Automatic  | Automatic |           |
| <input type="checkbox"/> | mmm        | 802.11bg | Automatic | 54         | Automatic  | Manual    |           |
| <input type="checkbox"/> | RFProfile1 | 802.11bg | Automatic | 54         | Automatic  | Automatic |           |
| <input type="checkbox"/> | zyin       | 802.11bg | Automatic | 54         | Automatic  | Automatic |           |

**NOTE**

Click to modify RF profile parameters.

----End

## 10.2.5.6 Configuring an ESS Profile

Extended service set (ESS) is a set of service parameters. When bound to the specified radio channel of an AP, the service parameters are applied to a wireless service function entity, VAP object. In this case, the AP provides differentiated wireless functions for users based on the service parameters.

### Prerequisites

SNMP write permission is set.

A maximum of 32 ESS profiles can be created on eSight.

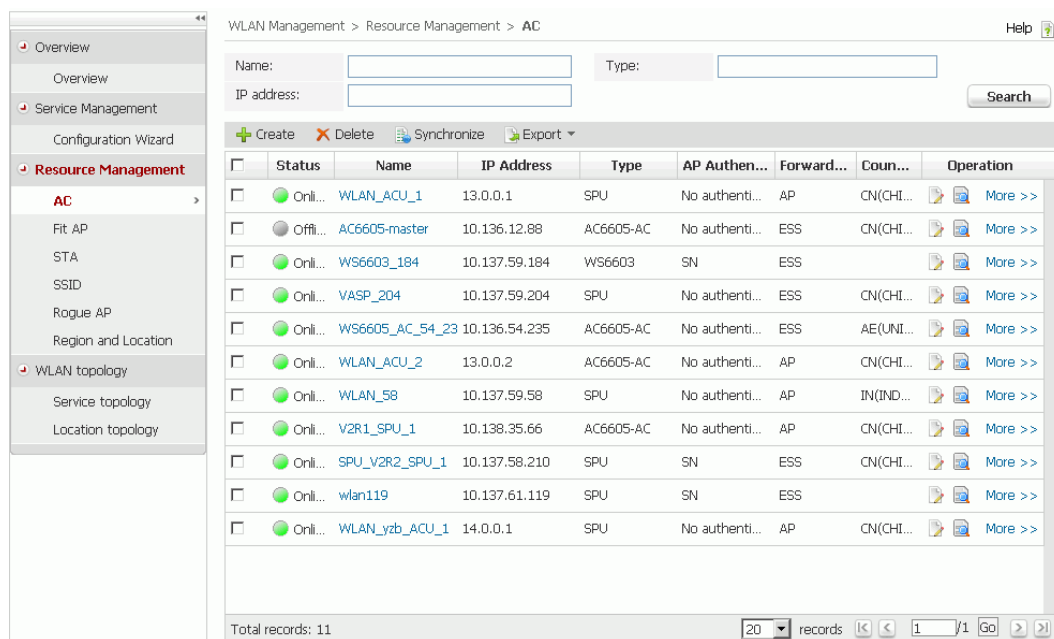
### Procedure

**Step 1** Choose **Network Application > WLAN Management**.

**Figure 10-44** WLAN management

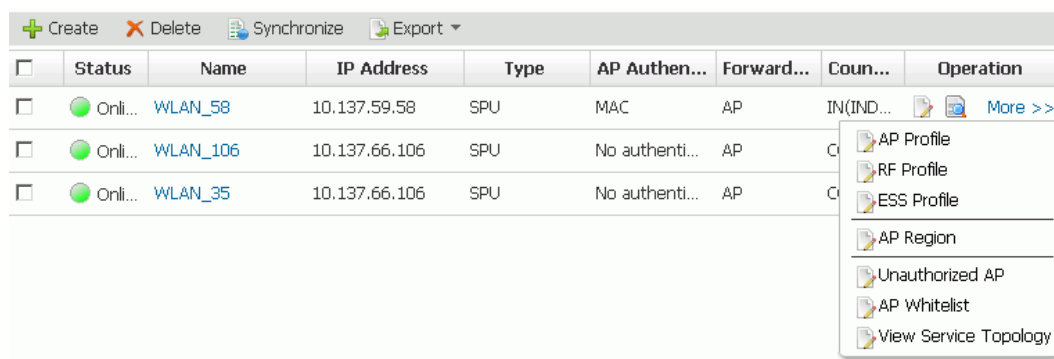
**Step 2** In the navigation tree on the left, choose **Resource Management > AC**.

**Figure 10-45** AC list



**Step 3** In the pane on the right, choose **More > ESS Profile**.

**Figure 10-46** AC operation



**Step 4** Click **Create**. In the window that is displayed, set ESS profile parameters.



**Figure 10-47** Creating ESS profile

WLAN Management > Resource Management > AC > ESS Profile > Create Help 

---

**Basic Info**

|                                           |             |                     |                                                                                               |
|-------------------------------------------|-------------|---------------------|-----------------------------------------------------------------------------------------------|
| * Name:                                   | ESSProfile1 | Type:               | Service                                                                                       |
| * SSID:                                   | Huawei      | * ESS interface:    | Wlan-Ess0  |
| * VLAN ID:                                | 10          | Hide SSID:          | No                                                                                            |
| Layer-2 user isolation:                   | No          | * Max. users limit: | 32                                                                                            |
| * Association timeout interval (minutes): | 5           | IGMP mode:          | Disabled                                                                                      |

**Authentication Parameters**

Encryption mode: ☒ WPA1-PSK ☐ WPA2-PSK ☐ WEP shared key ☐ WPA1 802.1X ☐ WPA2 802.1X  
☐ WEP open system

PSK type: ASCII USK type: tkip

\* PSK: \*\*\*\*\* \* Confirm PSK: \*\*\*\*\*

- **Max users:** Maximum number of users that a radio channel can carry when an ESS profile is bound to the radio channel.
- **Association timeout interval(minutes):** Maximum time for an AP to connect to a client. If they are not connected when the time passes by, the AP and the client do not confirm the connection request.
- **Hide SSID:** If this parameter is set, a client must learn the SSID of an AP before discovering AP.

**Step 5** Click **OK**. The new ESS profile is displayed in the list.

**Figure 10-48** ESS profile list

WLAN Management > Resource Management > AC > ESS Profile Back Help 

---

Name:  Type: All

SSID:

 Create  Delete  Synchronize

| <input type="checkbox"/> | Name        | Type    | SSID             | ESS Interface | VLAN ID | Operat...                                                                             |
|--------------------------|-------------|---------|------------------|---------------|---------|---------------------------------------------------------------------------------------|
| <input type="checkbox"/> | zyin1       | Service | z00109358wlan58@ | Wlan-Ess1     | 888     |  |
| <input type="checkbox"/> | zyin        | Service | z00109358wlan58  | Wlan-Ess0     | 888     |  |
| <input type="checkbox"/> | ywf         | Service | dsfa             | Wlan-Ess0     | 20      |  |
| <input type="checkbox"/> | ykTest      | Service |                  |               | 1       |  |
| <input type="checkbox"/> | ESSProfile1 | Service | Huawei           | Wlan-Ess0     | 10      |  |

**NOTE**

Click  to modify ESS profile parameters.

----End

### 10.2.5.7 Configuring an AP Region

Creating an AP region and adding APs into the AP region enable you to manage the APs in a centralized way.

#### Prerequisites

SNMP write permission is set.

#### Context

- An AP can be normally connected to a WLAN after it is added to only one AP region.
- By default, one AP region exists. When an AP is connected to a WLAN, it is automatically added to the default region. A user can specify any existing AP region as the default region.

#### Procedure

**Step 1** Choose **Network Application** > **WLAN Management**.

**Figure 10-49** WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management** > **AC**.

**Figure 10-50** AC list

WLAN Management > Resource Management > AC

Name:  Type:

IP address:

| <input type="checkbox"/> | Status   | Name            | IP Address    | Type      | AP Authen...   | Forward... | Coun...   | Operation |
|--------------------------|----------|-----------------|---------------|-----------|----------------|------------|-----------|-----------|
| <input type="checkbox"/> | Onli...  | WLAN_ACU_1      | 13.0.0.1      | SPU       | No authenti... | AP         | CN(CHI... | More >>   |
| <input type="checkbox"/> | Offli... | AC6605-master   | 10.136.12.98  | AC6605-AC | No authenti... | ESS        | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | WS6603_184      | 10.137.59.184 | WS6603    | SN             | ESS        |           | More >>   |
| <input type="checkbox"/> | Onli...  | VASP_204        | 10.137.59.204 | SPU       | No authenti... | ESS        | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | WS6605_AC_54_23 | 10.136.54.235 | AC6605-AC | No authenti... | ESS        | AE(UNI... | More >>   |
| <input type="checkbox"/> | Onli...  | WLAN_ACU_2      | 13.0.0.2      | AC6605-AC | No authenti... | AP         | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | WLAN_58         | 10.137.59.58  | SPU       | No authenti... | AP         | IN(IND... | More >>   |
| <input type="checkbox"/> | Onli...  | V2R1_SPU_1      | 10.138.35.66  | AC6605-AC | No authenti... | AP         | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | SPU_V2R2_SPU_1  | 10.137.58.210 | SPU       | SN             | ESS        | CN(CHI... | More >>   |
| <input type="checkbox"/> | Onli...  | wlan119         | 10.137.61.119 | SPU       | SN             | ESS        |           | More >>   |
| <input type="checkbox"/> | Onli...  | WLAN_yzb_ACU_1  | 14.0.0.1      | SPU       | No authenti... | AP         | CN(CHI... | More >>   |

Total records: 11  records  / 1

**Step 3** In the pane on the right, choose **More > AP Region**.

**Figure 10-51** AC operation

| <input type="checkbox"/> | Status  | Name     | IP Address    | Type | AP Authen...   | Forward... | Coun...   | Operation |
|--------------------------|---------|----------|---------------|------|----------------|------------|-----------|-----------|
| <input type="checkbox"/> | Onli... | WLAN_58  | 10.137.59.58  | SPU  | MAC            | AP         | IN(IND... | More >>   |
| <input type="checkbox"/> | Onli... | WLAN_106 | 10.137.66.106 | SPU  | No authenti... | AP         | C         | More >>   |
| <input type="checkbox"/> | Onli... | WLAN_35  | 10.137.66.106 | SPU  | No authenti... | AP         | C         | More >>   |

- AP Profile
- RF Profile
- ESS Profile
- AP Region**
- Unauthorized AP
- AP Whitelist
- View Service Topology

**Step 4** Click **Create**.

**Step 5** In the window that is displayed, set AP region parameters.

**Figure 10-52** Create AP region

WLAN Management > Resource Management > AC > AP Region > **Create** Help

|               |                                        |
|---------------|----------------------------------------|
| *ID:          | <input type="text" value="101"/>       |
| *Name:        | <input type="text" value="APRegion1"/> |
| *Deploy Mode: | <input type="text" value="Normal"/>    |
| Alias:        | <input type="text"/>                   |

The value of **Deploy Mode** can be set to one of the following:

- **Spare:** In this mode, all the APs in a region are sparsely located without any signal interference between each other. If you create one region for each AP, however, the configuration workload is heavy. Therefore, a special region can be created as a solution to contain all these APs. The attributes of these APs require no adjustment, and each AP can work with the greatest radio power.
- **Normal:** In this mode, the APs in a region are relatively sparsely located. To meet basic service requirements, each AP should work with at least 50% of the maximum radio power.
- **Densely:** In this mode, the APs in a region are densely located. To meet basic service requirements, each AP should work with at least 25% of the maximum radio power.

**Step 6** Click **OK**. The new AP region is displayed in the list.

**Figure 10-53** AP region list

WLAN Management > Resource Management > AC > **AP Region** Back Help

Name:  Alias:

| <input type="checkbox"/> | ID  | Name        | Alias | Default Re... | Deploy Mo... | Operation |
|--------------------------|-----|-------------|-------|---------------|--------------|-----------|
| <input type="checkbox"/> | 0   | ap-region-0 |       | Yes           | Normal       |           |
| <input type="checkbox"/> | 255 | test-test   |       | No            | Normal       |           |
| <input type="checkbox"/> | 101 | APRegion1   |       | No            | Normal       |           |

**NOTE**

Click to modify AP region parameters.

Click to set an AP region as a default AP region.

When the quality of radio signals deteriorates in an AP region, click to enable radio calibration in the AP region.

----End

## 10.2.5.8 Binding Profiles to an AP

Bind the related AP profile, radio profile, and ESS profile to an AP to complete AP service provision.

### Prerequisites

SNMP write permission is set.

### Procedure

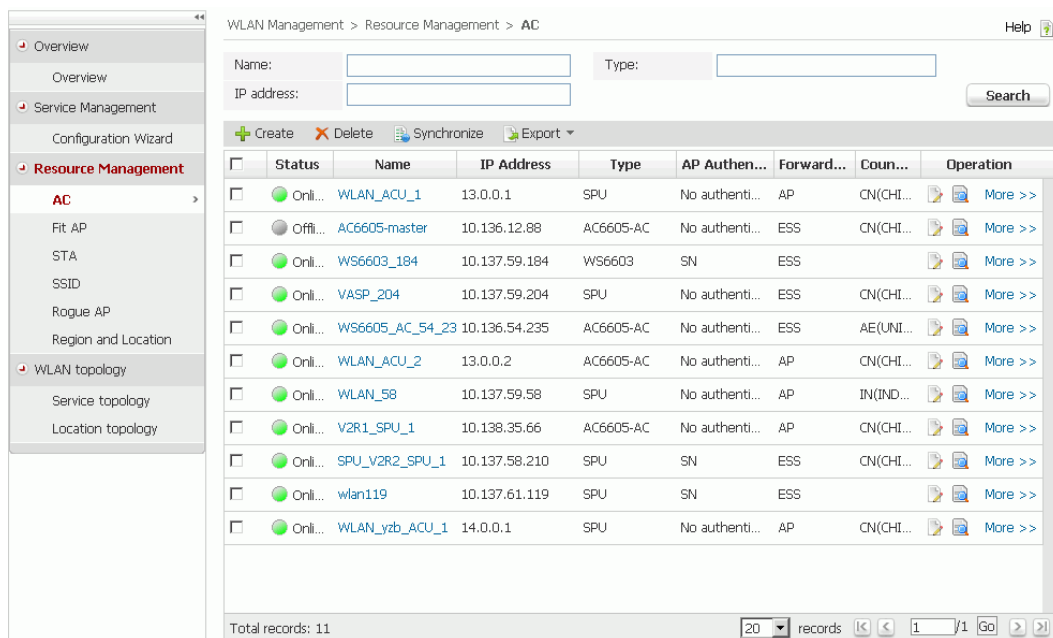
**Step 1** Choose **Network Application > WLAN Management**.

**Figure 10-54** WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management > AC**.

**Figure 10-55** AC list



**Step 3** In the pane on the right, click  in **Operation**.

- Step 4** Select an AP and click **Bind Profile** to bind a profile to the AP. APs whose bound profiles take effect may cause online users to go offline. When the message indicating that the profiles take effect is displayed, click **Yes**.

**Figure 10-56** AP list

WLAN Management > Resource Management > AC > AP [Back](#) [Help](#)

Name:

Type:

Location:

Status:

IP address:

Create Delete Bind Profile Synchronize Restart Restore Factory Settings

| <input type="checkbox"/> | Status | Name  | Alias | Type    | SN    | MAC         | IP Address   | AP R... | Location | Operati... |
|--------------------------|--------|-------|-------|---------|-------|-------------|--------------|---------|----------|------------|
| <input type="checkbox"/> | Onl... | zyin5 |       | WA63... | zyin5 | D8-01-01... | 193.168.0.12 | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin4 |       | WA63... | zyin4 | D8-01-01... | 193.168.0.11 | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin3 |       | WA63... | zyin3 | D8-01-01... | 193.168.0.4  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin2 |       | WA63... | zyin2 | D8-01-01... | 193.168.0.3  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin1 |       | WA63... | zyin1 | D8-01-01... | 193.168.0.2  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin0 |       | WA63... | zyin0 | D8-01-01... | 193.168.0.1  | zyin    |          |            |

Total records: 6  records  / 1

- Step 5** On the **Bind Profile** page, set the profiles bound to the AP as required.

**Figure 10-57 Binding profile**

WLAN Management > Resource Management > AC > AP > Bind Profile Help

AP profile:  ...

RF profile: + Bind - Unbind

| <input type="checkbox"/> | Radio ID | Radio P... | Workin... | Bandwi... | Channel... | Operati... | Transmi... | Availabl... |
|--------------------------|----------|------------|-----------|-----------|------------|------------|------------|-------------|
| <input type="checkbox"/> | 1        | zyin       | Open      | 20MHz     | 1          |            | 1          | All         |

ESS profile: + Bind - Unbind

| <input type="checkbox"/> | Radio ID | ESS Profile Name | SSID | ESS Type |
|--------------------------|----------|------------------|------|----------|
| <input type="checkbox"/> | 1        | zyin             | zyin | Service  |

OK Cancel

**NOTE**

Before binding **RF profile** and **ESS profile**, configure **Radio ID**.

**Figure 10-58 Configuring radio**

Configure Radio ×

\*Radio ID:

\*RF profile:  ...

Working status:  ▼

Bandwidth:  ▼

Channel value:

Transmit power level:

Available antennas:  ▼

OK Cancel

**TIP**

Some APs may support multiple radios. You can bind the radio profile and ESS profile to APs at multiple radios.

----End

## 10.2.6 Management and Maintenance

This topic describes tasks involved in WLAN maintenance and management.

## 10.2.6.1 Viewing AC Information

After configuring the WLAN service, you can view basic information about all ACs.

### Procedure

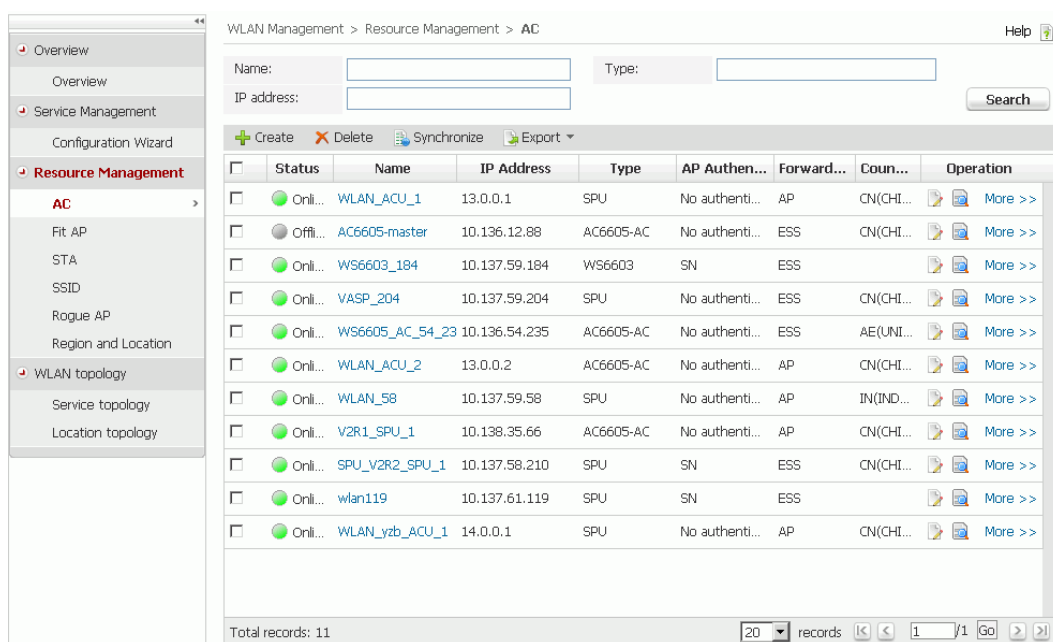
**Step 1** Choose **Network Application** > **WLAN Management**.

Figure 10-59 WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management** > **AC**.

Figure 10-60 AC list

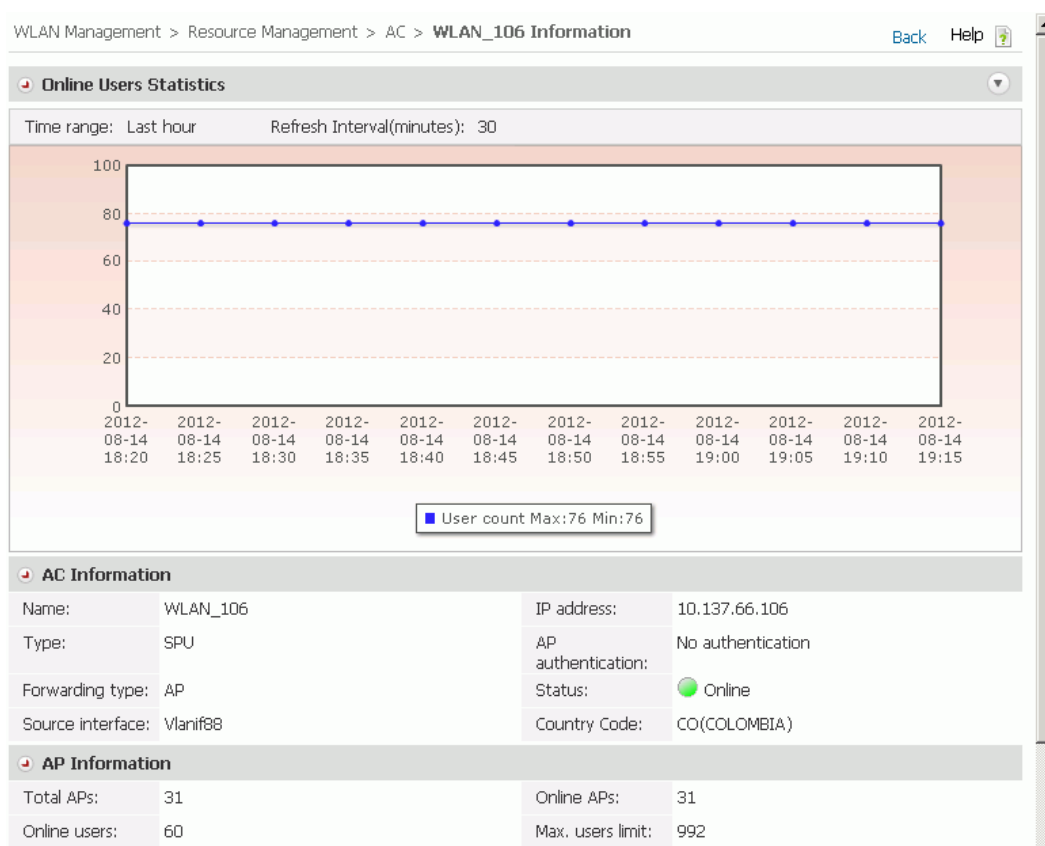


#### NOTE

To save AC information in eSight to local, click **Export**. You can choose to export all or some AC information.

**Step 3** Click the name of an AC on the page that is displayed to view information about the AC.



**Figure 10-61** AC information

----End

## Follow-up Procedure

The system provides statistics within one hour by default and refreshes statistics every 30 minutes. Click  in the upper right corner of **Online Users Statistics**, and you can set the time range and refresh interval.

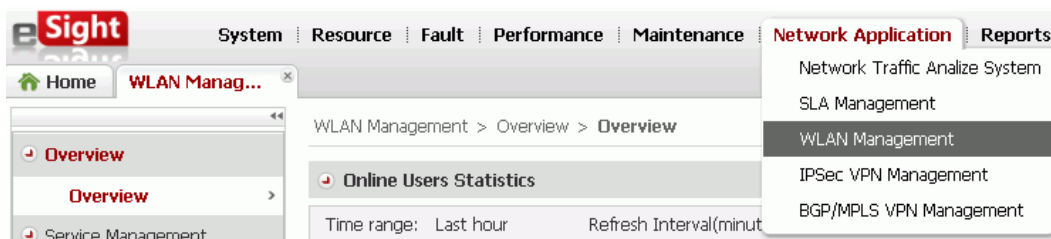
### 10.2.6.2 Viewing AP Information

After an AP is connected to an AC, you can query all AP information managed by eSight.

## Procedure

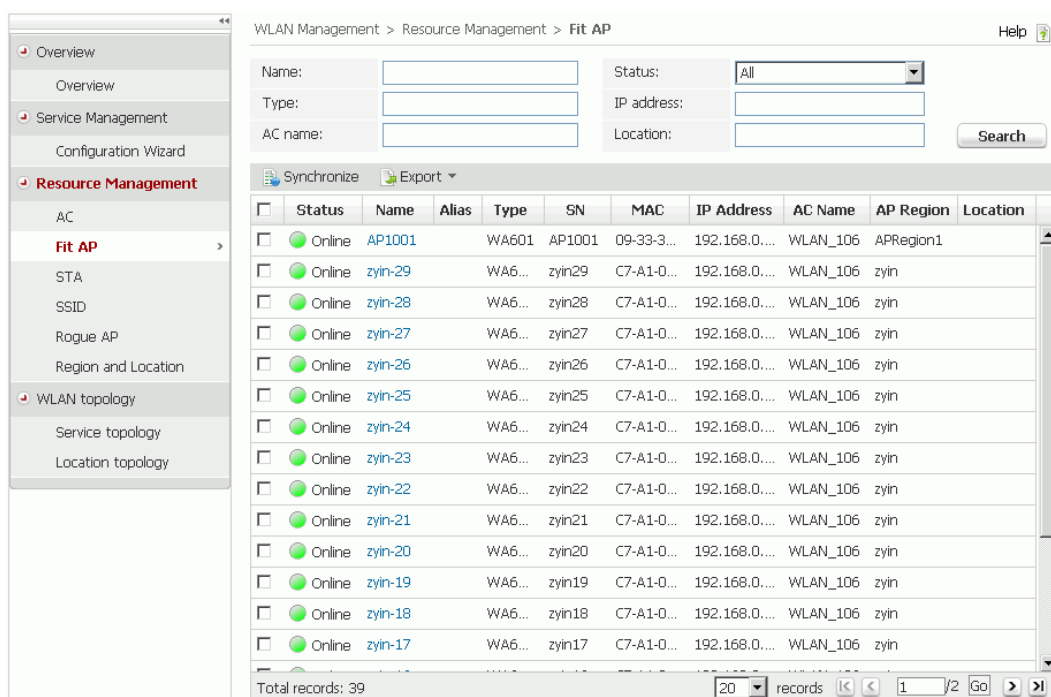
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-62 WLAN management



**Step 2** In the navigation tree, choose **Resource Management > Fit AP**.

Figure 10-63 Fit AP list



**Step 3** In the pane on the right, click **Synchronize** to synchronize the AP information to eSight.

**NOTE**

To save AP information in eSight to local, click **Export**. You can choose to export all or some AP information.

**Step 4** Click the name of an AP on the page that is displayed to view information about the AP.

**Figure 10-64** AP information

WLAN Management > Resource Management > Fit AP > **AP1001 Information** [Back](#) [Help](#) 

| AP Information |              |                       |                   |  |  |  |  |  |
|----------------|--------------|-----------------------|-------------------|--|--|--|--|--|
| Name:          | AP1001       | Alias:                |                   |  |  |  |  |  |
| SN:            | AP1001       | MAC:                  | 09-33-33-34-01-31 |  |  |  |  |  |
| Location:      |              | Type:                 | WA601             |  |  |  |  |  |
| Antenna:       | Auto         | Data forwarding mode: |                   |  |  |  |  |  |
| AP region:     | APRegion1    | IP address:           | 192.168.0.32      |  |  |  |  |  |
| AP profile:    | ap-profile-0 | AP software version:  | C00000030         |  |  |  |  |  |

| Bound RF Profile |             |            |           |             |             |             |             |              |
|------------------|-------------|------------|-----------|-------------|-------------|-------------|-------------|--------------|
| Radio ID         | Radio Pr... | Working... | Bandwidth | Channel ... | Operatin... | Transmit... | Operatin... | Available... |
| 1                | RFTempla... | Open       | 20MHz     | 1           | 6           | 1           | 12.0        | All          |

| Bound ESS Profile |                  |        |          |
|-------------------|------------------|--------|----------|
| Radio ID          | ESS Profile Name | SSID   | ESS type |
| 1                 | ESSTemplate1     | Huawei | Service  |

| Top 5 Alarms   |            |              |                 |              |                 |
|----------------|------------|--------------|-----------------|--------------|-----------------|
| Alarm Severity | Alarm Name | Alarm Source | Acknowledged... | Clear Status | Occurrence Time |
| No record.     |            |              |                 |              |                 |

| KPI | <a href="#">Configure</a> |
|-----|---------------------------|
|-----|---------------------------|

**Table 10-6** Important parameters

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data forwarding mode | <ul style="list-style-type: none"><li>Direct forwarding: The AP sends the original packets directly.</li><li>Tunnel forwarding: The AP encapsulates packets to the CAPWAP tunnel and forwards the packets to an upper-layer network to ensure packet forwarding security.</li></ul>                                                                                                                                            |
| AP region            | Region is a logical concept. You can place a group of APs to a region. Regions are planned based on the actual deployment. You can specify an AP region as the default region. When an AP goes online automatically (authentication not required), the AP joins the default region.                                                                                                                                            |
| Antenna              | If AP radio signals are transmitted through the antenna and AP signals are not good, use another mode to transmit signals.                                                                                                                                                                                                                                                                                                     |
| Channel Bandwidth    | To avoid interference of neighbor APs, you must set neighbor APs' radio channels to different frequencies. <ul style="list-style-type: none"><li>When the channel frequency is 20 MHz, the transmission rate is low but you can select many channels, effectively reducing the interference.</li><li>When the channel frequency is approximately 40 MHz, the transmission rate is high but you can select only a few</li></ul> |

| Parameter               | Description                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | channels. Bandwidths <b>40-MHz</b> and <b>40+MHz</b> have the same transmission rate but different available channels.                                                                                                                                                                                                        |
| Channel Value           | Value of managed channel.                                                                                                                                                                                                                                                                                                     |
| Operating Channel Value | Value of current operating channel.<br><b>NOTE</b><br>In a radio profile bound to an AP, if <b>Channel Mode</b> is set to <b>Manual</b> , <b>Operating Channel Value</b> is the same value as that of <b>Channel Value</b> . If <b>Channel Value</b> is set to <b>Automatic</b> , the parameter value is allocated by the AC. |
| Operating power         | Current operating power.<br><b>NOTE</b><br>The operating power determines the signal coverage scope displayed in the location topology. When the value of this parameter is 32767, the signal coverage scope is not displayed in the location topology.                                                                       |
| Transmit Power Level    | Value range: 0-15<br>Value <b>0</b> indicates full power. The power depends on the AP type. A greater power level indicates a lower power.                                                                                                                                                                                    |
| Available Antennas      | The number of available antennas must be less than or equal to the number of actual antennas.<br>To save power consumption, you can shut down excess antennas.                                                                                                                                                                |

----End

### 10.2.6.3 Browsing STAs

A user browses information on all wireless terminal on the live network.

#### Context

STA is short for station, referring to the terminal of a desktop with a wireless Network Interface Card (NIC) or a notebook computer.

#### Procedure

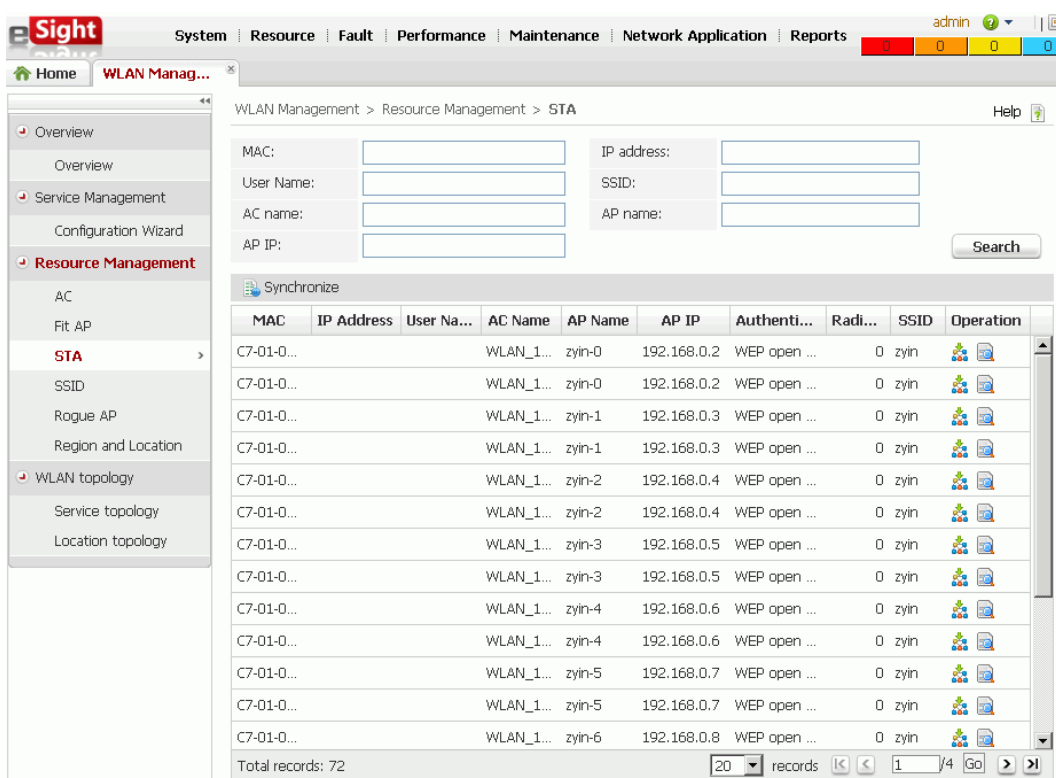
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-65 WLAN management

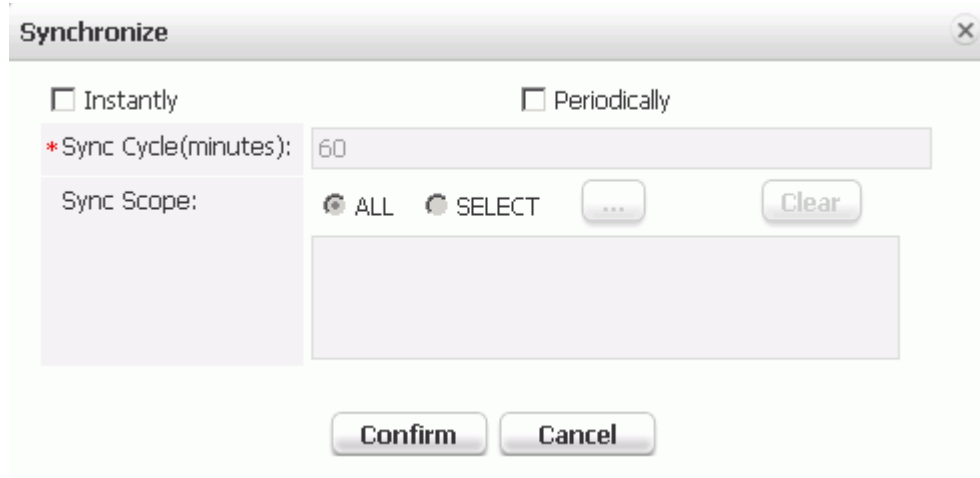


**Step 2** In the navigation tree on the left, choose **Resource Management > STA**.

Figure 10-66 STA list



**Step 3** Click **Synchronize** to browse information on all radio users on the live network.

**Figure 10-67** Synchronizing STA

1. In the **Synchronize** window, select **Instantly** or **Periodically**. You can also select both of them.
2. Set **Sync Cycle** if **Periodically** is selected.
3. **Optional:** Set **Sync Scope**.
4. Click **Confirm**.

----End

## Follow-up Procedure

**Table 10-7** Viewing STAs

| Application Scenario                                            | Procedure                                                                                                                                                                               |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Viewing AP which this STA connected to in the location topology | 1. Click  in <b>Operation</b> .<br>The AP which this STA connected to is displayed.                  |
| Viewing STA login information                                   | 1. Click  in <b>Operation</b> .<br>The STA login information including the online time is displayed. |

### 10.2.6.4 Browsing SSIDs Throughout the Network

SSIDs are used to discriminate subnets requiring identification authentication on a WLAN. Each subnet requires independent identification authentication. Only users succeeding in identification authentication can access the corresponding subnet. In this way, unauthorized users cannot access the WLAN.

#### Procedure

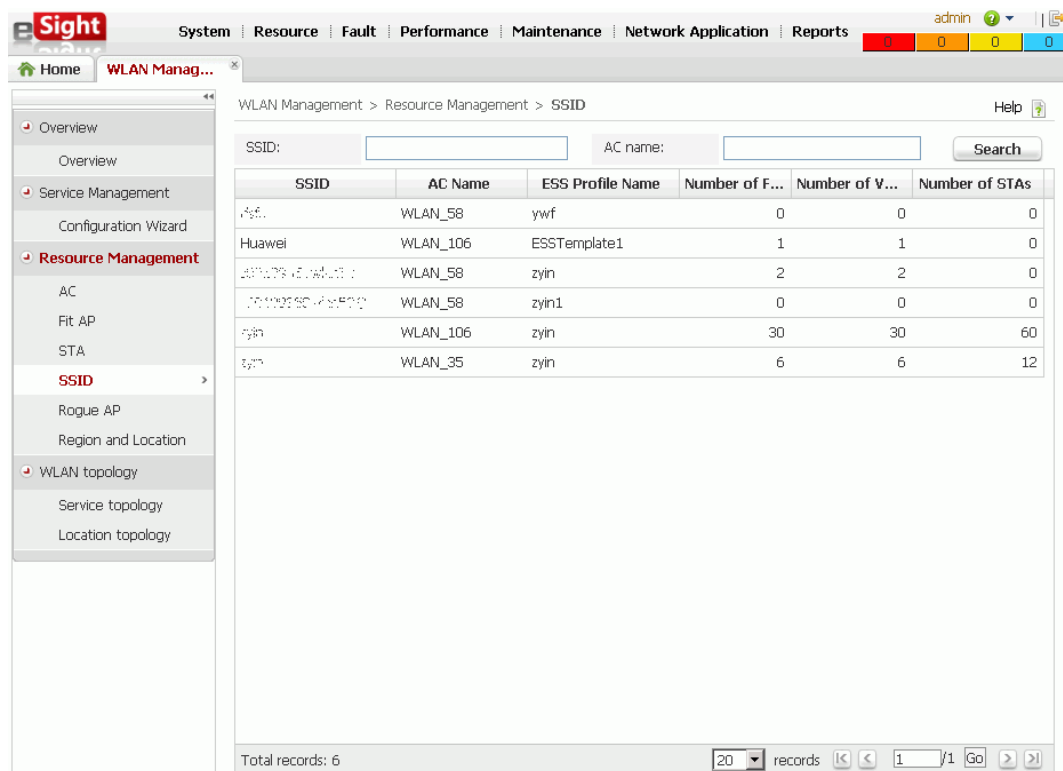
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-68 WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management > SSID**.

Figure 10-69 SSID list



----End

### 10.2.6.5 Browsing Rogue APs

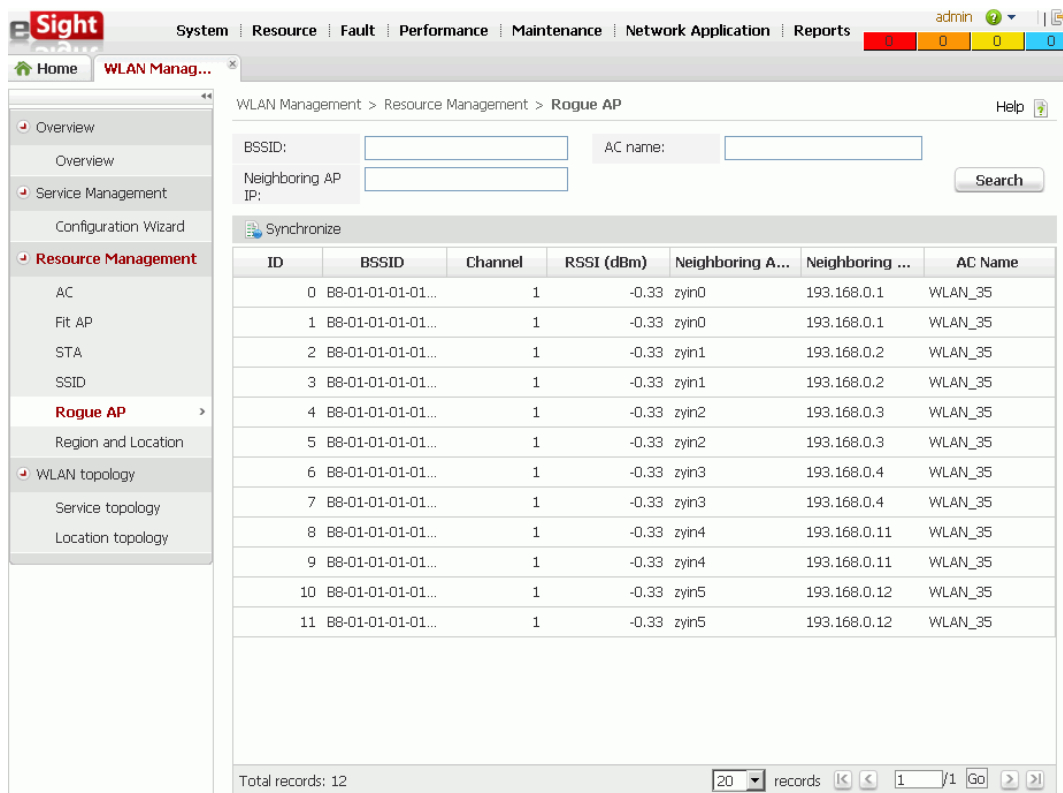
A rogue AP is an invalid AP that is connected to the WLAN without authentication or an AP that is not configured with correct security policies. An invalid AP enables unauthenticated network access. As a result, a radio terminal may access the WLAN through the invalid AP, wasting network resource.

#### Procedure

**Step 1** Choose **Network Application > WLAN Management**.

**Figure 10-70** WLAN management

**Step 2** In the navigation tree on the left, choose **Resource Management > Rogue AP**.

**Figure 10-71** Rogue AP list

**Step 3** Click **Synchronize** to browse all rogue APs on the live network.

**Table 10-8** Related Concepts

| Concept | Description                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BSSID   | The BSSID of AP. The SSID includes operator ID, AC ID, AP ID, RF ID, and WLAN ID.                                                                                                |
| Channel | APs communicate through a radio channel. When multiple APs exist in an area, channels set for the adjacent APs must be five channels away from each other to avoid interference. |



| Concept | Description                                           |
|---------|-------------------------------------------------------|
| RSSI    | RSSI is short for Received Signal Strength Indicator. |

----End

### 10.2.6.6 Browsing STA Access History

On the eSight, you can view the STA access history, including the login time and login result.

#### Prerequisites

- eSight has installed on the Linux server.
- The log function has been configured on the AC and the Linux server. For the detailed configuration, see the [10.2.4 Configuring the Log Function](#).

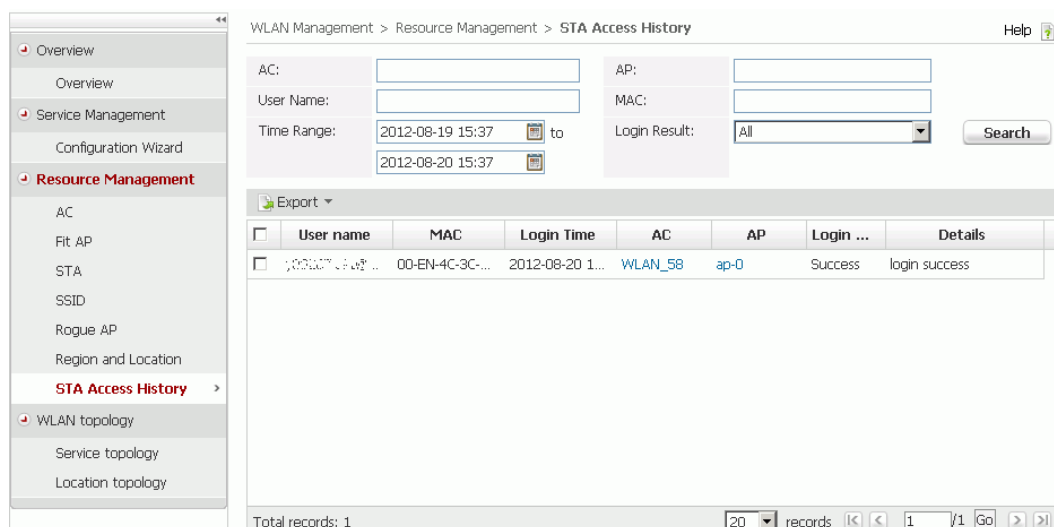
#### Procedure

**Step 1** Choose **Network Application** > **WLAN Management**.

**Figure 10-72** WLAN management



**Step 2** In the navigation tree, choose **Resource Management** > **STA Access History**.

**Figure 10-73** STA access history list

**Step 3** Specify the search criteria and click **Search**.

----End

### 10.2.6.7 Managing Regions and Locations

You can simulate the existing network to construct a virtual network architecture and add APs to the architecture, which makes it easy for you to view APs and facilitates operation and maintenance.

#### Context

- Relationship between regions and locations: A region consists of subregions and locations. A location is at the lowest layer of regions. Network devices can only be added to the location.
- The system supports a maximum of nine layers of regions and locations.
- You can view regions, locations, and AP information in location topology views.

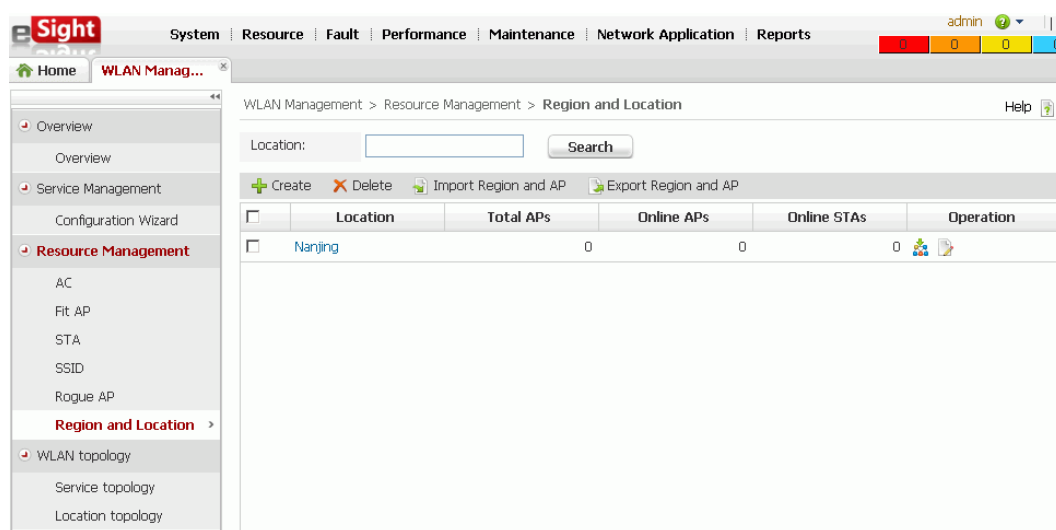
#### Procedure

**Step 1** Choose **Network Application > WLAN Management**.

**Figure 10-74** WLAN management

**Step 2** In the navigation tree, choose **Resource Management > Region and Location**.

**Figure 10-75** Region and location list



**Step 3** Perform either of the following operations as required.

- Create a subregion or location.

1. Click **Create**.



**NOTE**

To create a subregion or location in a region, first click the region name.

2. Set **Name** and select **Attribute**.

**Figure 10-76** Creating region and location

WLAN Management > Resource Management > Region and Location > **Create**

Region: Geographical location, you can add subregions and locations in a region.  
Location: Smallest region, you can add only network devices at a location.

\* Name:

\* Attribute: ☒ Region ☐ Location

3. Click **OK**.

- Import regions and devices in a batch.

1. Click **Import Region and AP**.

**Figure 10-77** Importing region and AP

WLAN Management > Resource Management > **Region and Location** Help

Location:  Search

+ Create - Delete Import Region and AP Export Region and AP

Template to download: [Region and Location Plan Profile](#)

\* Upload Resource File:  Upload Delete

| <input type="checkbox"/> | Location | Total APs | Online APs | Online STAs | Operation |
|--------------------------|----------|-----------|------------|-------------|-----------|
| <input type="checkbox"/> | Nanjing  | 0         | 0          | 0           |           |

- Click **Region and Location Plan Profile** to download the plan sheet template.
- Fill in the data sheet as defined by the template.
- Click , select a plan sheet, and click to import the plan sheet.

**NOTE**

The system checks whether the plan sheet is filled as defined by the template. If the plan sheet fails the check, perform operations as prompted.

The APs are imported to the locations specified in the plan sheet. If the AP is not in eSight, it is created offline.

**Figure 10-78** Imported result

+ Create - Delete Import Region and AP Export Region and AP

Template to download: [Region and Location Plan Profile](#)

\* Upload Resource File:  Upload Delete

Regions and locations imported completely. Imported:8. Succeeded:8. Failed:0. [Details](#)

| <input type="checkbox"/> | Location | Total APs | Online APs | Online STAs | Operation |
|--------------------------|----------|-----------|------------|-------------|-----------|
| <input type="checkbox"/> | Nanjing  | 0         | 0          | 0           |           |
| <input type="checkbox"/> | Shenzhen | 8         | 8          | 16          |           |
| <input type="checkbox"/> | A3       | 4         | 4          | 8           |           |
| <input type="checkbox"/> | A4       | 4         | 4          | 8           |           |
| <input type="checkbox"/> | 1F       | 2         | 2          | 4           |           |
| <input type="checkbox"/> | Area A   | 1         | 1          | 2           |           |
| <input type="checkbox"/> | Area B   | 1         | 1          | 2           |           |
| <input type="checkbox"/> | 2F       | 2         | 2          | 4           |           |
| <input type="checkbox"/> | Area A   | 1         | 1          | 2           |           |
| <input type="checkbox"/> | Area B   | 1         | 1          | 2           |           |

----End

## Follow-up Procedure

**Table 10-9** Managing regions and locations

| Application Scenario                                                      | Procedure                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adding APs to a location                                                  | To add APs to a location, use either of the following methods: <ul style="list-style-type: none"><li>• Import APs when regions are imported in a batch.</li><li>• Manually add APs in location topology views. See <a href="#">10.2.6.9 Viewing the Location Topology</a>.</li></ul> |
| Modifying the region or location name                                     | <ol style="list-style-type: none"><li>1. Click .</li><li>2. Enter a new name.</li><li>3. Click <b>OK</b>.</li></ol>                                                                                 |
| Deleting a region or location                                             | <ol style="list-style-type: none"><li>1. Select the region and location.</li><li>2. Click <b>Delete</b>.</li><li>3. Click <b>Yes</b>.</li></ol>                                                                                                                                      |
| Exporting regions and APs                                                 | <ol style="list-style-type: none"><li>1. Select the export range.</li><li>2. Click <b>Export Region and AP</b>.</li></ol>                                                                                                                                                            |
| Viewing and adjusting regions and locations in the location topology view | See <a href="#">10.2.6.9 Viewing the Location Topology</a> .                                                                                                                                                                                                                         |

### 10.2.6.8 Viewing the Service Topology

This topic describes how to view ACs, APs, rogue APs, stations (STAs), and the logical relationship between them in the service topology.

#### Context

ACs added in eSight are automatically displayed in the service topology.

#### Procedure

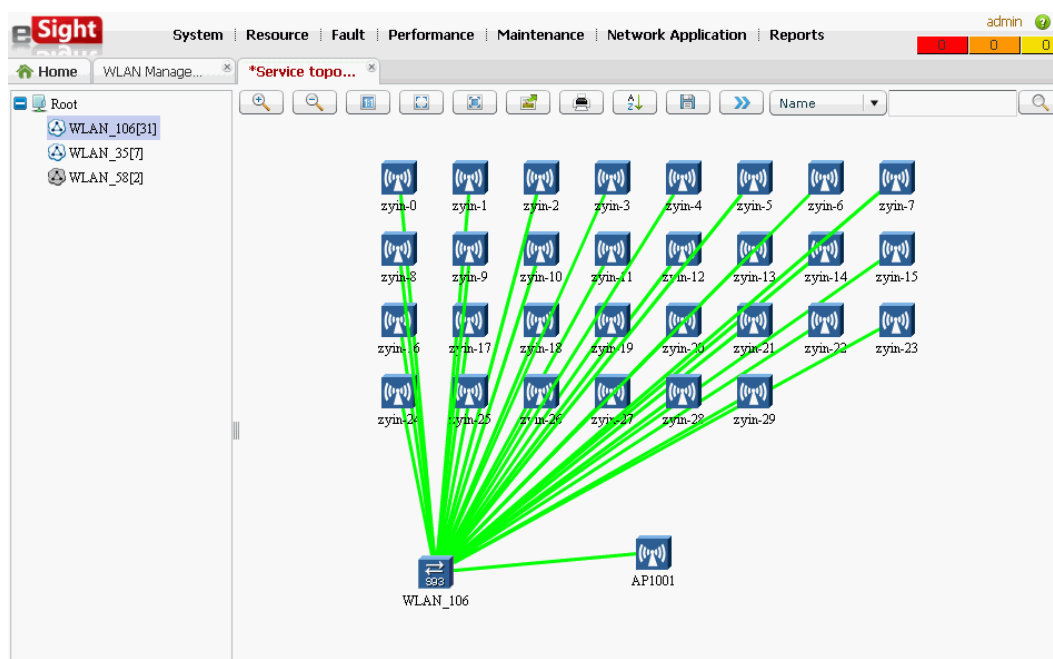
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-79 WLAN management



**Step 2** In the navigation tree, choose **WLAN topology** > **Service topology**.

Figure 10-80 WLAN service topology



**Step 3** View the WLAN service topology in either of the following ways:

- Select , and click  to expand the WLAN service topology. Then click  to collapse the WLAN service topology.
- Double-click  to access the WLAN service topology.

**Step 4** Right-click a device, and choose the required operation.

- **Synchronize:** Synchronize data on the selected AC to eSight.
- **View Physical Topology:** View the physical topology view of ACs.
- **View Alarms:** View the alarm list of an AC.
- **Details:** View detailed device information.
- **Ping:** Ping an AP and another network device to check the connectivity between them.

- **View Users:** View users connected to the AP.
- **Hide Users:** Hide users connected to the AP.

----End

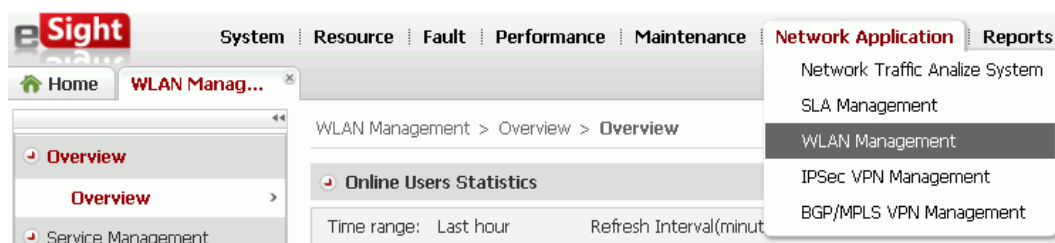
### 10.2.6.9 Viewing the Location Topology

You can create a location topology view and add APs to the location topology view based on the WLAN management requirements. In the location topology, you can view the current signal coverage scope and current device status, and simulate actual networks to facilitate daily maintenance.

#### Procedure

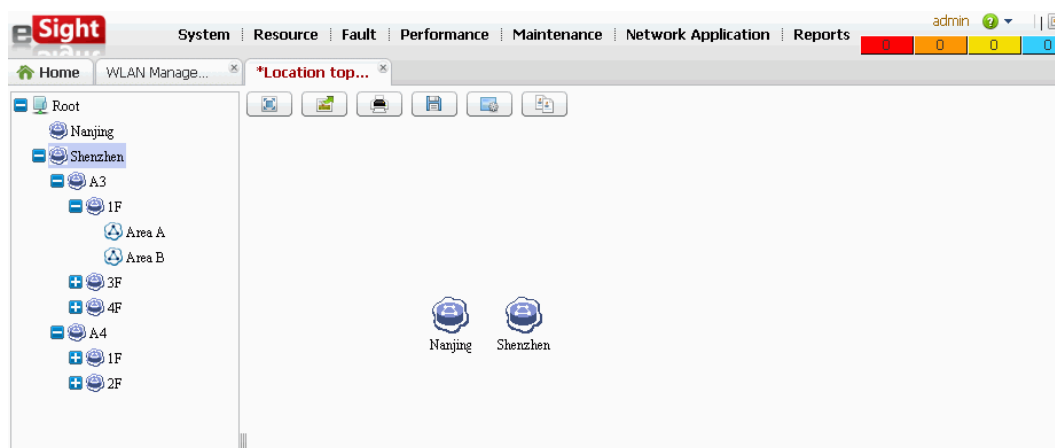
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-81 WLAN management



**Step 2** In the navigation tree, choose **WLAN topology > Location topology**.

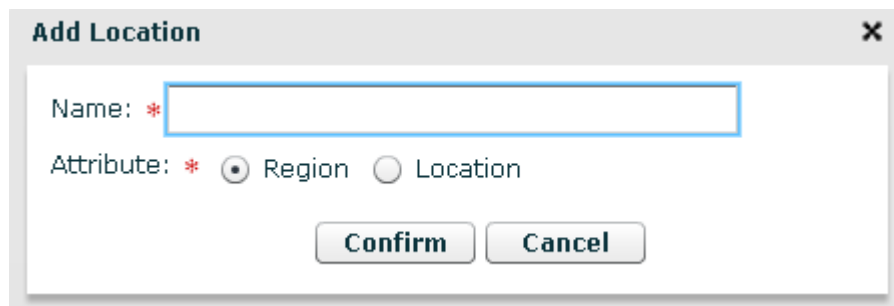
Figure 10-82 WLAN location topology



**Step 3** Add regions and locations in the location topology.

1. Right-click in the location topology, and choose **Add Location**.
2. In the dialog box that is displayed, set **Name** and **Attribute**.

**Figure 10-83** Adding location



3. Click **Confirm**.



**NOTE**

- A location topology view may support multiple layers of sub location topology views. A maximum of nine sub layers are supported.
- A location topology view may contain multiple devices.

**Step 4** Set the background of the lowest-layer location.

1. Double-click the location icon to access the lowest-layer location page.
2. Click  on the shortcut icon bar.
3. In the dialog box that is displayed, select a proper image of the site scenario based on the physical network environment.

**Figure 10-84** Set background



4. Click **Confirm**.



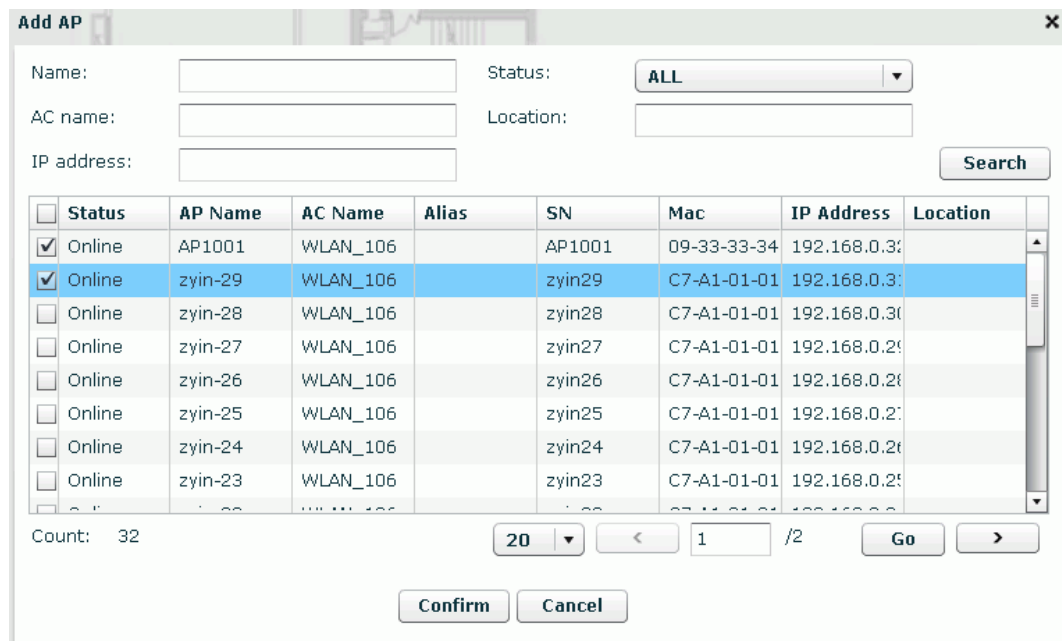
**NOTE**

An image can be in GIF, JPG, JPEG, or PNG format.

**Step 5** Add APs to the lowest-layer location topology.

1. Right-click in the location topology, and choose **Add AP**.



**Figure 10-85** Adding AP

The 'Add AP' dialog box contains the following fields and controls:

- Name:** Text input field.
- AC name:** Text input field.
- IP address:** Text input field.
- Status:** Dropdown menu with 'ALL' selected.
- Location:** Text input field.
- Search:** Button.
- Table:** A table with columns: Status, AP Name, AC Name, Alias, SN, Mac, IP Address, and Location. The table lists several APs, with 'zyin-29' selected.
- Count:** 32
- Page controls:** 20, <, 1, /2, Go, >
- Buttons:** Confirm, Cancel

| <input type="checkbox"/>            | Status | AP Name | AC Name  | Alias | SN     | Mac         | IP Address   | Location |
|-------------------------------------|--------|---------|----------|-------|--------|-------------|--------------|----------|
| <input checked="" type="checkbox"/> | Online | AP1001  | WLAN_106 |       | AP1001 | 09-33-33-34 | 192.168.0.34 |          |
| <input checked="" type="checkbox"/> | Online | zyin-29 | WLAN_106 |       | zyin29 | C7-A1-01-01 | 192.168.0.34 |          |
| <input type="checkbox"/>            | Online | zyin-28 | WLAN_106 |       | zyin28 | C7-A1-01-01 | 192.168.0.34 |          |
| <input type="checkbox"/>            | Online | zyin-27 | WLAN_106 |       | zyin27 | C7-A1-01-01 | 192.168.0.29 |          |
| <input type="checkbox"/>            | Online | zyin-26 | WLAN_106 |       | zyin26 | C7-A1-01-01 | 192.168.0.26 |          |
| <input type="checkbox"/>            | Online | zyin-25 | WLAN_106 |       | zyin25 | C7-A1-01-01 | 192.168.0.25 |          |
| <input type="checkbox"/>            | Online | zyin-24 | WLAN_106 |       | zyin24 | C7-A1-01-01 | 192.168.0.24 |          |
| <input type="checkbox"/>            | Online | zyin-23 | WLAN_106 |       | zyin23 | C7-A1-01-01 | 192.168.0.23 |          |

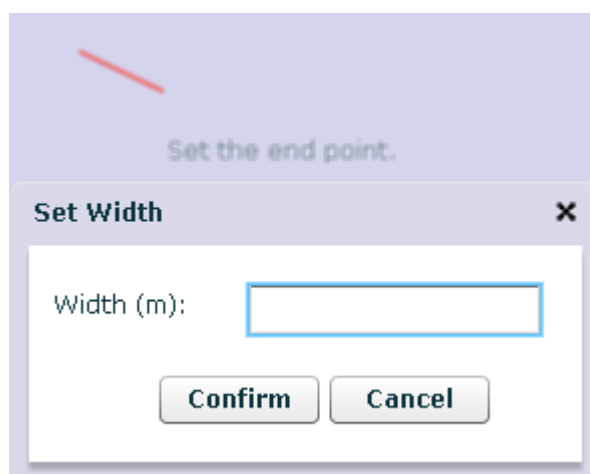
2. In the dialog box that is displayed, select the required APs.
3. Click **Confirm**.

**NOTE**

You can add APs only in the lowest-layer location topology.

**Step 6** Set the scale of the lowest-layer location.

1. Right-click in the location topology, and choose **Set scale**.
2. Set the start point, end point.
3. Set the actual distance between the two points.

**Figure 10-86** Setting scale

The 'Set Width' dialog box is shown over a network topology background. It contains the following elements:

- Set Width** title bar with a close button (X).
- Width (m):** Text input field.
- Buttons:** Confirm, Cancel

4. Click **Confirm**.

After the setting is complete, check the scale in the upper left corner of the topology background. It is recommended that the scale be larger than the minimum value in [Table 10-10](#).

The minimum value of the scale is provided based on the AP quantity and signal coverage, in meters. [Table 10-10](#) lists the minimum value of the scale.

**Table 10-10** Minimum value of the scale

| AP Quantity | BY Signal Strength | BY Signal Strength (Blocks) | BY Rate | BY Rate (Blocks) | BY Channel (Collision Domains) | BY Channel (Collision Domains and Blocks) |
|-------------|--------------------|-----------------------------|---------|------------------|--------------------------------|-------------------------------------------|
| 10          | 0.2                | 10                          | 0.2     | 10               | 40                             | 50                                        |
| 20          | 0.2                | 20                          | 0.2     | 20               | 80                             | 90                                        |
| 30          | 0.2                | 40                          | 0.2     | 40               | 100                            | 120                                       |
| 40          | 0.2                | 50                          | 0.2     | 50               | 150                            | 160                                       |
| 50          | 0.2                | 60                          | 0.2     | 60               | 200                            | 250                                       |

**NOTE**

If the configured scale does not take effect, access the location topology view again or clear the browser cache and access the location topology view again.

**Step 7** Right-click in the location topology, and choose **Display Signal Coverage > Required channel display mode**.

**Figure 10-87** Displaying signal coverage

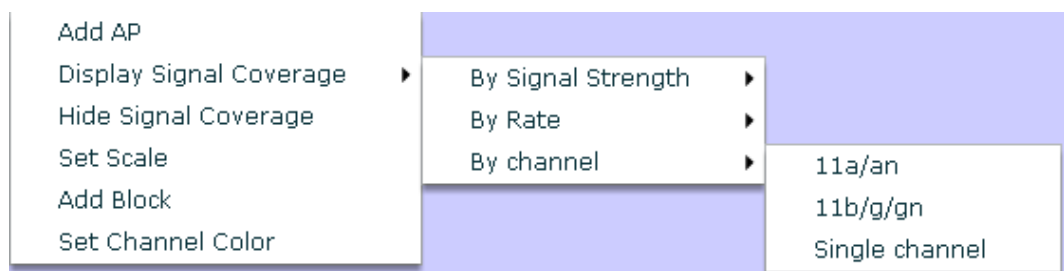


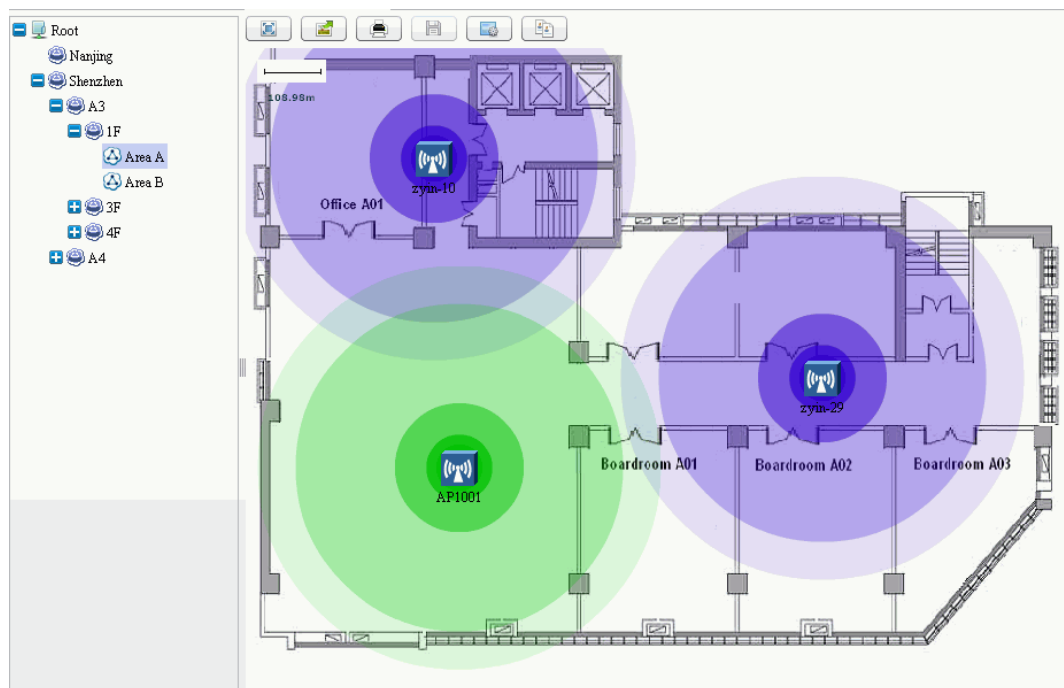
**Table 10-11** Menu description

| Operation    | Description                                                                                                                                      | Setting                                                                                                                                  |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Add Location | Add a location based on the physical location of a device on the live network to display the device layer relationship in the location topology. | Right-click in the location topology, and choose <b>Add Location</b> .<br><b>NOTE</b><br>A location can only be added to <b>Region</b> . |
| Set Channel  | Set colors for channels as                                                                                                                       | Right-click in the location                                                                                                              |

| Operation               | Description                                                                                                                                                                                                                                                                                                                                                                                                                               | Setting                                                                                                                                                                                                                                                                            |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Color                   | required.                                                                                                                                                                                                                                                                                                                                                                                                                                 | topology, and choose <b>Set Channel Color</b> .<br><br><b>NOTE</b><br>All channels are displayed when <b>Display only operating channels</b> is deselected.                                                                                                                        |
| Display Signal Coverage | The signal coverage scope can be displayed in any of the following modes: by signal strength, by rate, and by channel.<br><br><b>NOTE</b><br>The signal coverage scope displayed is determined by the operating power in the radio profile. If the signal coverage scope is not displayed properly, check the operating power in the radio profile.<br><br><b>TIP</b><br>To check channel collisions, display signal coverage by channel. | Right-click in the location topology, and choose <b>Display Signal Coverage</b> .                                                                                                                                                                                                  |
| Hide Signal Coverage    | Hide the signal coverage scope.                                                                                                                                                                                                                                                                                                                                                                                                           | Right-click in the location topology, and choose <b>Hide Signal Coverage</b> .                                                                                                                                                                                                     |
| Set scale               | Set the scale based on the actual network layout size to map the network layout to the location topology.                                                                                                                                                                                                                                                                                                                                 | In the location topology, right-click, and choose <b>Set scale</b> .<br><br><b>NOTE</b><br>When setting a scale in the location topology for the first time, initialize the scale to ensure that the scale is the same as that in the background.                                  |
| Add Block               | Add blocks for the following purposes: <ul style="list-style-type: none"><li>Ensuring that the location topology view is consistent with the real network layout.</li><li>Controlling signal attenuation.</li></ul>                                                                                                                                                                                                                       | Right-click in the location topology, and choose <b>Add Block</b> .<br><br><b>NOTE</b><br>Block depth to display in the location topology is calculated based on the scale and actual block depth. When block depth to display exceeds 50 pixel, it will be displayed as 50 pixel. |

**Step 8** Click  on the shortcut icon bar to save the location topology.

**Figure 10-88** Location topology



**Step 9 Optional:** Click  on the shortcut icon bar to export and save the location topology view to the local.

**Step 10 Optional:** Click  on the shortcut icon bar to print the location topology view.

----End

## 10.2.6.10 Diagnosing Faults

eSight allows you to test the connectivity between an AP and an AC and between two APs.

### Prerequisites

The AP or AC that you want to test the connectivity is online.

The Telnet parameters are set correctly for the AC.

### Context

Ping is used to test whether a host is reachable across an IP network by sending ping packets to the host. Use the ping function to check whether a fault occurs on a network or test the network quality.

Tracert is used to discover the routes that packets actually pass when traveling from the source host to the destination host. Use the tracert function to locate a network fault.

When a fault is detected on a network using the Ping function, use the tracert function to locate the fault.

## Procedure

**Step 1** Choose **Network Application** > **WLAN Management**.

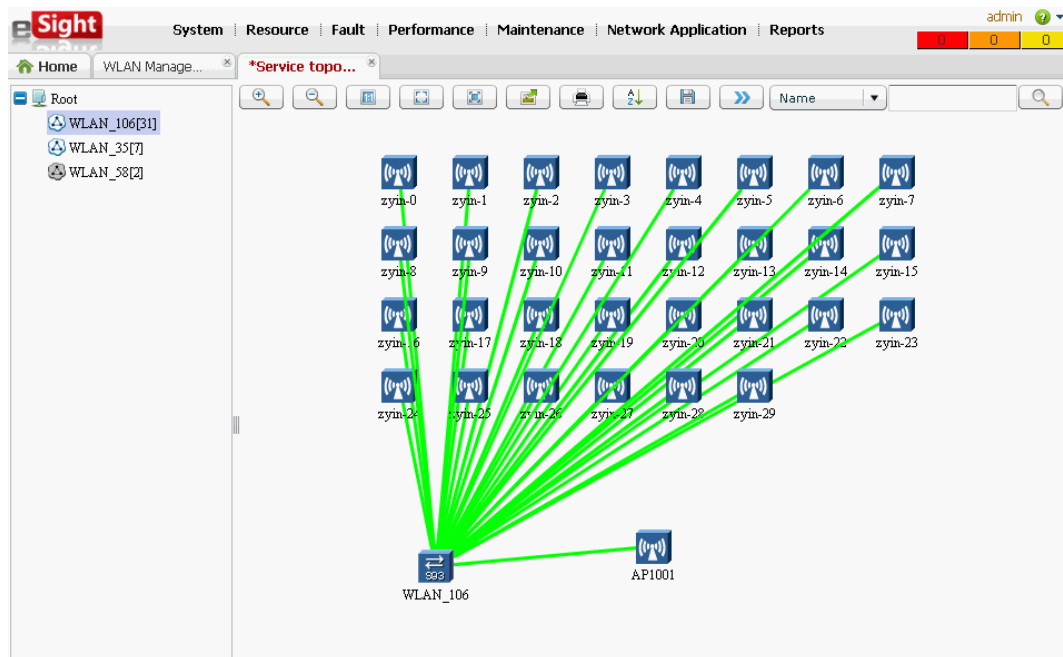
**Figure 10-89** WLAN management



**Step 2** In the navigation tree, choose **WLAN topology** > **Location topology**.

**Step 3** Double-click  to access the WLAN service topology.

**Figure 10-90** WLAN service topology



**Step 4** Select a proper diagnosis method based on the site scenario.

**Table 10-12** Diagnosis description

| Diagnosis Method                    | Application Scenario                                                                                           | Operation                                                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Perform the ping operation on an AP | <ul style="list-style-type: none"> <li>Check the connectivity by pinging a network device on an AP.</li> </ul> | <ol style="list-style-type: none"> <li>Right-click an AP, and select <b>Ping</b>.</li> <li>In the <b>AP Ping</b> window, enter the target device IP</li> </ol> |

| Diagnosis Method                                                            | Application Scenario                                                                                                                                                                                                                                                                                                                                                                                                                              | Operation                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                             | <ul style="list-style-type: none"><li>Check the connectivity between an AP and the FTP server during an upgrade.</li></ul>                                                                                                                                                                                                                                                                                                                        | address, and click <b>ping</b> . The ping result is displayed.                                                                                                                                                               |
| Perform the ping or tracert operation on the tunnel between an AP and an AC | <ul style="list-style-type: none"><li>If an AP is faulty, the ping operation cannot be performed on the AP. When this occurs, perform the ping operation on the matching AC to test the tunnel between the AC and AP.</li><li>Ping is used to check whether a fault occurs on the tunnel between an AP and AC or test the network quality.</li><li>Tracert is used to locate a network fault after it is detected by the ping function.</li></ul> | <ol style="list-style-type: none"><li>Right-click the tunnel between an AP and AC, and select <b>Ping</b> or <b>Tracert</b>.</li><li>In the window where the ping or tracert result is displayed, click <b>OK</b>.</li></ol> |

**Figure 10-91** Perform the ping or tracert operation on the tunnel between an AP and an AC

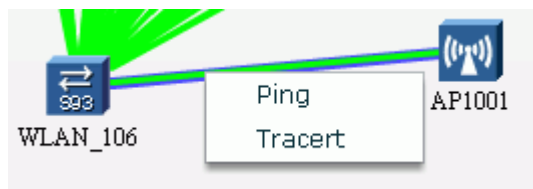
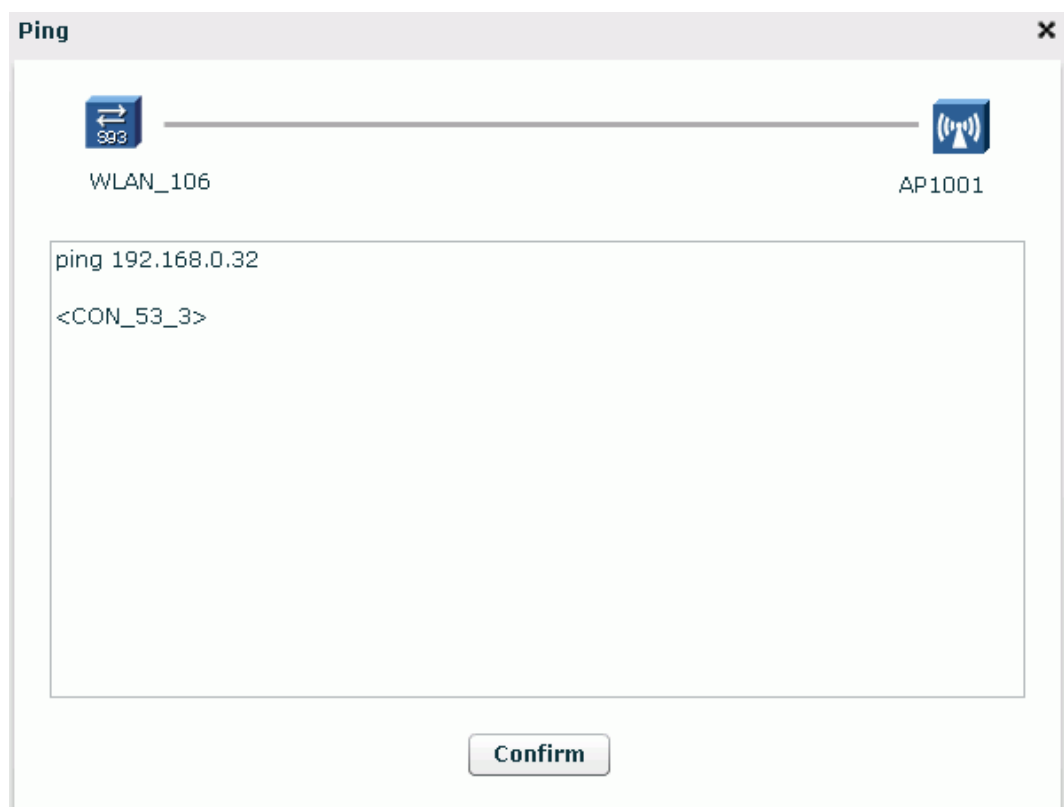


**Figure 10-92** Ping



----End

### 10.2.6.11 Rectifying AP Faults

This topic describes how to restore an AP to factory settings, replace an AP, or restart an AP based on the site scenario.

#### Context

- Restore an AP to factory settings: Perform this operation when AP configuration is faulty or when the network is calibrated.
- Restart an AP: Perform this operation when an AP is upgraded online or when the network is calibrated.
- Replace an AP: Perform this operation when a hardware fault occurs on an AP. This relieves you from reconfiguring data.

#### Procedure

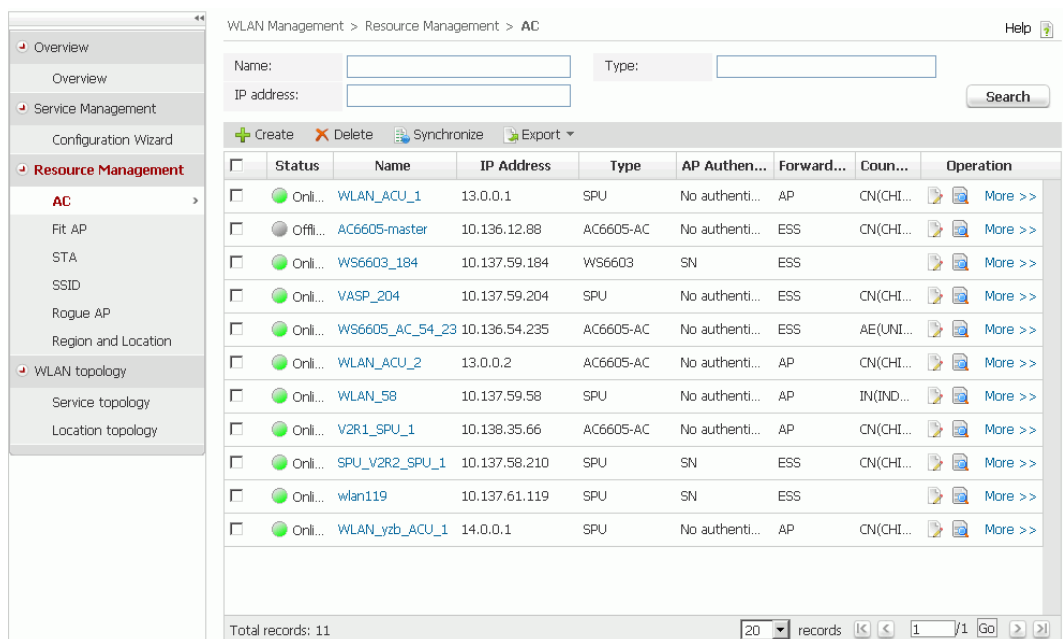
**Step 1** Choose **Network Application > WLAN Management**.

Figure 10-93 WLAN management



**Step 2** In the navigation tree on the left, choose **Resource Management > AC**.

Figure 10-94 AC list



**Step 3** In the pane on the right, click  in **Operation**.

**Step 4** Restart the AP, restore the AP to factory settings, or replace the AP based on the site scenario.



**Figure 10-95** AP list

WLAN Management > Resource Management > AC > AP Back Help ?

Name:  Status:   
Type:  IP address:   
Location:  Search

+ Create ✗ Delete Bind Profile Synchronize Restart Restore Factory Settings

| <input type="checkbox"/> | Status | Name  | Alias | Type    | SN    | MAC         | IP Address   | AP R... | Location | Operati... |
|--------------------------|--------|-------|-------|---------|-------|-------------|--------------|---------|----------|------------|
| <input type="checkbox"/> | Onl... | zyin5 |       | WA63... | zyin5 | D8-01-01... | 193.168.0.12 | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin4 |       | WA63... | zyin4 | D8-01-01... | 193.168.0.11 | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin3 |       | WA63... | zyin3 | D8-01-01... | 193.168.0.4  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin2 |       | WA63... | zyin2 | D8-01-01... | 193.168.0.3  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin1 |       | WA63... | zyin1 | D8-01-01... | 193.168.0.2  | zyin    |          |            |
| <input type="checkbox"/> | Onl... | zyin0 |       | WA63... | zyin0 | D8-01-01... | 193.168.0.1  | zyin    |          |            |

Total records: 6 20 records 1/1 Go

- Restart an AP or APs.
  1. Select one or more APs, and click **Restart**.

The **Confirm** dialog box is displayed, indicating that the operation will interrupt services.
  2. Click **Yes**.
- Restore an AP or APs to factory settings.
  1. Select one or more APs, and click **Restore Factory Settings**.

The **Confirm** dialog box is displayed, indicating that the operation will interrupt services.
  2. Click **Yes**.
- Replace an AP.
  1. Select an AP, and click .
  2. Set **SN** and **MAC** for the new AP.
  3. Click **OK**.

----End

## 10.2.7 Example: Typical WLAN Management Operations

This topic uses a configuration example to describe how to configure the WLAN service.

## Prerequisites

- ACs have been created in eSight.
- APs and ACs are connected properly.
- The SNMP read and write permissions have been configured.
- The AC source interface has been configured.
- The Dynamic Host Configuration Protocol (DHCP) server has been started on ACs.

## Scenario

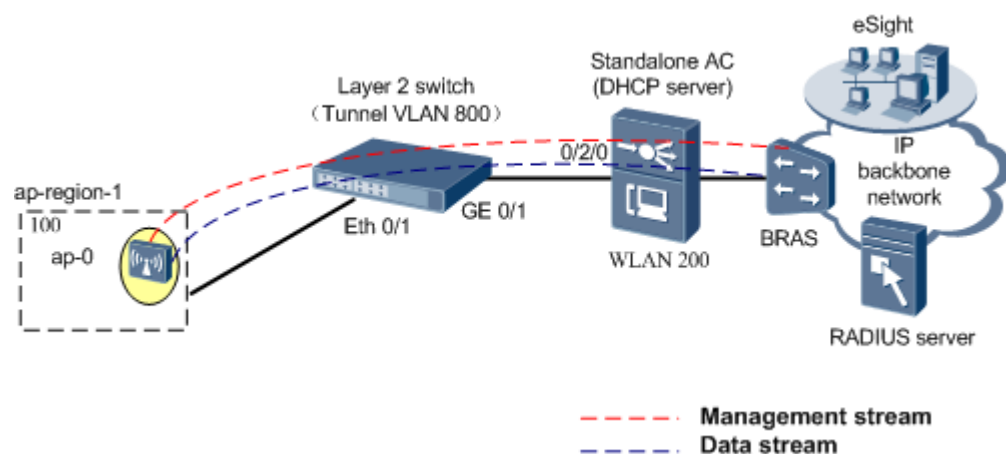
A network provider provides the WLAN service for the small region ap-region-1 through the AP ap-0.

## Network

The AC and AP are connected directly on a two-layer network. The AC functions as the DHCP server and assigns the IP address matching the Vlanif88 interface in the IP address pool to the AP.

The AP ap-0 forwards service data directly. Network services are allocated by VLAN ID (100) and forwarded by the AC.

**Figure 10-96** Configuration network



## Data Plan

- AC configuring data

| Name    | IP Address    | Source Interface | Type | AP Authentication | Forwarding Type |
|---------|---------------|------------------|------|-------------------|-----------------|
| WLAN200 | 10.137.59.200 | Vlanif88         | SPU  | No authentication | ESS             |

## • AP configuring data

| Name | SN         | MAC               | Type    | Antenna | Data forwarding mode |
|------|------------|-------------------|---------|---------|----------------------|
| ap-0 | AA48005562 | 00-25-9E-EB-FF-D4 | WA603DN | auto    | Direct forwarding    |

## • AP profile

| Name        | MTU  | Log Backup Server IP |
|-------------|------|----------------------|
| ap_template | 1500 | 10.67.38.52          |

## • Radio configuration

| Radio ID | RF Profile | Working Status | Bandwidth | Channel Value | Transmit Power Level | Available Antennas | ESS Profile  |
|----------|------------|----------------|-----------|---------------|----------------------|--------------------|--------------|
| 0        | template   | Open           | 20 MHz    | 1             | 1                    | All                | ess_template |

## • RF profile

| Name     | RF Type  | Rate Mode | Rate (Mbit/s) | Channel Mode | Power Mode |
|----------|----------|-----------|---------------|--------------|------------|
| template | 802.11bg | Automatic | 54            | Automatic    | Automatic  |

## • ESS profile

| Name         | Type    | SSID | ESS interface | VLAN ID | Hide SSID |
|--------------|---------|------|---------------|---------|-----------|
| ess_template | Service | 100  | Wlan-Ess630   | 100     | No        |

| Layer-2 user isolation | Max. users | Association timeout interval | IGMP mode | User data forwarding mode | Encryption mode |
|------------------------|------------|------------------------------|-----------|---------------------------|-----------------|
| No                     | 32         | 5                            | Disabled  | Direct forwarding         | WEP open system |

**Table 10-13** Configuration Procedure

| NO. | Step                     | Description                                                                                                                                            |
|-----|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Select an AC             | Select a proper AC based on the data plan.<br><b>NOTE</b><br>When ACs are created in eSight, they will be automatically discovered to WLAN management. |
| 2   | Configure AC information | Configure the AC authentication mode and forwarding mode.                                                                                              |
| 3   | Select APs               | If APs exist, select proper APs. If no AP exists, create APs offline or import APs in batches. APs are created offline in this topic.                  |
| 4   | Configure profiles       | Configure the AP profile, radio profile, and ESS profile, and bind these profiles with APs.                                                            |
| 5   | Deploy profiles on APs   | Deploy configured services on APs.                                                                                                                     |

## Procedure

### Step 1 Select an AC.

1. Choose **Network Application > WLAN Management**.
2. In the navigation tree, choose **Service Management > Configuration Wizard**.
3. Select **WLAN200** based on the data plan, and click **Next**.

### Step 2 Set AC basic attributes: Set AC parameters based on the AC configuration data in the data plan, and click **Next**.

### Step 3 Select APs.

1. Click **Add AP**.
2. In the **Select APs** window that is displayed, choose **Add AP > Create Manually**.
3. In the **Create Manually** window that is displayed, set parameters based on the AP configuration data in the data plan, and click **OK**. Then click **OK** in the dialog box that is displayed.
4. Click **Next**.

### Step 4 Configure profiles.

1. Create the AP profile, radio profile, and ESS profile based on the data plan.
2. Select a proper profile and set parameters based on the data plan. Then click **Next**.

### Step 5 Deploy the AP: Click **Deploy**. Then view the execution status in the **Deploy Status** column.

The deployment information is displayed in the **Result** column.

### Step 6 Click **Finish**.

----End

## 10.3 BGP/MPLS VPN Management

This topic describes terms, functions, and typical configuration examples of BGP/MPLS VPN management provided by eSight.

### 10.3.1 Understanding BGP/MPLS VPN

BGP/MPLS VPN is a Layer 3 Virtual Private Network (L3VPN). It uses BGP to advertise VPN routes and uses MPLS to forward VPN packets on backbone networks of service providers (SPs).

Enterprises or SPs use the BGP/MPLS VPN service to carry value-added services (VASs), such as data, voice, and video services.

#### 10.3.1.1 Terms

This topic describes BGP/MPLS VPN terms to help you better monitor and manage the BGP/MPLS VPN service on eSight.

[Table 10-14](#) lists the basic concepts.

**Table 10-14** Basic concepts

| Concept      | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CE           | It is an edge device on the user network. A CE provides interfaces to directly connect to the SP network. A CE can be a router, a switch, or a host. CEs cannot detect VPNs and do not need to support MPLS.                                                                                                                                                                                                       |
| PE           | It is an edge device on the SP network. A PE is directly connected to a CE. On the MPLS network, all handlings related to the VPN are performed on the PE. The requirement on the PE performance is high.<br>A PE can be connected to multiple CEs. A CE can be connected to multiple PEs of the same SP or of different SPs.                                                                                      |
| P            | It is a backbone device on the SP network. A P device is not directly connected to a CE. A P device needs to provide only basic MPLS forwarding capabilities, without maintaining the VPN information.                                                                                                                                                                                                             |
| Site         | A site is a group of IP systems with IP connectivity, which can be achieved independent of SP networks. A site is a basic unit for composing a VPN.                                                                                                                                                                                                                                                                |
| AS           | An autonomous system (AS) is a collection of IP networks and routers under the control of one or more network operators that presents a common routing policy to the Internet. An AS contains multiple devices.                                                                                                                                                                                                    |
| VPN Instance | A VPN instance is a VPN routing and forwarding (VRF) table.                                                                                                                                                                                                                                                                                                                                                        |
| VPN Target   | VPN targets are used by VPN instances to control VPN member relationship and routing principles of directly connected sites and remote sites. Each VPN instance is associated with one or more VPN targets (a site can belong to different VPNs), which are of the following types: <ul style="list-style-type: none"><li>Export target: A local PE learns IPv4 routes from the directly connected site,</li></ul> |

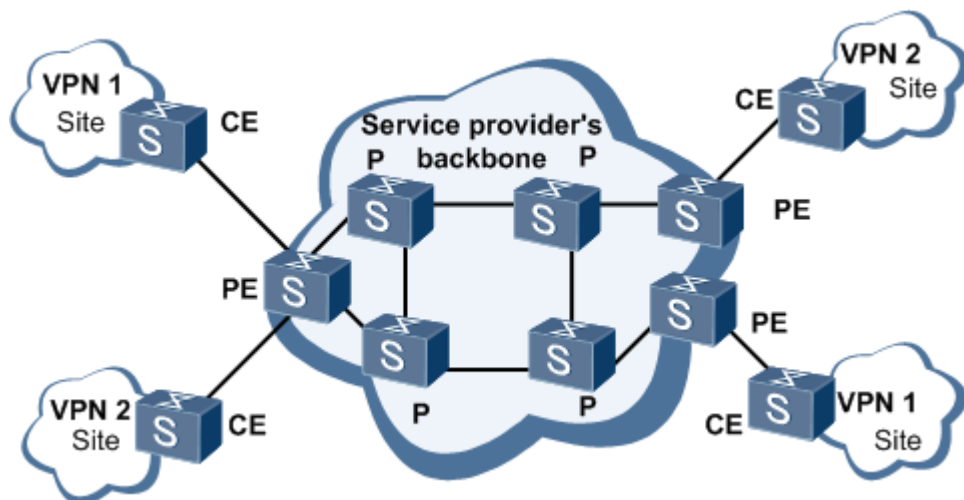
| Concept | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>then converts it to the VPN IPv4 routes and sets the export target attribute for these routes. The export target attribute is released together with routes as the BGP extension community attribute.</p> <ul style="list-style-type: none"><li>• Import target: When a PE receives VPN-IPv4 routes advertised by other PEs, the PE checks the export target attribute. When this attribute matches import target of a VPN instance, the PE adds the route to the route table of the VPN instance.</li></ul> <p>VPN target attributes define the sites that can receive a VPN route, and the sites from which the PE can receive routes.</p> <p>When receiving a route from a directly connected CE, the PEs associate this route with one or more export target attributes. BGP advertises the attributes with the VPN-IPv4 route to related PEs. When receiving the VPN-IPv4 route, the PEs compare the export target attributes with import target attributes of all their VPN instances. If the export target and import target attributes match each other, the PEs add the route to their VPN routing tables.</p> |

## BGP/MPLS VPN Basic Model

Both single-AS and inter-AS networks are based on the BGP/MPLS VPN basic model, which consists of the following parts: Customer Edges (CEs), Provider Edges (PEs), and Providers (Ps).

Figure 10-97 shows the BGP/MPLS VPN basic model.

**Figure 10-97** BGP/MPLS VPN basic model



### 10.3.1.2 Functions

The BGP/MPLS VPN management component provides the following functions for Huawei routers and switches of all series and mainstream non-Huawei devices: automatic discovery, service monitoring, and fault locating.

- Automatic discovery: Automatically discovers running services on networks to eSight for unified management and monitoring.
- Service monitoring: Monitors service operating status and quality with the following: viewing service topology, monitoring service performance, viewing service reports, and auditing service quality.
- Fault locating: Enables you to view alarms and locate faults. Alarms are displayed in the service topology and service list in centralized mode. You can select a service or select a link on the topology page to generate a diagnosis task. Then check the network connection status and locate faults based on the diagnosis result.

### 10.3.1.3 Application Scenarios

There are two categories of BGP/MPLS VPN networks: single-AS network and inter-AS network.

Single-AS networks are as follows:

- Full-Mesh
- Hub-Spoke
- MCE
- HoVPN

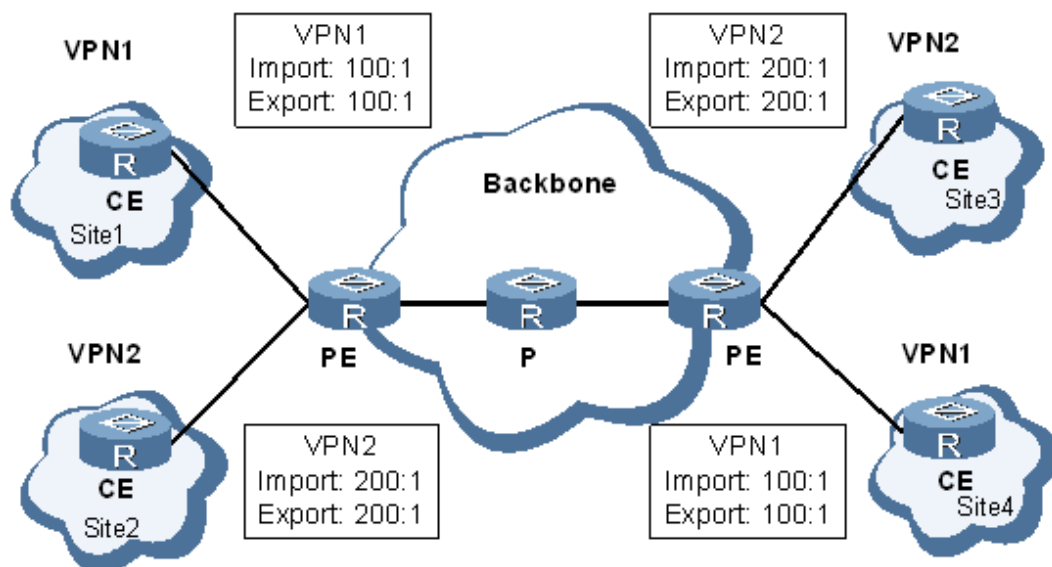
Inter-AS networks are as follows:

- Inter-AS VPN Option A
- Inter-AS VPN Option B

#### Full-Mesh Network

All users on a VPN form a closed user group and can forward data to each other, but these users cannot communicate with any users outside the VPN. A VPN target must be exclusively distributed to a VPN as the export target and import target.

[Figure 10-98](#) shows the Full-Mesh network.

**Figure 10-98** Full-Mesh network

## Hub-Spoke Network

If a central access control device is to be set on a VPN to enable other users to access each other through the central access control device, the Hub-Spoke network scheme can be used. The site where the access control device locates is called a Hub site; other sites are called Spoke sites. At the Hub site, a device that accesses the VPN backbone network is called a Hub-CE; at a Spoke site, a device that accesses the VPN backbone network is called a Spoke-CE. On the VPN backbone network, a device that accesses the Hub site is called a Hub-PE; a device that accesses a Spoke site is called a Spoke-PE.

A Spoke site advertises routes to the Hub site; then the Hub site advertises the routes to other Spoke sites. No direct route exists between the Spoke sites. The Hub site controls the communication between the Spoke sites.

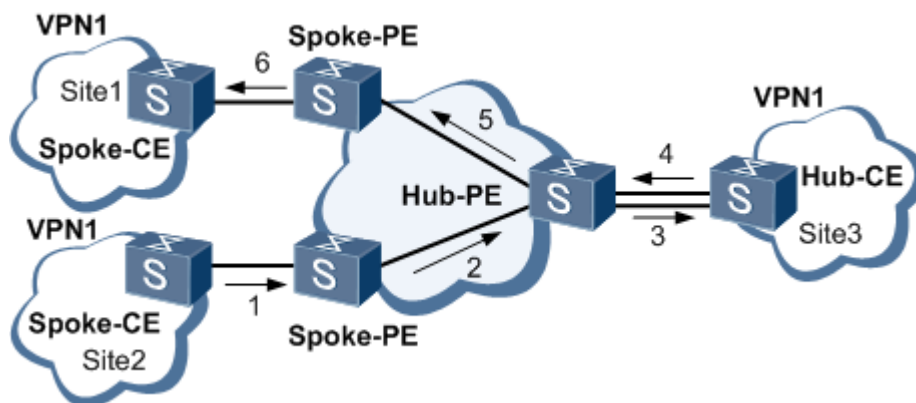
In the Hub-Spoke network scheme, two VPN targets are configured to stand for Hub and Spoke respectively.

The configuration of a VPN target on a PE must comply with the following rules:

- The export target and the import target of the Spoke-PE at a Spoke site are Spoke and Hub respectively. The import route target of a Spoke-PE is different from the export route targets of other Spoke-PEs.
- A Hub-PE requires two interfaces or sub-interfaces. One interface or sub-interface receives routes from Spoke-PEs, and the import target of the VPN instance on the interface is Spoke. The other interface or sub-interface advertises the routes to Spoke-PEs, and the export target of the VPN instance on the interface is Hub.

Figure 10-99 shows the Hub-Spoke network.



**Figure 10-99** Hub-Spoke network

## MCE Network

The traditional BGP/MPLS IP VPN architecture requires that each VPN instance use an independent CE to connect to PEs.

With increasingly divided user services and high security requirements, a private network must be divided into different VPNs. Users on different VPNs are isolated. In the Multi-VPN-Instance CE (MCE) network scheme, an MCE can be connected to multiple VPNs to isolate services or users.

In the MCE network scheme, PEs provide the following functions:

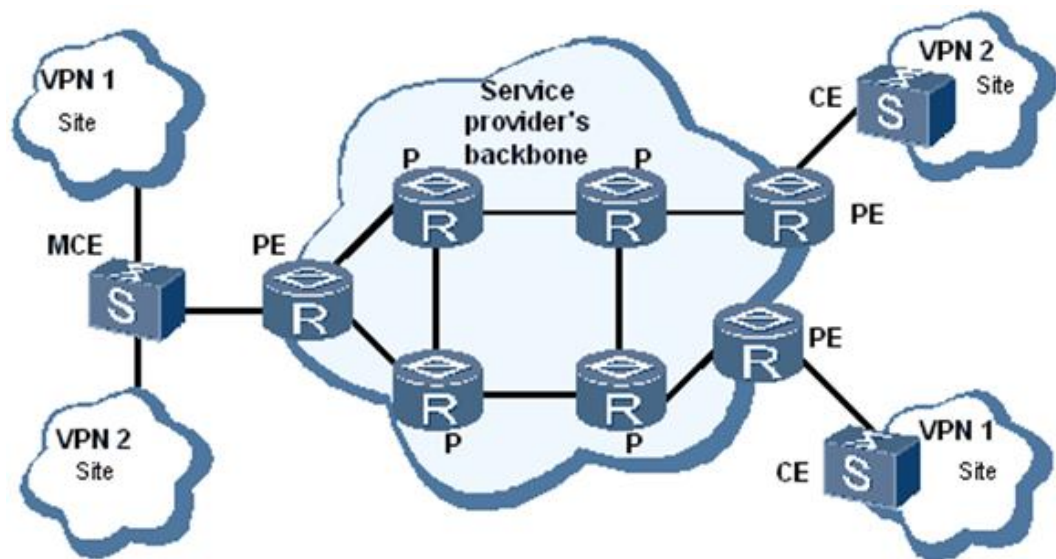
- Create and maintain an independent multi-VRF table for each VPN.
- Process all VPN services.

MCEs provide the following functions:

- Create and maintain an independent multi-VRF table for each VPN.
- Bind VLAN interfaces on CEs to VPNs or VRFs to isolate services on different VPNs.

[Figure 10-100](#) shows the MCE network.

**Figure 10-100** MCE network



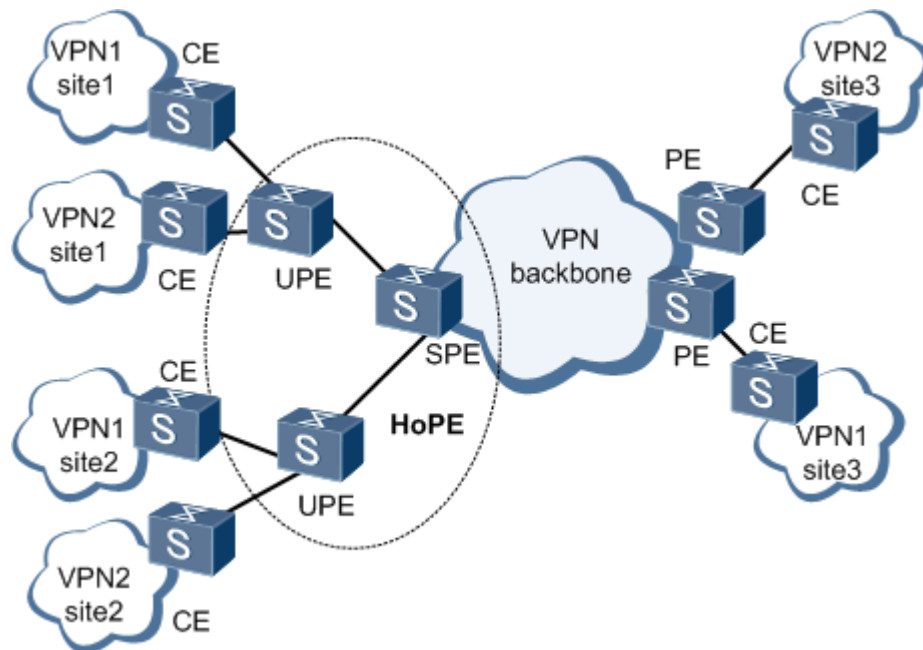
## HoVPN Network

On a Hierarchy of VPN (HoVPN), the functions of a PE are distributed among multiple PEs. Playing different roles, the PEs form a hierarchical architecture and fulfill the functions of a centralized PE. An HoVPN is also called a Hierarchy of PE (HoPE).

On a BGP/MPLS VPN, as the key devices, PEs provide the following functions:

- Access user services and require a great number of interfaces.
- Manage and advertise VPN routes, and process user packets. PEs require large-capacity memory and high forwarding capabilities.

Figure 10-101 shows the HoVPN network.

**Figure 10-101** HoVPN network

PEs are classified into the following types based on the location:

- UPE: User-end provider edges (UPEs) are connected to user devices. UPEs maintain the routes of directly connected VPN sites, but do not maintain the routes of remote VPN sites. UPEs assign inner labels to the routes of directly connected sites, and advertise the labels with the VPN routes to SPEs using MP-BGP.
- SPE: Service Provider-end PEs (SPEs) manage and advertise VPN routes. SPEs maintain all routes of the VPN sites connected through UPEs, including the routes of local and remote sites. SPEs advertise only the default routes of VPN instances that carry labels to UPEs.

## Inter-AS VPN Option A Network

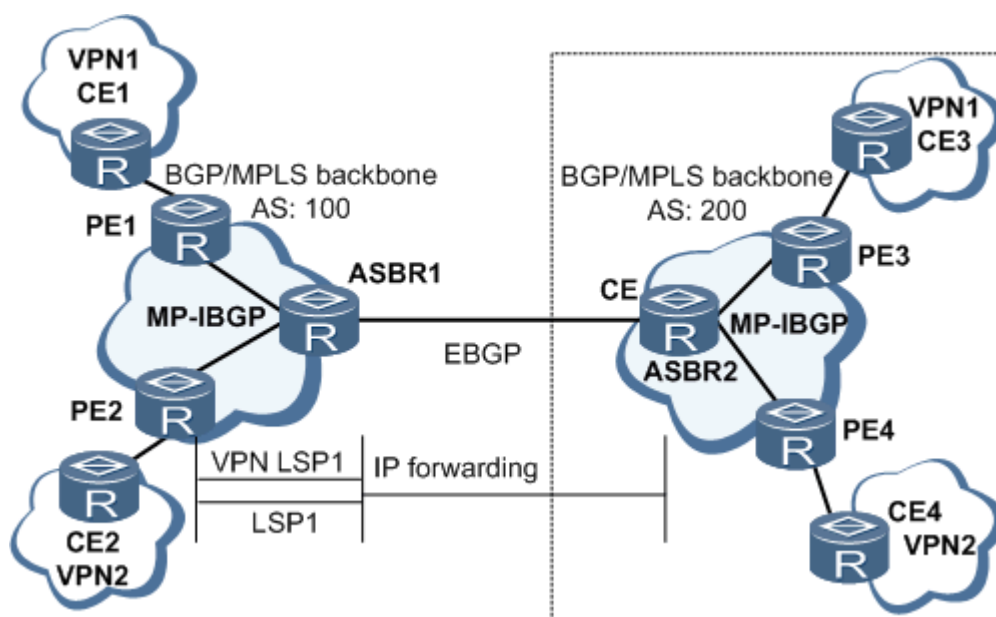
With the wide application of MPLS VPN solutions, different Metropolitan Area Networks (MANs) of a carrier or collaborating backbone networks of different carriers frequently span multiple ASs.

Generally, an MPLS VPN architecture runs within an AS in which the VPN routing information is flooded on demand. The VPN routing information within the AS cannot be flooded to the AS of other SPs. To exchange VPN information between different ASs, the inter-AS MPLS VPN model is introduced. The inter-AS MPLS VPN model is an extension of the existing protocol and MPLS VPN framework. Through this model, the route prefix and label information can be advertised over the links between different carrier networks.

As a basic BGP/MPLS VPN application in the inter-AS scenario, Option A does not need special configurations and MPLS does not need to run between Autonomous System Boundary Routers (ASBRs). With Option A, ASBRs in two ASs are directly connected and function as PEs in their respective ASs. Either of the ASBR PEs takes the peer ASBR as its CE and advertises IPv4 routes to the peer ASBR using External BGP (EBGP).

Figure 10-102 shows the Inter-AS VPN Option A network.

**Figure 10-102** Inter-AS VPN Option A network



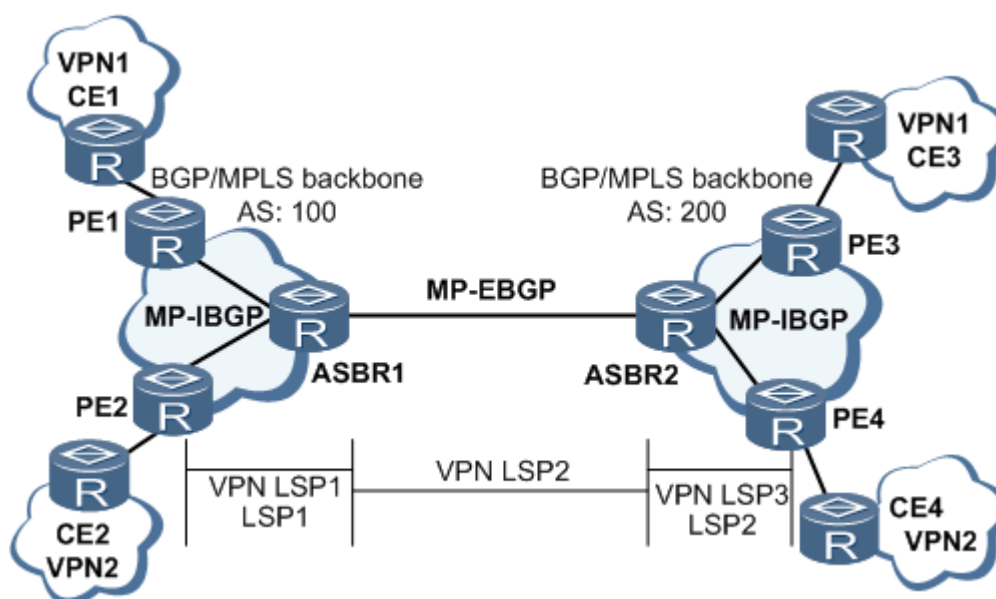
In the preceding figure, ASBR2 is a CE for ASBR1 in AS100, and ASBR1 is a CE for ASBR2.

## Inter-AS VPN Option B Network

In Option B, using MP-EBGP, two ASBRs receive the labeled VPN-IPv4 routes from the PEs in the ASs respectively and then exchange the routes.

Figure 10-103 shows the Inter-AS VPN Option B network.

**Figure 10-103** Inter-AS VPN Option B network



## Comparison Between Options A and B

Table 10-15 lists the Comparison Between Options A and B.

**Table 10-15** Comparison between Options A and B

| Inter-AS VPN | Characteristics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Option A     | This solution is easy to implement because MPLS is not required between ASBRs and no special configuration is required. The expansibility, however, is poor because ASBRs must manage all VPN routes and create VPN instances for each VPN. As a result, a large number of VPN-IPv4 routes exist on the PE. In addition, because common IP forwarding is performed between ASBRs, each inter-AS VPN requires different interfaces, which can be subinterfaces, physical interfaces, or bound logical interfaces. Therefore, Option A requires high performance of PEs. If a VPN spans multiple ASs, the intermediate ASs must support VPN services. This requires complex configurations and greatly affects the operation of the intermediate ASs. If the number of inter-AS VPNs is small, Option A can be used. |
| Option B     | Unlike Option A, Option B is not limited by the number of links between ASBRs. VPN routing information is stored on and forwarded by ASBRs. When a great number of VPN routes exist, the overburdened ASBRs are likely to become bottlenecks. Therefore, in the MP-EBGP solution, the ASBRs that maintain VPN routing information do not forward IP addresses on the public network.                                                                                                                                                                                                                                                                                                                                                                                                                               |

### 10.3.2 Overview

This topic describes the BGP/MPLS VPN management process from the following tasks: deploying a network, deploying services, discovering services, and maintaining services.

Figure 10-104 shows the BGP/MPLS VPN management process.

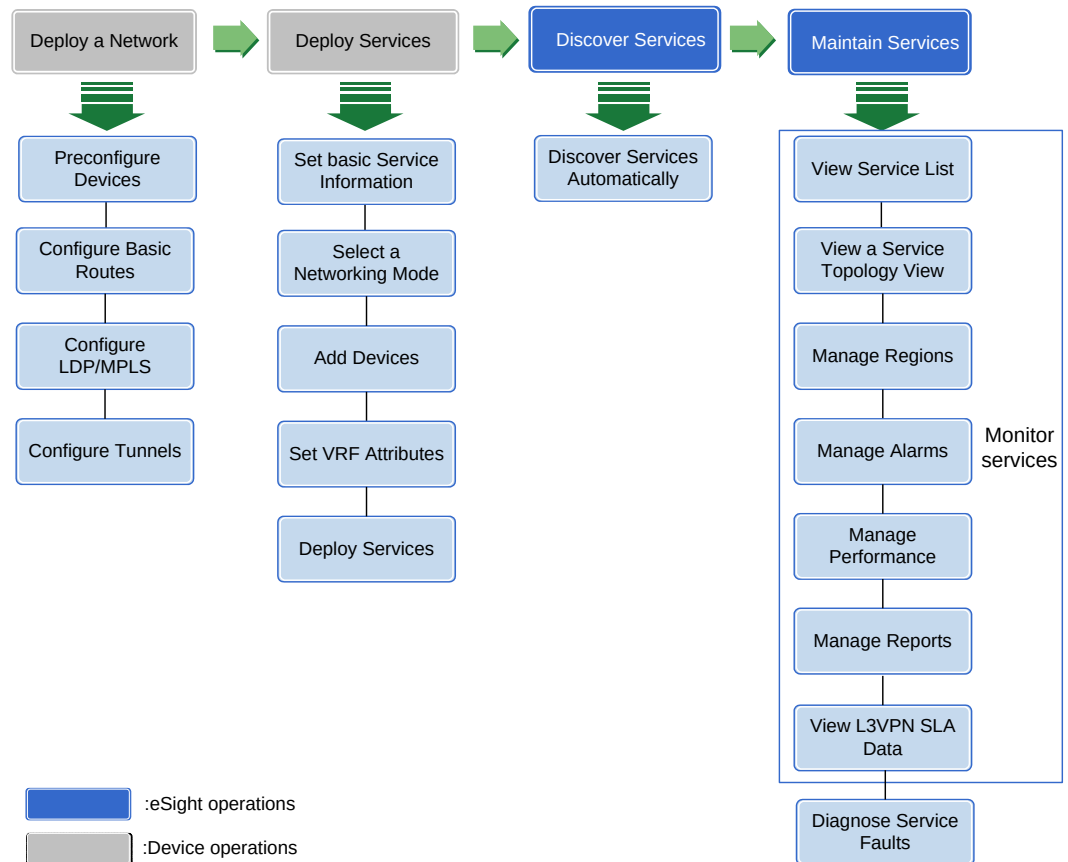
**Figure 10-104** BGP/MPLS VPN management process

Table 10-16 lists the management process in detail.

**Table 10-16** BGP/MPLS VPN management process

| Operation         |                                  | Description                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deploy a network  |                                  | Perform this task before you deploy L3VPN services. This task includes preconfiguring devices, and configuring basic routes, LDP/MPLS, and tunnels. This task is performed on devices.                                                                                                                                   |
| Deploy services   |                                  | Create and configure services on devices. Before creating services, you can view service resources to understand existing VRF information. This task is performed on devices.                                                                                                                                            |
| Discover services |                                  | Discover existing services on a network to eSight for unified management. This task is performed on eSight.                                                                                                                                                                                                              |
| Maintain services | <a href="#">Monitor services</a> | This task includes monitoring service alarms, performance, service quality, and performance reports, and viewing the service topology. The service topology provides access to service operations, displays alarms in colors, and allows you to view alarms using the topology access. This task is performed on eSight. |

| Operation |                                         | Description                                                                                                                                                                                                                     |
|-----------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <a href="#">Diagnose Service Faults</a> | Service alarms are displayed in a service list or service topology in centralized mode. You can click a service alarm to view alarm details and use service diagnosis tools to locate faults. This task is performed on eSight. |

## 10.3.3 Automatic Discovery

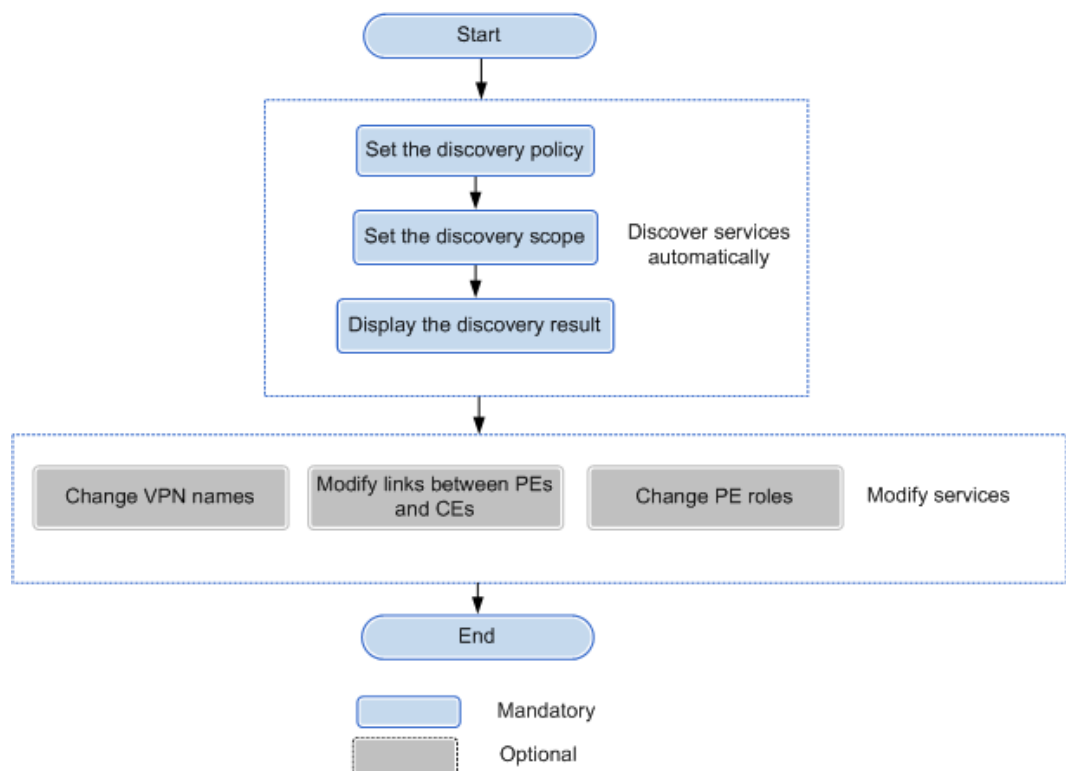
When BGP/MPLS VPN services are deployed or changed on a network, the BGP/MPLS VPN automatic discovery function can discover updated L3VPN services to eSight.

### 10.3.3.1 Automatic Discovery Process

This topic describes the BGP/MPLS VPN automatic discovery process.

[Figure 10-105](#) shows the automatic discovery flowchart.

**Figure 10-105** Automatic discovery flowchart



[Table 10-17](#) lists the automatic discovery process in detail.

**Table 10-17** Automatic discovery process

| Operation | Description                                                             |
|-----------|-------------------------------------------------------------------------|
| Discover  | Set the discovery policy and discovery scope to discover L3VPN services |

| Operation              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| services automatically | <p>on devices that have completed network deployment and service deployment to eSight.</p> <p>Discover services automatically including: Set the discovery policy, Set the discovery scope, and Display the discovery result.</p> <ol style="list-style-type: none"><li>1. Set the discovery policy<br/>The discovery policy can be discovery by Discover by VRF connection or discovery by VRF name.<br/>You can use the policy of discovery by VRF name when VRF names are the same on VPN.</li><li>2. Set the discovery scope<br/>The discovery scope can be selected devices or global PEs/CEs.</li><li>3. Display the discovery result<br/>The discovery result includes the following information: L3VPN name, discovery status, and actual operation.</li></ol>                                                                                                                                                                                                                                                                |
| Modify services        | <p>Modify the following information about discovered services: L3VPN name, device role, and service link.</p> <p>Modify services including: Change the L3VPN name, Modify links between PEs and CEs, and Change the PE role.</p> <ol style="list-style-type: none"><li>1. Change the L3VPN name<br/>Change names of discovered L3VPNs.</li><li>2. Modify links between PEs and CEs<br/>eSight can automatically discover service links between PEs and CEs if they exchange private routes using Open Shortest Path First (OSPF), Intermediate System to Intermediate System (ISIS), or External BGP (EBGP), where BGP refers to Border Gateway Protocol. When PEs and CEs exchange private routes using static routes or Routing Information Protocol (RIP), eSight cannot automatically discover service links between them. You must manually add, delete, or modify CEs.</li><li>3. Change the PE role<br/>You can change the PE role based on the site scenario. The values are <b>PE</b>, <b>UPE</b>, and <b>SPE</b>.</li></ol> |

### 10.3.3.2 Discovering Services Automatically

This topic describes how to set the discovery policy and discovery scope to discover L3VPN services on devices where the network and services have been deployed to eSight.

#### Prerequisites

- You are an "operator" or a superior eSight user and have the device management permission.
- The network and services have been deployed on devices.



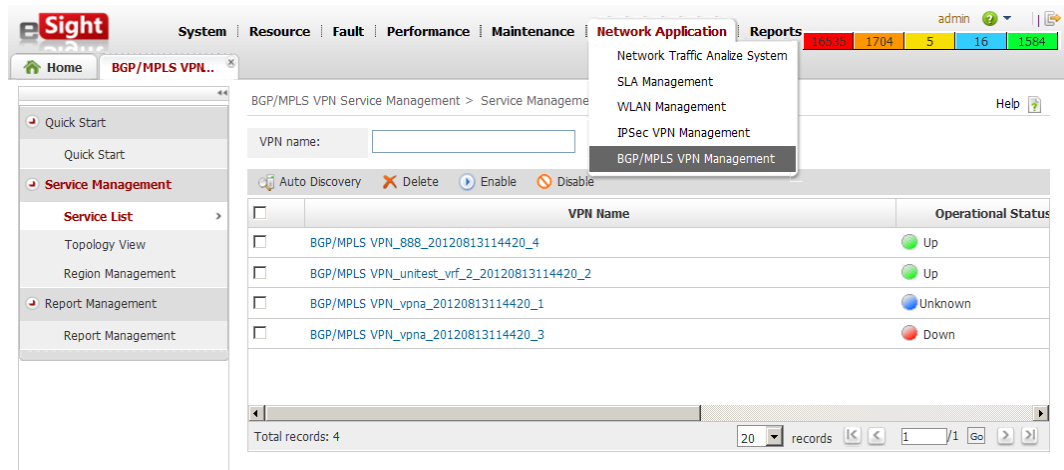
## Context

BGP/MPLS VPN service automatic discovery does not affect NE configurations. BGP/MPLS VPN service data is uploaded only to or updated only in eSight.

## Procedure

**Step 1** Choose **Network Application** > **BGP/MPLS VPN Management**.

**Figure 10-106** BGP/MPLS VPN management



**Step 2** In the navigation tree, choose **Service Management** > **Service List**, and click **Auto Discover**.

**Step 3** Select the discovery policy and discovery scope.

**Figure 10-107** Discovering services automatically

Synchronize updated VPN services to eSight when BGP/MPLS VPN services are deployed or changed on a network.

Discovery policy: ☒ Discover by VRF connection ☐ Discover by VRF name (use this policy when VRF names are the same on VPN)

Discovery range: ☐ Select Device Global PE/CE

| <input checked="" type="checkbox"/> | Name        | IP Address    | Type      | Vendor | Synchronization Result |
|-------------------------------------|-------------|---------------|-----------|--------|------------------------|
| <input checked="" type="checkbox"/> | S93         | 10.137.61.32  | S9306     | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_23 | 198.221.20.23 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_24 | 198.221.20.24 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_30 | 198.221.20.30 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_25 | 198.221.20.25 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_28 | 198.221.20.28 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_21 | 198.221.20.21 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_27 | 198.221.20.27 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_29 | 198.221.20.29 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_22 | 198.221.20.22 | S5352C-EI | Huawei |                        |
| <input checked="" type="checkbox"/> | CON6K_53_26 | 198.221.20.26 | S5352C-EI | Huawei |                        |

Discovery result:

| VPN Name   | Discovery Status | Operation |
|------------|------------------|-----------|
| No record. |                  |           |

Discovery policy:

- If you select **Discover by VRF connection**, VRFs are discovered as services according to routing policy. The import RT of a device is the export RT of another device.
- If you select **Discover by VRF name**, VRFs are discovered as services according to VRF name.

Discovery scope:

- Select **Select Device**, and click . In the dialog box that is displayed, select one or more NEs, and click **OK**. eSight discovers services on the selected NE(s).
- If you select **Global PE/CE**, eSight discovers services on devices that support L3VPN services.

#### Step 4 Click **Discover**.

eSight synchronizes data with NEs and discovers services on NEs based on the configured discovery policy and discovery scope. The data synchronization progress and service discovery progress are displayed.



#### NOTE

To terminate automatic discovery in progress, click **Cancel**.

----End

## Result

The results are displayed in the automatic discovery result list.

**VPN Name:** L3VPN service name that has been discovered. Click a service name to modify the service.

**NOTE**

The **VPN Name** value is in the format BGP/MPLS VPN\_time\_sequence number.

The values of **Discovery Status** are as follows:

- **New service:** Indicates that a service is newly added to eSight in automatic discovery.
- **Change service:** Indicates that a service exists in eSight and is updated in automatic discovery. For example, if a link between two PEs or a link between a PE and a CE is changed, automatic discovery synchronizes the link in eSight with that on NEs.
- **Service deleted:** Indicates that a service is deleted from eSight in automatic discovery.

## Follow-up Procedure

The following table describes the operations that you can perform on the **Auto Discover** page after discovering services.

| Operation                    | Operation Method                                                                                                                                        |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change service name          | Click  corresponding to a service to change the service name.          |
| View service access topology | Click  corresponding to a service to view the service access topology. |

### 10.3.3.3 Modifying Services

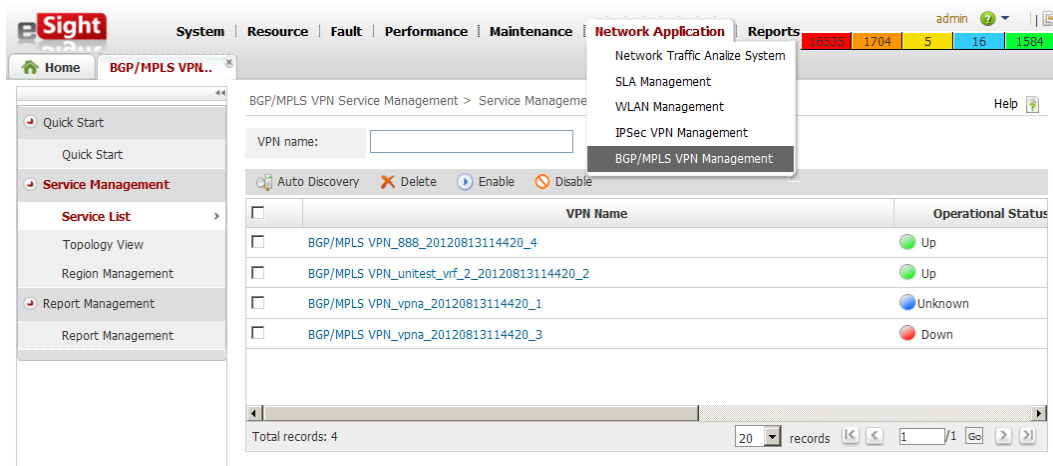
This topic describes how to change names, device roles, and service links for discovered L3VPN services.

## Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

## Procedure

**Step 1** Choose **Network Application > BGP/MPLS VPN Management**.

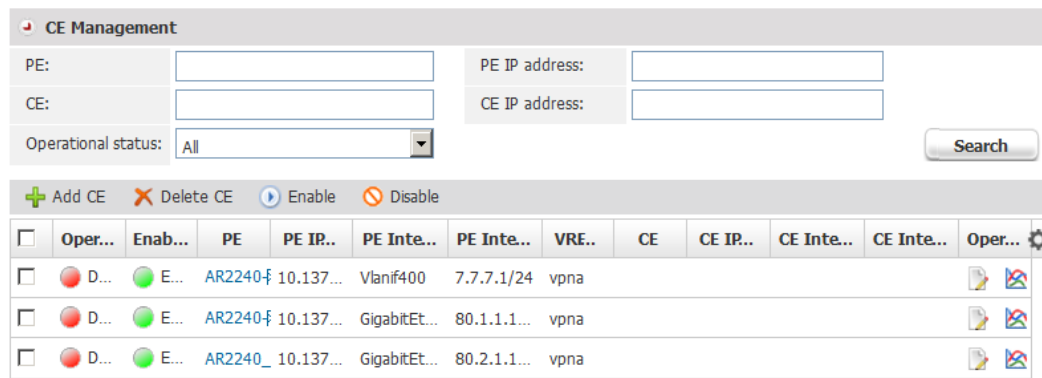
**Figure 10-108** BGP/MPLS VPN management

**Step 2** In the navigation tree, choose **Service Management** > **Service List**, click  **Change the name**, and change the L3VPN service name.

**Step 3** In **Service List** or the automatic discovery result, click an L3VPN service that you want to modify.

The page for modifying the L3VPN service is displayed.

**Step 4** In the **CE Management** list, click **Add CE**, **Delete CE**, or **Modify CE** to change links between PEs and CEs.

**Figure 10-109** CE management**NOTE**

eSight can automatically discover service links between PEs and CEs if they exchange private routes using Open Shortest Path First (OSPF), Intermediate System to Intermediate System (ISIS), or External BGP (EBGP), where BGP refers to Border Gateway Protocol. When PEs and CEs exchange private routes using static routes or Routing Information Protocol (RIP), eSight cannot automatically discover service links between them. You must manually add, delete, or modify CEs in eSight.

**Step 5** In the **Service Link** list, click **Change Device Role**, and change the PE role based on the site scenario. Device roles include **UPE**, **SPE**, and **PE**.

**Figure 10-110** Service link

| Source D.. | Source D..   | Source IP.. | Source VRF | Destinati.. | Destinati..  | Destinati.. | Destinati.. | Operation |
|------------|--------------|-------------|------------|-------------|--------------|-------------|-------------|-----------|
| PE         | AR2240-网...  | 7.7.7.9     | vpna       | PE          | AR2240_22... | 8.8.8.9     | vpna        |           |
| PE         | AR2240_22... | 8.8.8.9     | vpna       | PE          | AR2240-网...  | 7.7.7.9     | vpna        |           |

----End

## 10.3.4 Monitoring Services

This topic describes how to monitor the operating status of BGP/MPLS VPN services that are automatically discovered by eSight.

### 10.3.4.1 Viewing Service List

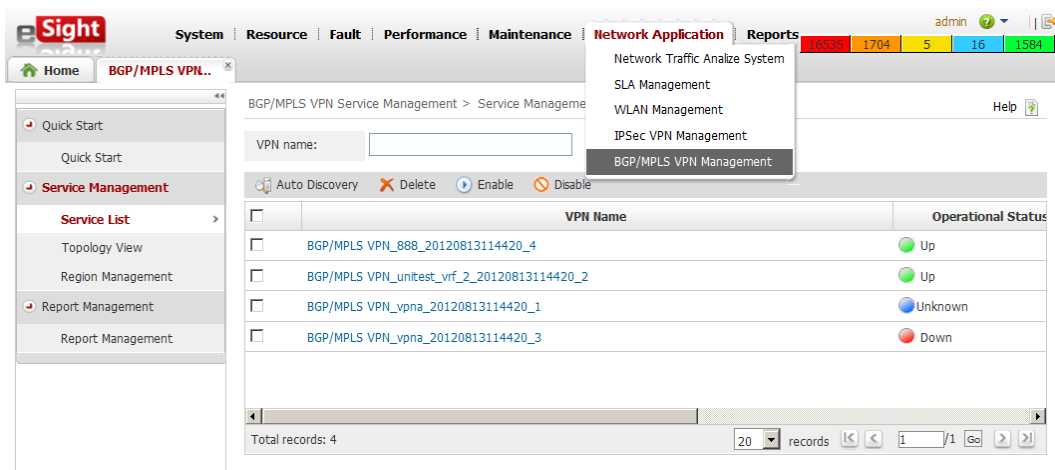
This topic describes how to view the L3VPN service list and L3VPN service details.

## Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

## Procedure

**Step 1** Choose **Network Application** > **BGP/MPLS VPN Management**.

**Figure 10-111** BGP/MPLS VPN management

**Step 2** In the navigation tree, choose **Service Management** > **Service List**.

**Figure 10-112** Service list

| Auto Discovery  Delete  Enable  Disable |                                                 |                    |               |                |           |
|-----------------------------------------|-------------------------------------------------|--------------------|---------------|----------------|-----------|
| <input type="checkbox"/>                | VPN Name                                        | Operational Status | Enable Status | Alarm Severity | Operation |
| <input type="checkbox"/>                | BGP/MPLS VPN_DC-rnd_20120406095418_1            | Partially Down     | Enabled       |                |           |
| <input type="checkbox"/>                | BGP/MPLS VPN_StarWars_20120323113735_3          | Partially Down     | Enabled       | Major          |           |
| <input type="checkbox"/>                | BGP/MPLS VPN_TheLordoftheRings_20120323113735_2 | Partially Down     | Enabled       | Major          |           |

The L3VPN service list is displayed, including the following information: **VPN Name**, **Operating Status**, **Enable Status**, and **Alarm Severity**.

**NOTE**

**Operating Status:** link status between a PE and CE and VRF operating status.

**Enable Status:** management status of an interface that connects a PE.

**Alarm Severity:** highest severity of L3VPN alarms generated by both devices and L3VPN services. L3VPN alarms are of the following types: alarms indicating status of L3VPN service interfaces on PEs or CEs, alarms indicating VRF status, performance counter alarms for L3VPN services, device offline alarms, and L3VPN service SLA alarms.

- Step 3** Click an L3VPN service, and view the following information about the service: **CE Management**, **Service Link**, **VRF Instance**, and **Route Configuration**.

**Figure 10-113** Service information

| > CE Management                |          |           |               |
|--------------------------------|----------|-----------|---------------|
| > Service Link                 |          |           |               |
| > VRF Instance                 |          |           |               |
| > Route Configuration          |          |           |               |
| BGP OSPF ISIS Static Route RIP |          |           |               |
| Name                           | VRF Name | AS Number | Route ID      |
| gugan_AR3260_222               | vpna     | 100       | 202.92.36.222 |
| gugan_AR3260_223               | vpna     | 100       | 33.1.1.1      |

----End

## Follow-up Procedure

In the L3VPN service list, you can perform the following operations.

| Operation                | Operation Method                                                                                                                                       |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable an L3VPN service  | Click <b>Enable</b> . The L3VPN service changes to the <b>Enabled</b> state.                                                                           |
| Disable an L3VPN service | Click <b>Disable</b> . The L3VPN service changes to the <b>Disabled</b> state.<br><b>NOTE</b><br>An L3VPN service is interrupted after being disabled. |

| Operation               | Operation Method                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------|
| Delete an L3VPN service | Click  Delete . |

### 10.3.4.2 Viewing a Service Topology View

This topic describes how to view an L3VPN service topology view to understand the topology structure and service operating status.

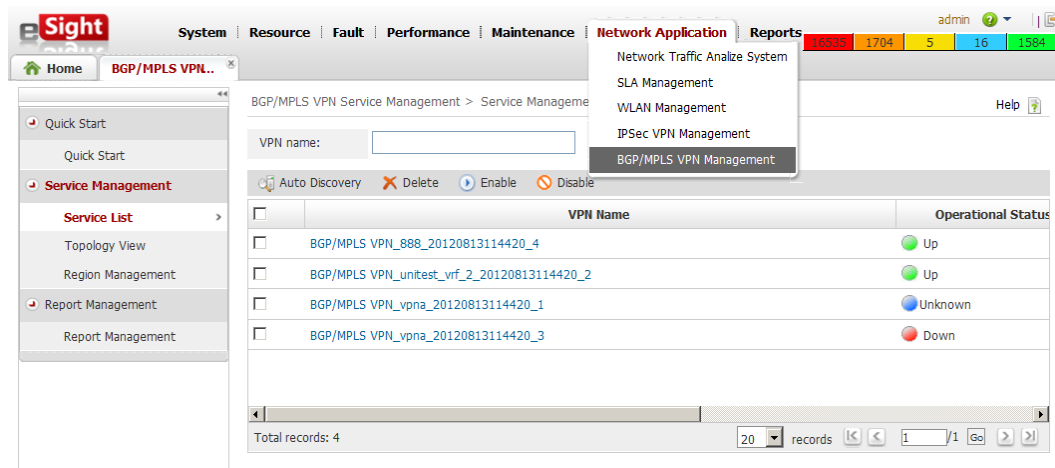
#### Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

#### Procedure

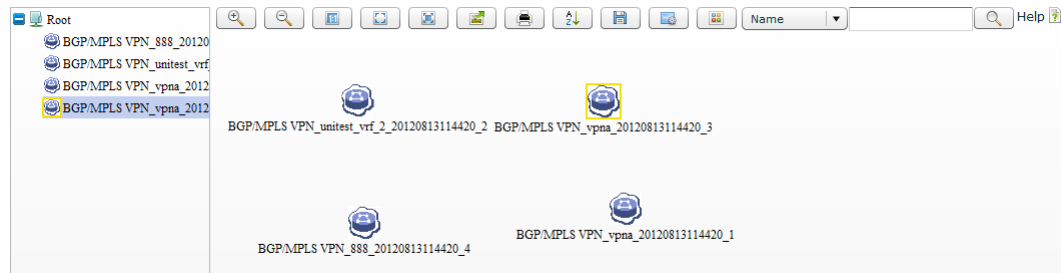
**Step 1** Choose **Network Application > BGP/MPLS VPN Management**.

**Figure 10-114** BGP/MPLS VPN management



**Step 2** View the entire network topology view in either of the following ways:

- In the navigation tree, choose **Service Management > Service List**. Select an L3VPN service, click  and choose  **Topology View** .  
The **Topology View** page is displayed.
- In the navigation tree, choose **Service Management > Topology View**.  
The **Topology View** page is displayed.

**Figure 10-115** BGP/MPLS VPN topology view

**Step 3** On the **Topology View** page, view the L3VPN topology view of the entire network.

- View the topology view of a single L3VPN service, as shown in [Figure 10-116](#).

**Figure 10-116** Topology view of a single L3VPN service

- View the highest L3VPN alarm severity. When an L3VPN alarm is generated, the matching L3VPN service is enclosed in a box. The box color indicates the highest severity of L3VPN alarms, as shown in [Figure 10-117](#).

**Figure 10-117** Highest L3VPN alarm severity

#### NOTE

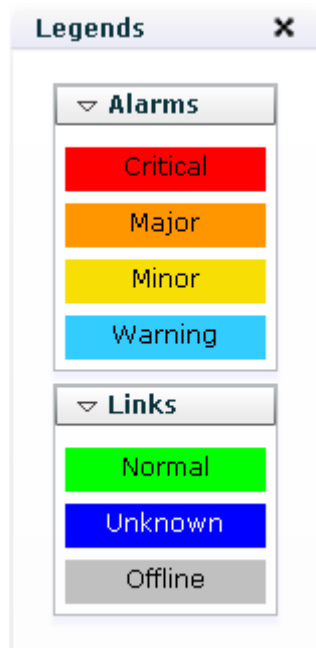
L3VPN alarms are generated by both devices and L3VPN services. L3VPN alarms are of the following types: alarms indicating status of L3VPN service interfaces on PEs or CEs, alarms indicating VRF status, performance counter alarms for L3VPN services, device offline alarms, and L3VPN service SLA alarms.

The box color indicates the alarm severity. The red color indicates critical alarms. The orange color indicates major alarms. The yellow color indicates minor alarms. The blue color indicates warnings.

- Click , and view topology legends, as shown in [Figure 10-118](#). This helps you understand the alarm status and operating status of topology objects.



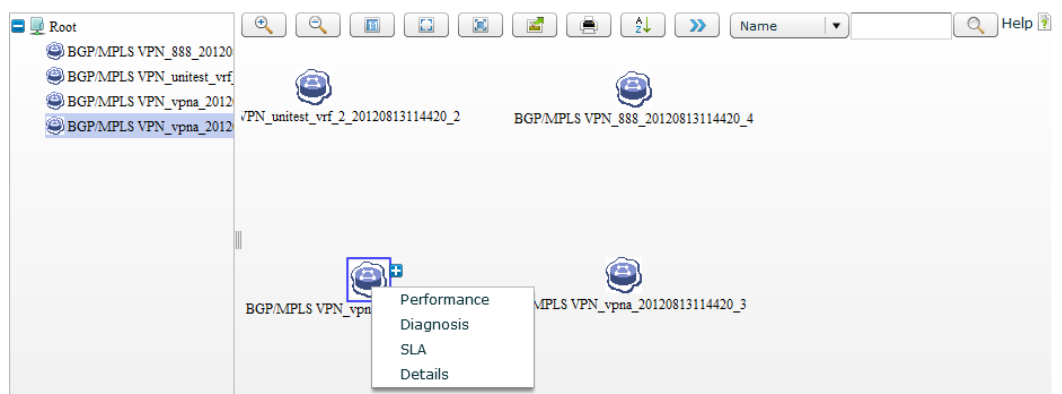
**Figure 10-118** Topology legends



**Step 4** On the **Topology View** page, select an L3VPN service, and perform the following operations as required:

- View performance data: Right-click, and choose **Performance**.
- Diagnose the service quickly: Right-click, and choose **Diagnosis**.
- Monitor service quality: Right-click, and choose **SLA**.
- View details: Right-click, and choose **Details**.
- Expand or collapse the service topology view: Click  to expand the service topology view. Click  to collapse the service topology view.

**Figure 10-119** BGP/MPLS VPN topology operations



**Step 5** On the **Topology View** page, double-click an L3VPN service to view the topology details.

In the topology view of a single service, you can view the source PE and destination PE, CEs connected to the PEs, links between PEs, and links between PEs and CEs.

**NOTE**

If no CE is selected in automatic service discovery, only PE information is displayed in the PE-CE link information.

In the topology view of a single service, you can perform the following operations:

- View basic information about a device: Right-click a device, and choose **Management** . Then view basic information on the **Management** page.
- View alarms on a device (both alarms generated by the device and alarms generated by eSight): Right-click a device, and choose **View alarms** . Then view alarms on the **View alarms** page.
- Diagnose links between PEs or between PEs and CEs: Right-click a link, and choose **Link diagnosis** . Then diagnose the link on the **Quick Diagnosis** page.
- View L3VPN performance trend: Right-click a link between a PE and a CE, and choose **Link performance** . Then view L3VPN performance trend on the **Link performance** page.
- View the highest L3VPN alarm severity on a PE or CE in a tooltip, as shown in [Figure 10-120](#).

**Figure 10-120** Highest L3VPN alarm severity on a PE

**NOTE**

When an L3VPN alarm is generated on a PE or CE, the alarm is displayed in a tooltip. The tooltip color indicates the highest L3VPN alarm severity. The red color indicates critical alarms. The orange color indicates major alarms. The yellow color indicates minor alarms. The blue color indicates warnings.

- View links: Links are displayed as straight lines. View links between PEs and CEs, between PEs, between PEs and regions, and between CEs and regions.
- View link status: The link color indicates the link status between two devices.

**NOTE**

The green color indicates a normal link. The blue color indicates an unknown link. The gray color indicates that a device is offline or an interface is disabled.

- View region information, as shown in [Figure 10-121](#). If an L3VPN alarm is generated in a region, the region is enclosed in a box.

**Figure 10-121** Region information



Double-click a region icon, and view devices and links between devices in the region.

**NOTE**

A region will be displayed in a topology view only after devices involved in an L3VPN service are imported to region management.

----End

### 10.3.4.3 Managing Regions

A region is a set of network devices at the same location. You can manage regions to implement hierarchical management of network devices.

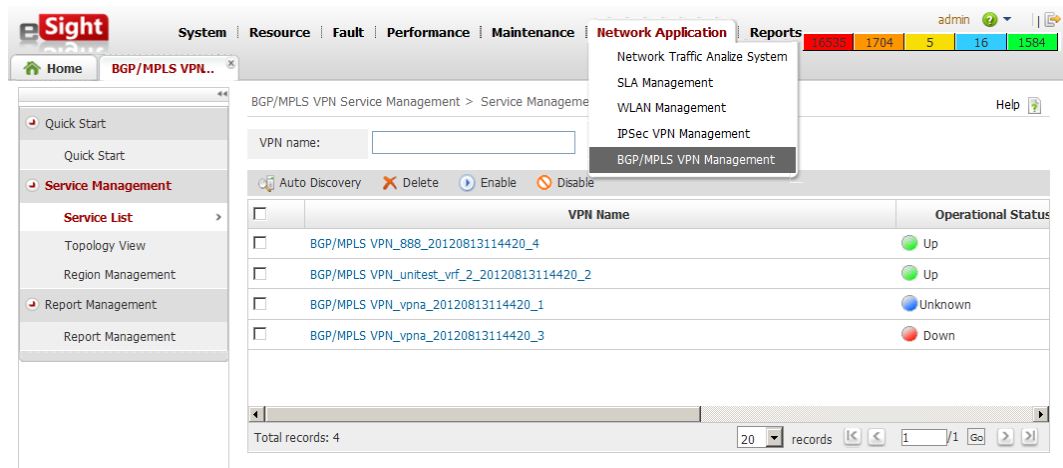
#### Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

#### Procedure

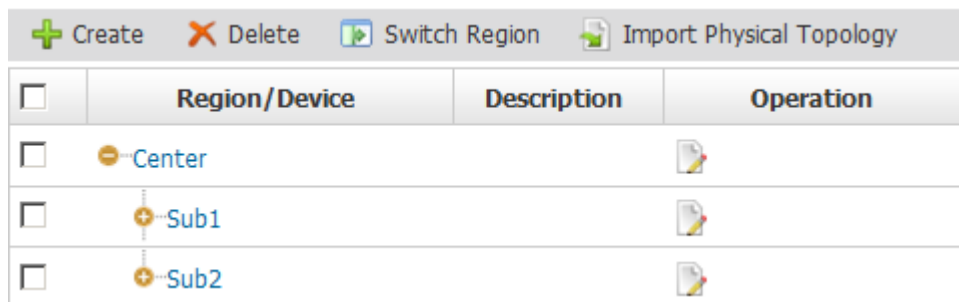
**Step 1** Choose **Network Application** > **BGP/MPLS VPN Management**.

**Figure 10-122** BGP/MPLS VPN management



**Step 2** In the navigation tree, choose **Service Management** > **Region Management**.

**Figure 10-123** Managing regions



Perform the following operations shown in [Table 10-18](#) in the region management list.

**Table 10-18** Region management operations

| Operations                      | Operation Method                                                                                                                                                                                                                                                                   |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a region                 | Click  <b>Create</b> .                                                                                                                                                                            |
| Modify a region                 | Click  in the <b>Operation</b> column.                                                                                                                                                            |
| Import a physical topology view | Click  <b>Import Physical Topology</b> .<br><b>NOTE</b><br>When subnets created in a physical topology view are imported to the region management page, devices on the subnets are also imported. |
| Delete a region                 | 1. Select a region.<br>2. Click  <b>Delete</b> .                                                                                                                                                  |
| View region information         | Select a record in the <b>Subregion/Device</b> column, and view region details.                                                                                                                                                                                                    |

----End

## Follow-up Procedure

- Perform the following operations on the region details page as required.

| Operation                    | Operation Method                                                                                                                                                                                                                                                                                                       |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add a subregion              | Click  <b>Add Subregion</b> .<br><b>NOTE</b> <ul style="list-style-type: none"><li>A subregion can be added only to an existing region or subregion.</li><li>A region can contain a maximum of nine layers of subregions.</li></ul> |
| Switch regions for a device  | Select a device in a region, and click  <b>Switch Region</b> .<br><b>NOTE</b><br>Subregions cannot be switched to other regions.                                                                                                  |
| Import a device              | Click  <b>Import PE Device</b> .                                                                                                                                                                                                    |
| Delete a subregion or device | Select a subregion or device, and click  <b>Delete</b> .                                                                                                                                                                          |
| View region information      | Select a record in the <b>Sub Region/PE Name</b> column, and view subregion details.                                                                                                                                                                                                                                   |

- Perform the following operations on the subregion details page as required.

| Operation                    | Operation Method                                                                                                                                                                                                                                                                                                     |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add a subregion              | Click  <b>Add Subregion</b> .<br><b>NOTE</b> <ul style="list-style-type: none"><li>A subregion can be added only to an existing region or subregion.</li><li>A region can contain a maximum of nine layers of subregions.</li></ul> |
| Switch regions for a device  | Select a device in a region, and click  <b>Switch Region</b> .<br><b>NOTE</b><br>Subregions cannot be switched to other regions.                                                                                                  |
| Import a device              | Click  <b>Import PE Device</b> .                                                                                                                                                                                                    |
| Delete a subregion or device | Select a subregion or device, and click  <b>Delete</b> .                                                                                                                                                                          |
| View region information      | Select a record in the <b>Sub Region/PE Name</b> column, and view subregion details.                                                                                                                                                                                                                                 |

#### 10.3.4.4 Managing Alarms

This topic describes how to monitor L3VPN alarms to understand L3VPN service operating status in a timely manner and ensure normal running of L3VPN services.

#### Prerequisites

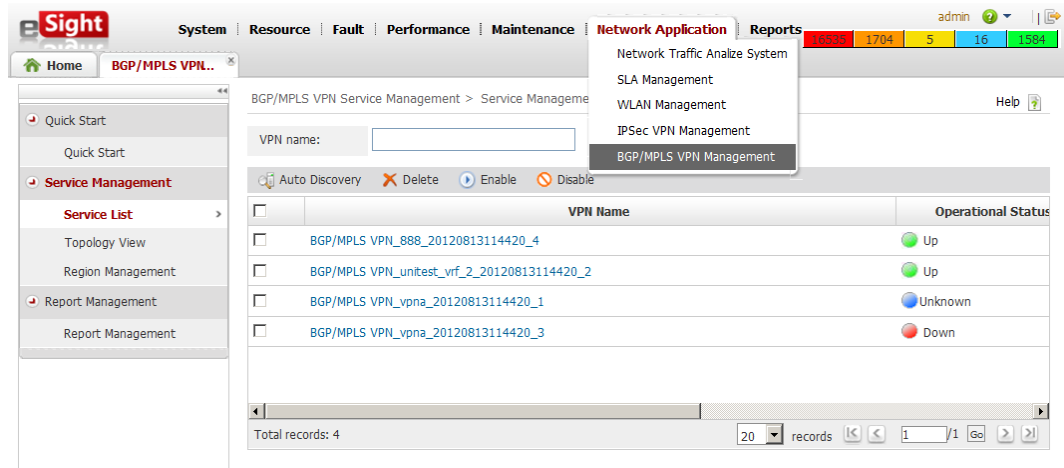
L3VPN services have been discovered to eSight using the automatic discovery function.

#### Context

L3VPN alarms are generated by both devices and L3VPN services. L3VPN alarms are of the following types: alarms indicating status of L3VPN service interfaces on PEs or CEs, alarms indicating VRF status, performance counter alarms for L3VPN services, device offline alarms, and L3VPN service SLA alarms.

#### Procedure

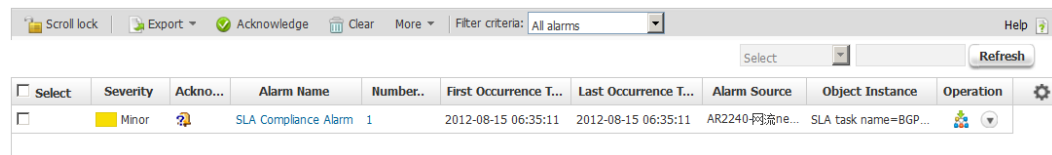
**Step 1** Choose **Network Application > BGP/MPLS VPN Management**.

**Figure 10-124** BGP/MPLS VPN management

**Step 2** In the navigation tree, choose **Service Management** > **Service List**.

**Step 3** View L3VPN alarms.

- In the navigation tree, choose **Service Management** > **Service List**. Select an L3VPN record, click and choose **View alarms**. Current L3VPN alarms are displayed on the **VPN Alarm** page.

**Figure 10-125** BGP/MPLS VPN alarm

**Step 4** View the highest L3VPN alarm severity in either of the following ways:

- In the navigation tree, choose **Service Management** > **Service List**. Then view the highest alarm severity in the **Alarm Severity** column.
- In the navigation tree, choose **Service Management** > **Topology View** to access the service topology of the entire network. When an L3VPN alarm is generated, the matching L3VPN service is enclosed in a box. The box color indicates the highest severity of L3VPN alarms, as shown in [Figure 10-126](#).

**Figure 10-126** Highest L3VPN alarm severity

#### NOTE

The box color indicates the alarm severity. The red color indicates critical alarms. The orange color indicates major alarms. The yellow color indicates minor alarms. The blue color indicates warnings.

----End

### 10.3.4.5 Managing Performance

This topic describes how to view L3VPN service performance history and tendency.

#### Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

#### Context

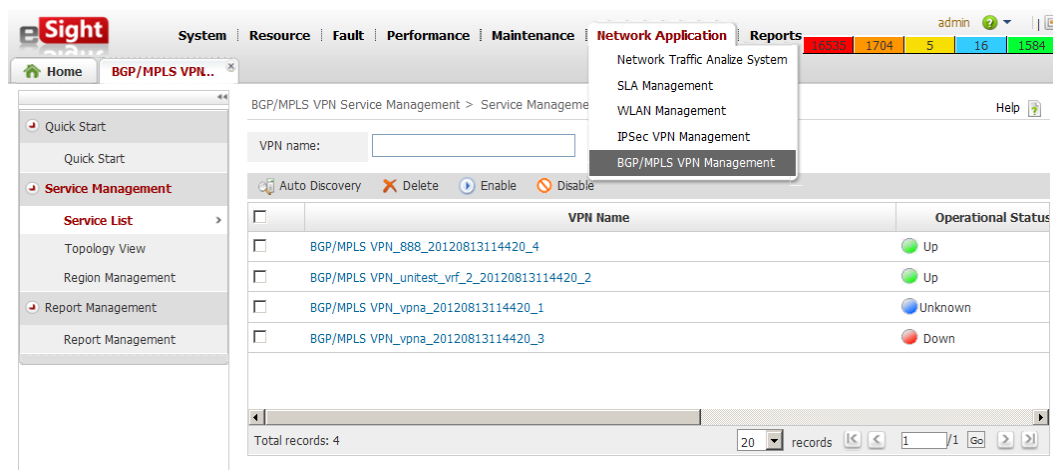
By default, eSight collects the following counters for L3VPN services that are discovered automatically:

- Interface inbound traffic
- Interface outbound traffic
- Number of received bytes on VRF
- Number of sent bytes on VRF
- VRF byte receiving rate
- VRF byte sending rate
- Number of VRF active routes
- Number of VRF routes
- VRF active route percentage

#### Procedure

**Step 1** Choose **Network Application** > **BGP/MPLS VPN Management**.

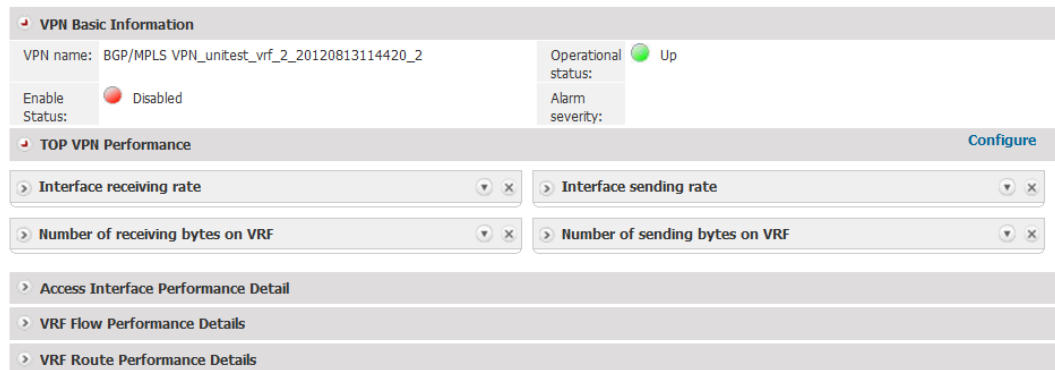
**Figure 10-127** BGP/MPLS VPN management



**Step 2** Open the **Performance counter** page in either of the following ways:

- Open the **Performance counter** page through the **Resource Management** entry.
  1. In the navigation tree, choose **Service Management** > **Service List**.

2. In the L3VPN service list, select an L3VPN service, and click  in the **Operation** column.
- Open the **Performance counter** page through the **Topology View** entry.
1. In the navigation tree, choose **Service Management** > **Topology View**.
2. In the L3VPN service topology of the entire network, select an L3VPN service, right click, and choose **Performance**.

**Figure 10-128** Performance**NOTE**

L3VPN service performance includes interface performance and VRF performance. If the default performance counters cannot meet your requirements, customize performance counters using the performance management function.

Table 10-19 lists measurement objects and counter groups that L3VPN services support.

**Table 10-19** Measurement objects and counter groups that L3VPN services support

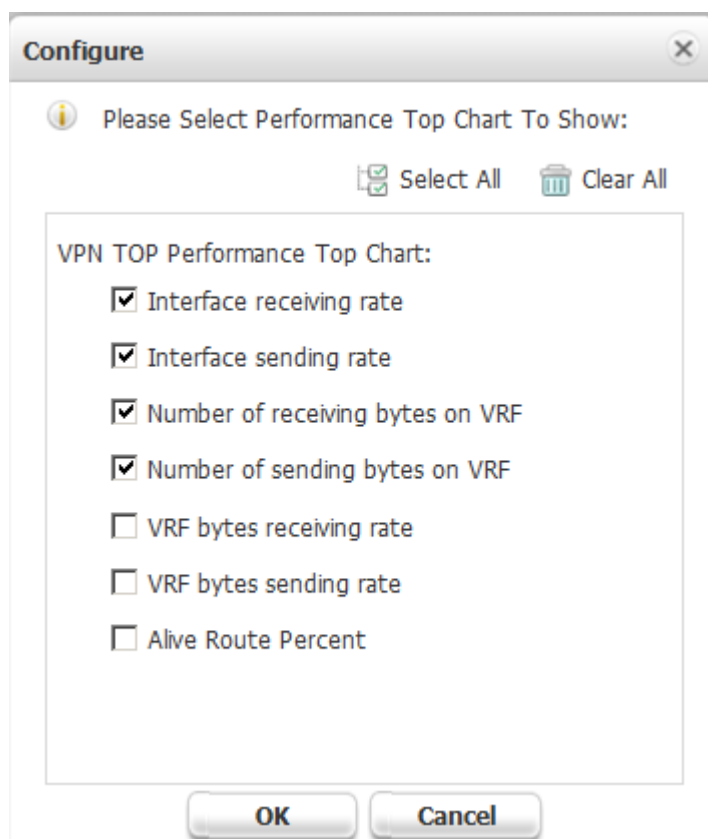
| Measurement Object | Counter                                                                               |
|--------------------|---------------------------------------------------------------------------------------|
| Interface          | Interface Advanced Statistics, Interface Traffic Statistics, and Interface Statistics |
| VRF                | L3VPN base statistics                                                                 |
|                    | VRF Route Number Stat                                                                 |

**Step 3** On the **Performance counter** page, view performance history.

1. Set **Time period**, click **OK**, and view performance history in the specified time period.
2. In the **TOP VPN Performance** area, click **Configure**, and select L3VPN top performance charts to display.



**Figure 10-129** Configure



3. In the **Access Interface Performance Detail**, **VRF Flow Performance Details**, or **VRF Route Performance Details** area, select a VRF, click , and view L3VPN performance details.

----End

### 10.3.4.6 Managing Reports

This topic describes how to view L3VPN report data.

#### Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

#### Context

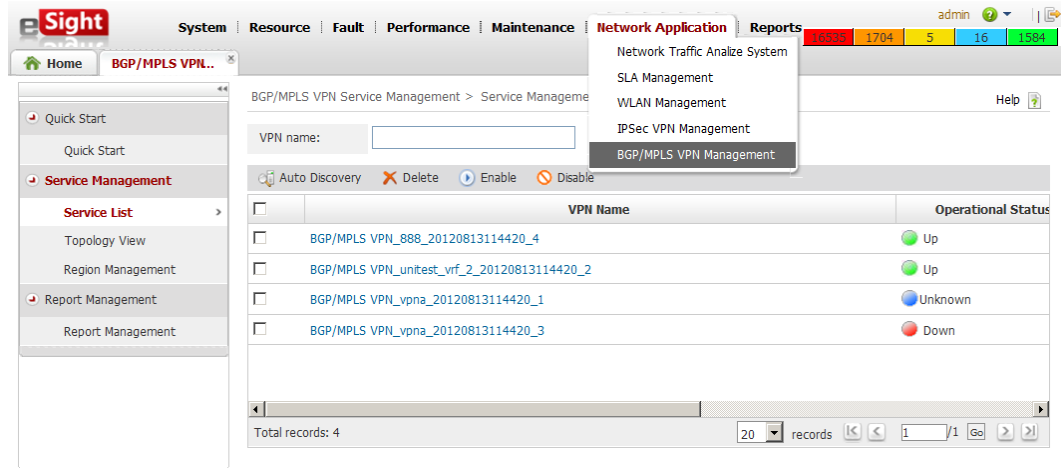
By default, eSight creates the following report tasks for L3VPN services that are discovered automatically:

- Interface traffic performance report
- Service VRF report
- VRF traffic report

## Procedure

**Step 1** Choose **Network Application** > **BGP/MPLS VPN Management**.

**Figure 10-130** BGP/MPLS VPN management



**Step 2** In the navigation tree, choose **Report Management** > **Report Management**.

**Figure 10-131** Report management

| VPN Name                                | Interface Traffic Performance Report | Service VRF Report | VRF Traffic Statistic Report |
|-----------------------------------------|--------------------------------------|--------------------|------------------------------|
| BGP/MPLS VPN_DC-rnd_20120406095418_1    |                                      |                    |                              |
| BGP/MPLS VPN_StarWars_2012032311373...  |                                      |                    |                              |
| BGP/MPLS VPN_TheLordoftheRings_20120... |                                      |                    |                              |
| BGP/MPLS VPN_auto_20120326091822_1      |                                      |                    |                              |
| BGP/MPLS VPN_nicy_20120406095418_2      |                                      |                    |                              |
| BGP/MPLS VPN_test1_20120406095418_3     |                                      |                    |                              |
| BGP/MPLS VPN_vpna_20120323113735_1      |                                      |                    |                              |

**Step 3** View the interface traffic performance report.

1. Select an L3VPN service, and click in the **Interface Traffic Performance Report** column.  
The **Statistics Time Segment** page is displayed.
2. Set **Start Time** and **End Time**, and click **OK**.  
The interface traffic performance report in the selected time segment is displayed on the **Interface Traffic Performance Report** page.

**Step 4** View the service VRF report.

1. Select an L3VPN service, and click in the **Service VRF Report** column.  
The **Statistics Time Segment** page is displayed.
2. Set **Start Time** and **End Time**, and click **OK**.

The service VRF report in the selected time segment is displayed on the **VRF Statistic Report** page.

**Step 5** View the VRF traffic report.

1. Select an L3VPN service, and click  in the **VRF Traffic Statistic Report** column. The **Statistics Time Segment** page is displayed.
2. Set **Start Time** and **End Time**, and click **OK**.  
The VRF traffic report in the selected time segment is displayed on the **VRF Traffic Statistic Report** page.

----End

### 10.3.4.7 Viewing L3VPN SLA Data

This topic describes how to view L3VPN SLA data.

#### Prerequisites

- eSight has been installed and the SLA component has been started.
- L3VPN services have been discovered to eSight using the automatic discovery function.
- SLA tasks have been started. (SLA tasks are stopped by default.)

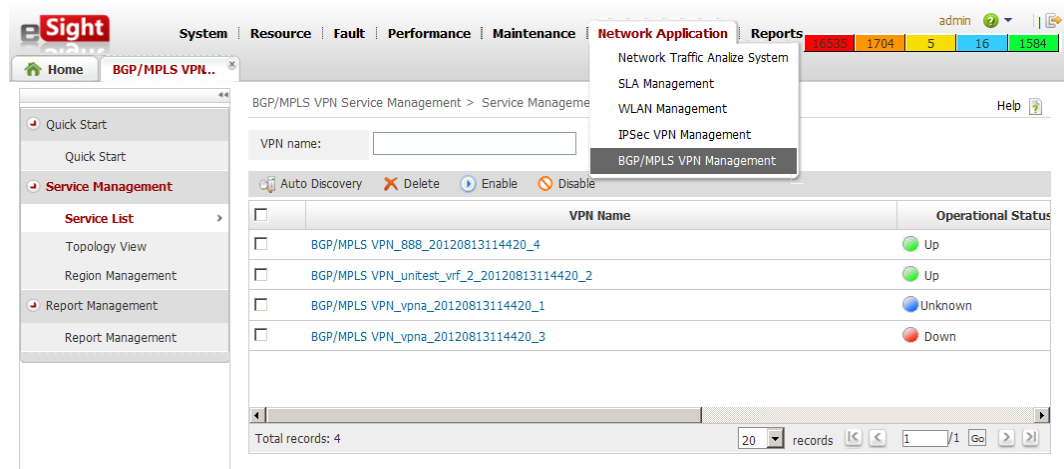
#### Context

- eSight automatically creates SLA tasks for L3VPN services that are discovered automatically and have PE-PE links or PE-CE links.
- The SLA function is available only to Huawei source devices.

#### Procedure

**Step 1** Choose **Network Application > BGP/MPLS VPN Management**.

**Figure 10-132** BGP/MPLS VPN management



**Step 2** In the navigation tree, choose **Service Management** > **Service List**. Select an L3VPN service, click  and choose  **SLA**.

**Figure 10-133** Service list

| <input type="checkbox"/> | VPN Name                                        | Operational Status                                                                               | Enable Status                                                                              | Alarm Severity | Operation                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | BGP/MPLS VPN_DC-rnd_20120406095418_1            |  Partially Down |  Enabled  |                |     |
| <input type="checkbox"/> | BGP/MPLS VPN_StarWars_20120323113735_3          |  Up             |  Enabled  | Minor          |     |
| <input type="checkbox"/> | BGP/MPLS VPN_TheLordoftheRings_2012032311373... |  Up             |  Enabled  | Minor          |     |
| <input type="checkbox"/> | BGP/MPLS VPN_auto_20120326091822_1              |  Up             |  Enabled  |                |     |
| <input type="checkbox"/> | BGP/MPLS VPN_ncy_20120406095418_2               |  Down           |  Disabled | Major          |     |

**Step 3** On the **SLA** page that is displayed, view **TOP Service Quality Compliance** and **SLA service list**.

**Figure 10-134** SLA

| Lowest Service Quality Compliance                                                                                                                                                  |                                                                                              |                    |                       |               |                     |                                                                                               |                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------------|-----------------------|---------------|---------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SLA service list                                                                                                                                                                   |                                                                                              |                    |                       |               |                     |                                                                                               |                                                                                                                                                                             |
| Task:                                                                                                                                                                              |                                                                                              |                    | Source device:        |               |                     |                                                                                               |                                                                                                                                                                             |
| Task Status:                                                                                                                                                                       | All                                                                                          |                    | Daily compliance (%): |               |                     | Search                                                                                        |                                                                                                                                                                             |
|  Start  Stop |                                                                                              |                    |                       |               |                     |                                                                                               |                                                                                                                                                                             |
| <input type="checkbox"/>                                                                                                                                                           | Status                                                                                       | Task               | Service Name          | Source Device | Destination IP A... | Daily Compliance                                                                              | Operation                                                                                                                                                                   |
| <input type="checkbox"/>                                                                                                                                                           |  Start... | BGP/MPLS VPN_vp... | ICMP Echo             | AR2240        | 8.8.8.9             | 100.00%  |   |
| <input type="checkbox"/>                                                                                                                                                           |  Start... | BGP/MPLS VPN_vp... | ICMP Echo             | AR2240_221_1  | 7.7.7.9             | 100.00%  |   |

----End

## 10.3.5 Diagnosing Service Faults

When you want to understand L3VPN operating status or when an L3VPN service generates an alarm, you can use the BGP/MPLS VPN fault diagnosis function to check service link connectivity in L3VPN and locate faults.

### Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

### Context

- eSight allows you to diagnose BGP/MPLS VPN services in either of the following modes based on the site scenario: by network segment (PE-PE and PE-CE) and by network layer. [Table 10-20](#) lists the scenarios for using different L3VPN diagnosis options or tools.

**Table 10-20** Scenarios for using different L3VPN diagnosis options or tools

| Diagnosis Option/Tool | Function                                                                                                                          | Application Scenario                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| VRF Ping              | Check service link connectivity in L3VPN.                                                                                         | Check private network connectivity in L3VPN.                                                                                 |
| LSP Ping              | Check label switched path (LSP) connectivity.                                                                                     | Check LSP connectivity in L3VPN.                                                                                             |
| ICMP Ping             | Check connectivity at the network layer. Understand network conditions based on information such as packet loss rate and latency. | Generally ICMP ping is used to check public or private network connectivity after faults at the service layer are rectified. |

- In addition to the previous diagnosis tools, BGP/MPLS VPN services also support VRF traceroute, LSP traceroute, and ICMP traceroute. Traceroute application scenarios are similar to ping application scenarios. Traceroute can obtain information (such as packet loss rate and latency) about nodes between source and destination to locate faults. Ping can only check connectivity between source and destination. Therefore, use ping to diagnose connectivity between source and destination first. If a connectivity fault occurs, use traceroute to locate the fault.
- Different link types support different diagnosis options or tools. In [Table 10-21](#), **Y** indicates that a link supports a diagnosis option or tool.

**Table 10-21** Mapping between diagnosis options/tools and link types

| Diagnosis Option/Tool | Link Type |       |              |       |
|-----------------------|-----------|-------|--------------|-------|
|                       | PE-PE     | CE-CE | PE-Remote CE | PE-CE |
| ICMP Ping             | Y         | Y     | -            | -     |
| VRF Ping              | Y         | -     | Y            | Y     |
| LSP Ping              | Y         | -     | -            | -     |
| ICMP TraceRoute       | Y         | Y     | -            | -     |
| VRF TraceRoute        | Y         | -     | Y            | Y     |
| LSP TraceRoute        | Y         | -     | -            | -     |
| Public route          | Y         | -     | -            | -     |
| Private route         | Y         | -     | Y            | Y     |
| BGP VPN V4 peer       | Y         | -     | -            | -     |
| VPN V4 route          | Y         | -     | -            | -     |

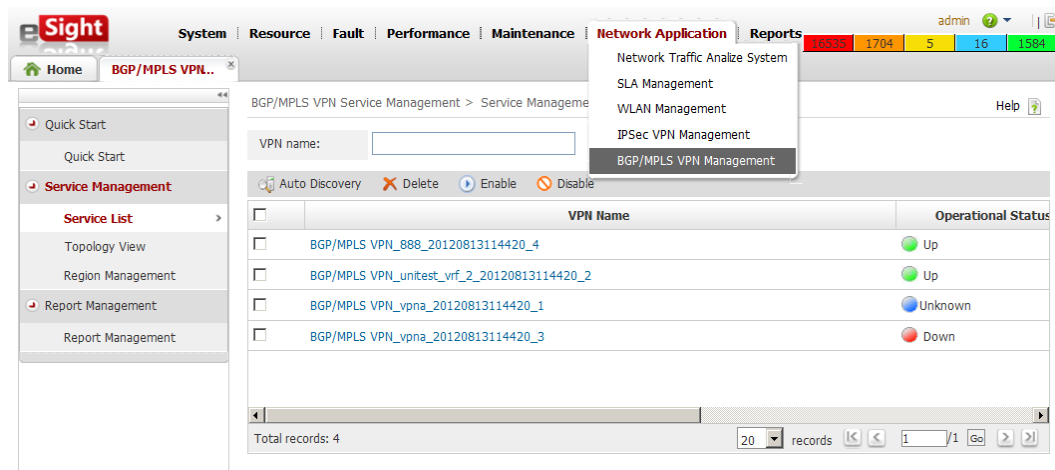
| Diagnosis Option/Tool | Link Type |       |              |       |
|-----------------------|-----------|-------|--------------|-------|
|                       | PE-PE     | CE-CE | PE-Remote CE | PE-CE |
| VRF FIB Information   | Y         | -     | Y            | Y     |
| LSP information       | Y         | -     | -            | -     |

- The BGP/MPLS VPN fault diagnosis function is available only to Huawei devices.

## Procedure

**Step 1** Choose **Network Application > BGP/MPLS VPN Management**.

**Figure 10-135** BGP/MPLS VPN management



**Step 2** In the navigation tree, choose **Service Management > Service List**.

**Step 3** Select an L3VPN record, and click .

The **Quick Diagnosis** window is displayed.

**Step 4** In the **Diagnosis object** area, set **Link type** and **Search criteria**, and click **Search**.

Diagnosis objects that meet requirements are displayed in the search result area.

**Figure 10-136** Diagnosis object

**Diagnosis object:**

|                         |       |                     |  |
|-------------------------|-------|---------------------|--|
| Link type:              | PE-CE | Source device:      |  |
| Source IP address:      |       | Destination device: |  |
| Destination IP address: |       |                     |  |

**Search**

| <input checked="" type="checkbox"/> | Link Type | Source Device | Source IP Address | Destination Device | Destination IP Address |
|-------------------------------------|-----------|---------------|-------------------|--------------------|------------------------|
| <input checked="" type="checkbox"/> | PE-CE     | S7703_15      | 192.1.1.1         | S7712_201          | 192.1.1.2              |

**Step 5** Select a link that you want to diagnose.

**Step 6** Select diagnosis options or tools in the **Diagnosis option/tool** area.

Click **Advanced**, and set diagnosis option parameters.

**Figure 10-137** Diagnosis option/tool

**Diagnosis option/tool:**

|                      |                                               |                                                           |                                                           |
|----------------------|-----------------------------------------------|-----------------------------------------------------------|-----------------------------------------------------------|
| Ping:                | <input type="checkbox"/> ICMP <b>Advanced</b> | <input checked="" type="checkbox"/> VRF F <b>Advanced</b> | <input checked="" type="checkbox"/> LSP F <b>Advanced</b> |
| Collect information: | <input type="checkbox"/> Public route         | <input checked="" type="checkbox"/> Private route         | <input checked="" type="checkbox"/> BGP VPN V4 peer       |
|                      | <input type="checkbox"/> VPN V4 route         | <input checked="" type="checkbox"/> VRF FIB information   | <input type="checkbox"/> LSP information                  |
| Traceroute:          | <input type="checkbox"/> ICMP <b>Advanced</b> | <input type="checkbox"/> VRF T <b>Advanced</b>            | <input type="checkbox"/> LSP T <b>Advanced</b>            |

**Quick Diagnosis**

**Step 7** Click **Quick Diagnosis**. Then view information on the **Ping result**, **Collected Information**, or **Trace result** tab page in the **Diagnosis result** area based on diagnosis options supported by a specific link type.

----End

## 10.3.6 Example: Typical BGP/MPLS VPN Management Operations

This topic describes how to discover the Hub-Spoke VPN service automatically and view the topology and details.

### Prerequisites

- You are an operator or a superior eSight user and have the device management permission.
- The network and services have been deployed on devices.
- Devices have been added to eSight and Telnet parameters have been set.

## Scenario

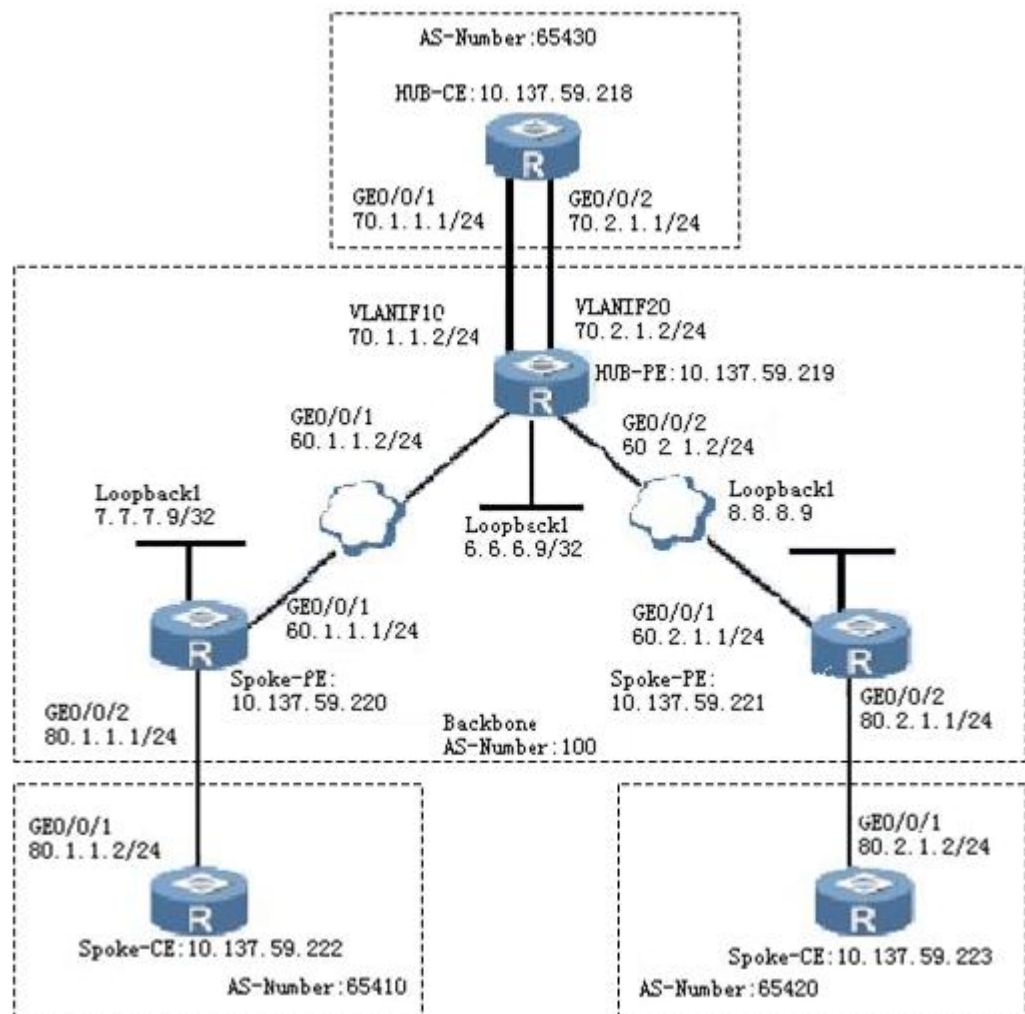
A large-scale enterprise has many branches and service systems such as the network management system (NMS), Business and Operation Support System (BOSS), and Office Automation (OA). The service systems are maintained and managed by different departments. The servers and core devices of all service systems are located in headquarters. The entire enterprise uses an MPLS backbone network to bear all internal services. Different service systems are deployed on different VPNs to implement communication and isolation between each other.

## Network

PEs are deployed at both branches and headquarters. The PE (10.137.59.220) at branch 1 and PE (10.137.59.221) at branch 2 are used to connect the service system in their respective branches. The PE (10.137.59.219) at the headquarters is used to connect servers of different service systems.

Figure 10-138 shows Configuration network.

**Figure 10-138** Configuration network





## Data Plan

Table 10-22 lists the Data Plan in detail.

**Table 10-22** Data Plan

| NE Name      | NE Type | IP Address    | Role     | Location     |
|--------------|---------|---------------|----------|--------------|
| AR3260_218_1 | AR3260  | 10.137.59.218 | Hub-CE   | Headquarters |
| AR2240_219_1 | AR2240  | 10.137.59.219 | Hub-PE   | Headquarters |
| AR2240_220_1 | AR2240  | 10.137.59.220 | Spoke-PE | Branch       |
| AR2240_221_1 | AR2240  | 10.137.59.221 | Spoke-PE | Branch       |
| AR3260_222_1 | AR3260  | 10.137.59.222 | Spoke-CE | Branch       |
| AR3260_223_1 | AR3260  | 10.137.59.223 | Spoke-CE | Branch       |

## Procedure

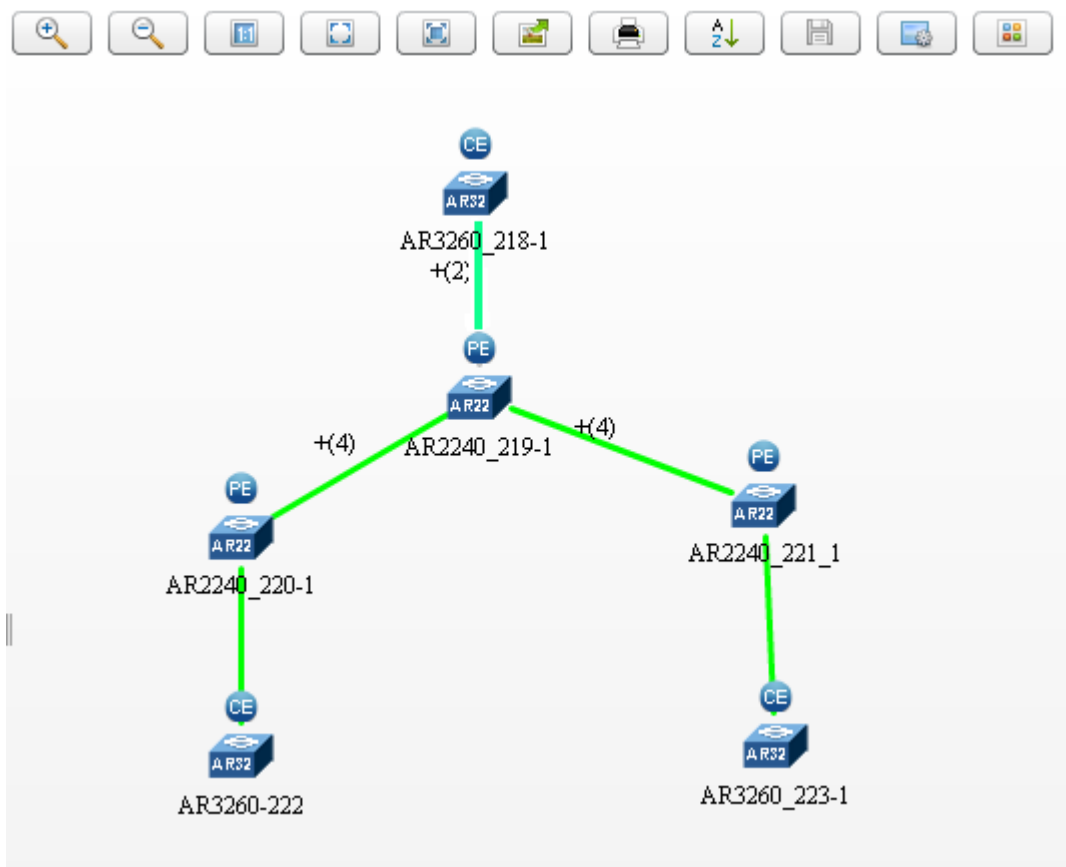
**Step 1** Discover VPN services automatically.

1. Choose **Network Application** > **BGP/MPLS VPN Management**.
2. In the navigation tree, choose **Service Management** > **Service List**, and click **Auto Discover**.
3. Set **Discovery policy** to **Discover by VRF connection**.
4. Click **Select Device** next to **Discovery range**. In the **Select Device** dialog box that is displayed, select devices whose IP addresses belong to the IP address segment (10.137.59.218-10.137.59.223), and click **OK**.
5. Click **Discover**. The discovered VPN services are displayed in the lower table.
6. In the **Discovery result** area, click **Change Name** in the **Operation** column, and change the VPN name.

**Step 2** View the VPN topology.

1. In the **Discovery result** area, click **Topology View** in the **Operation** column. The VPN topology of the entire network is displayed.
2. On the VPN topology page of the entire network, double-click a VPN icon to access the topology page of the specified VPN.
  - Blue tips above devices indicate device roles, such as  and .
  - Move the pointer to a device or link to view the device or link information.
  - Click , and change device positions in the topology view by different sorting modes. Figure 10-139 shows a VPN service topology view.

**Figure 10-139** VPN service topology view



**Step 3** View detailed information about a VPN service.

1. In the navigation tree, choose **Service Management** > **Service List**.
2. Click a VPN name to view its detailed information, including **CE Management**, **Service Link**, **VRF Instance**, and **Route Configuration**.

----End

## 10.4 SLA Management

eSight provides the service level agreement (SLA) monitoring and management functions, including SLA Overview, SLA services, SLA tasks, and quick diagnosis.

### 10.4.1 What Is SLA?

The service level agreement (SLA) is a service agreement between a service provider and a customer to ensure the service performance and reliability under specified costs.

#### 10.4.1.1 SLA Terms

This topic describes SLA terms.

**Table 10-23** SLA terms

| Term        | Description                                                                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SLA service | An SLA service is the integration of common services, service quality, and test instances. Common services refer to voice and video applications. Test instances refer to diagnosis tests such as UDP Echo and FTP tests. Service quality refers to the thresholds configured for test instance counters. |
| SLA task    | An SLA task is a test instance for monitoring network links and the service quality on these network links.                                                                                                                                                                                               |
| Rating      | A rating indicates service quality standards. A higher service rating indicates higher requirements on service counters such as the packet loss rate, latency, and jitter.                                                                                                                                |
| Compliance  | The compliance indicates the ratio of the actual network quality to the expected quality, in percentage.                                                                                                                                                                                                  |

### 10.4.1.2 SLA Functions

The service level agreement (SLA) is a network performance diagnosis tool. It sends packets between multiple NEs or links to evaluate the network performance.

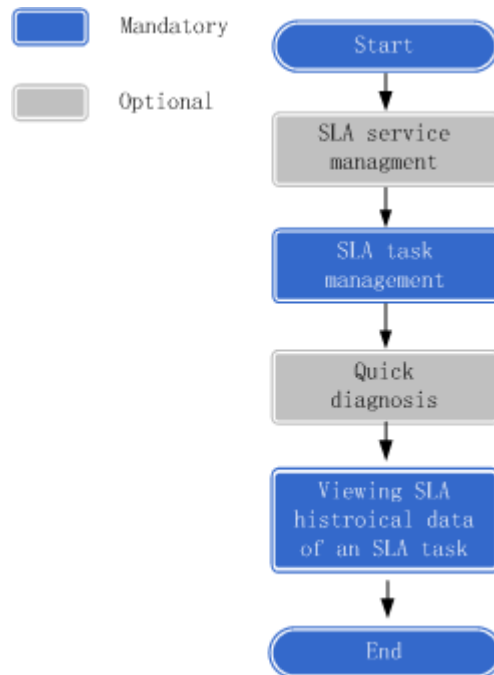
The SLA provides the following advantages:

- Instructs users to execute network applications based on the evaluation result.
- Sends notifications to users when faults occur on the network.
- Evaluates the network performance continuously or periodically.
- Checks and confirms the service quality, implementing differentiated services.

The SLA has the following functions:

- Network performance evaluation: The SLA provides 10 test instances (such as UDP Echo, TCP Connect, HTTP, DNS, and ICMP Jitter), covering more than a hundred counters such as latency, jitter, and packet loss rate.
- Compliance: The SLA calculates the compliance based on the configured counters, thresholds, and weights, and displays the result in graphics on the GUI.
- Threshold alarm: Users can set thresholds for network performance counters based on the actual network conditions. If a performance counter exceeds the threshold, an alarm is generated.
- Compliance alarm: If the conformity is lower than the expectation, an alarm is generated.
- Periodical monitoring: The SLA can periodically monitor a network on specified dates.
- Measurement result query: Users can query the counter measurement result in any periods and export the measurement result.

Overview of SLA management operations:

**Figure 10-140** Overview of SLA management operations

- Managing SLA services: You can use SLA services to define the test methods and service quality standards for services. SLA provides more than 10 predefined services. You can also customize services.
- Managing SLA tasks: Users can select a link and test services on the link to calculate the SLA compliance and trigger alarms when the alarm threshold is reached. This helps to evaluate the link network quality.
- Quick diagnosis: Users can check links monitored by SLA tasks.
- Viewing historical task data: You can view a task's compliance graph and the graph of the comparison between a counter's threshold and actual values in a specified period.

### 10.4.1.3 SLA Default Settings and Device Configurations

Before using the SLA component, you must learn about the SLA default settings and the Device Configurations to ensure smooth operations.

#### Default Settings

eSight provides default services and service ratings for users to select. See [Table 10-24](#).

**Table 10-24** Typical service and service rating

| Typical Service   | Test Instance                         | Rating |
|-------------------|---------------------------------------|--------|
| Video             | UDP Jitter, ICMP Jitter, and UDP Echo | 4-star |
| Audio             | UDP Jitter                            | 5-star |
| Data              | TCP Connect                           | 3-star |
| Web page browsing | HTTP                                  | 4-star |

| Typical Service                                 | Test Instance              | Rating |
|-------------------------------------------------|----------------------------|--------|
| FTP application                                 | FTP, ICMP Echo             | 4-star |
| Network managements                             | SNMP                       | 4-star |
| Real-time application                           | UDP Jitter and ICMP Jitter | 4-star |
| Portal                                          | HTTP, DNS, and TCP Connect | 4-star |
| Client-server traffic and database transactions | TCP Connect and ICMP Echo  | 4-star |
| E-commerce                                      | UDP Echo and ICMP Echo     | 4-star |

## Specifications Calculation Supported by the eSight

- Latency: interval for receiving a packets minus the interval for sending the packet.
- Jitter: interval for receiving two consecutive packets minus the interval for sending them.
- Packet loss ratio = (Total number of sent packets - Total number of received packets)/Total number of packets x 100%



### NOTE

TCP and FTP test instances are used as examples. Packet loss ratio = (Total number of probes - Number of successful probes)/Total number of probes x 100%

## Test Instances and Counters Supported by the eSight

Table 10-25 describes test instances and counters supported by the eSight.

**Table 10-25** Test instances and counters supported by the eSight

| Counter                         | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|---------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
| Packet loss rate                | Y         | Y           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| Max. RTD (ms)                   | Y         | Y           | Y        | Y          | Y           | Y    | Y   | Y    | N    | N   |
| Average RTD (ms)                | Y         | Y           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| Average jitter                  | N         | Y           | N        | Y          | N           | N    | N   | N    | N    | N   |
| Number of timeouts              | Y         | Y           | Y        | Y          | Y           | Y    | Y   | Y    | N    | Y   |
| Time of Getting IP Address (ms) | N         | N           | N        | N          | N           | N    | N   | Y    | N    | N   |
| Transfer Speed (M/s)            | N         | N           | N        | N          | N           | N    | N   | N    | N    | Y   |
| Max.                            | N         | Y           | N        | Y          | N           | N    | N   | N    | N    | N   |

| Counter                                                   | IC<br>MP<br>Echo | IC<br>MP<br>Jitter | UD<br>P<br>Echo | UD<br>P<br>Jitter | TCP<br>Connect | SN<br>MP | DN<br>S | DH<br>CP | HT<br>TP | FTP |
|-----------------------------------------------------------|------------------|--------------------|-----------------|-------------------|----------------|----------|---------|----------|----------|-----|
| unidirectional delay from source to destination (ms)      |                  |                    |                 |                   |                |          |         |          |          |     |
| Max. unidirectional delay from destination to source (ms) | N                | Y                  | N               | Y                 | N              | N        | N       | N        | N        | N   |
| Average jitter from source to destination (ms)            | N                | Y                  | N               | Y                 | N              | N        | N       | N        | N        | N   |
| Average jitter from destination to source (ms)            | N                | Y                  | N               | Y                 | N              | N        | N       | N        | N        | N   |
| MOS value                                                 | N                | N                  | N               | Y                 | N              | N        | N       | N        | N        | N   |
| Max. duration for establishing an FTP connection (ms)     | N                | N                  | N               | N                 | N              | N        | N       | N        | N        | Y   |
| Max. duration for FTP data transmission (ms)              | N                | N                  | N               | N                 | N              | N        | N       | N        | N        | Y   |
| Max. duration for FTP probe (ms)                          | N                | N                  | N               | N                 | N              | N        | N       | N        | N        | Y   |
| Number of forced FTP transfer terminations                | N                | N                  | N               | N                 | N              | N        | N       | N        | N        | Y   |
| Number of RTT statistics failures                         | N                | N                  | N               | N                 | N              | N        | Y       | N        | N        | N   |
| Number of packets with incorrect No.                      | N                | N                  | N               | N                 | N              | N        | Y       | N        | N        | N   |
| Number of initialization or resource application failures | N                | N                  | N               | N                 | N              | N        | Y       | N        | N        | Y   |

| Counter                             | IC<br>MP<br>Echo | IC<br>MP<br>Jitter | UD<br>P<br>Echo | UD<br>P<br>Jitter | TCP<br>Con<br>nect | SN<br>MP | DN<br>S | DH<br>CP | HT<br>TP | FTP |
|-------------------------------------|------------------|--------------------|-----------------|-------------------|--------------------|----------|---------|----------|----------|-----|
| Max. HTTP test duration (ms)        | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| Max. HTTP transaction duration (ms) | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| Other HTTP error count              | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| Max. TCP connection RTT (ms)        | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| TCP connection error count          | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| Number of TCP connection timeouts   | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| Max. DNS RTT (ms)                   | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |
| Time of parsing DNS                 | N                | N                  | N               | N                 | N                  | N        | Y       | N        | Y        | N   |
| Number of DNS resolution failures   | N                | N                  | N               | N                 | N                  | N        | N       | N        | Y        | N   |

## Test Instances Supported by Devices

Table 10-26 describes test instances supported by devices.

**Table 10-26** Test instances supported by devices

| Device Type | Device Version                          | IC<br>MP<br>Echo | IC<br>MP<br>Jitter | UD<br>P<br>Echo | UD<br>P<br>Jitter | TCP<br>Con<br>nect | SN<br>MP | DN<br>S | DH<br>CP | HT<br>TP | FTP |
|-------------|-----------------------------------------|------------------|--------------------|-----------------|-------------------|--------------------|----------|---------|----------|----------|-----|
| S2300       | V100 R005 C00, V100 R005 C01, V100 R006 | Y                | N                  | Y               | Y                 | Y                  | Y        | Y       | N        | Y        | Y   |

| Device Type | Device Version                                                                                      | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|-----------------------------------------------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
|             | C00, V100 R006 C01, V200 R001                                                                       |           |             |          |            |             |      |     |      |      |     |
|             | V100 R003 C00, V100 R003 C01                                                                        | Y         | N           | Y        | Y          | Y           | Y    | Y   | N    | Y    | N   |
| S2700       | V100 R005 C01, V100 R006 C00, V100 R006 C01, V200 R001                                              | Y         | N           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S3300       | V100 R003 C00, V100 R003 C01, V100 R005 C00, V100 R005 C01, V100 R006 C00, V100 R006 C01, V200 R001 | Y         | N           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S3700       | V100 R005 C01, V100                                                                                 | Y         | N           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |



| Device Type | Device Version                                                            | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|---------------------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
|             | R006 C00, V100<br>R006 C01, V200<br>R001                                  |           |             |          |            |             |      |     |      |      |     |
| S5300       | V100 R003 C00                                                             | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
|             | V100 R003 C01, V100 R005 C00, V100 R005 C01, V100 R006 C00, V100 R006 C01 | Y         | N           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
|             | V200 R001                                                                 | Y         | Y           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S5700       | V100 R005 C01, V100 R006 C00, V100 R006 C01, V200 R001                    | Y         | N           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S6300       | V100 R006 C00, V100 R006 C01, V200 R001                                   | Y         | Y           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |

| Device Type | Device Version                                               | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|--------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
| S6700       | V100R006C00, V100R006C01, V200R001                           | Y         | Y           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S9300       | V100R003C00, V100R003C01, V100R006C00, V100R006C01, V200R001 | Y         | Y           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S9700       | V200R001                                                     | Y         | Y           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| S7700       | V100R003C01, V100R006C00, V100R006C01, V200R001              | Y         | Y           | Y        | Y          | Y           | Y    | Y   | N    | Y    | Y   |
| NE20        | V200R005C01, V200R005C02, V200R005C03, V200R005C05           | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | N   |

| Device Type | Device Version                                                                                          | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|---------------------------------------------------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
| NE20 E-8    | V200 R003 C00, V200 R003 C01, V200 R005 C00, V200 R005 C01, V200 R005 C02, V200 R005 C03, V200 R005 C05 | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | N   |
| NE20 E-X6   | V600 R003 C00                                                                                           | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| NE40        | V300 R002 C00, V300 R002 C01, V300 R003 C00, V300 R003 C01, V300 R003 C02, V300 R005 C00, V300 R005 C01 | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| NE40        | V300 R001                                                                                               | N         | N           | N        | N          | N           | N    | N   | N    | N    | N   |

| Device Type | Device Version                                                                                                                        | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
| E           | C00                                                                                                                                   |           |             |          |            |             |      |     |      |      |     |
|             | V300 R002 C00, V300 R003 C00, V300 R003 C01, V300 R003 C02                                                                            | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
|             | V300 R006 C00, V300 R006 C01, V600 R001 C00, V600 R001 C01, V600 R003 C00, V600 R003 C01, V600 R003 C02, V600 R003 C03, V600 R003 C05 | Y         | Y           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| NE40 E-4    | V300 R003 C00, V300 R003 C01, V300 R003                                                                                               | N         | N           | N        | N          | N           | N    | N   | N    | N    | N   |

| Device Type | Device Version                                                                            | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|-------------------------------------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
|             | C02                                                                                       |           |             |          |            |             |      |     |      |      |     |
| NE40E-X3    | V300R006C00, V300R006C01                                                                  | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| NE80        | V300R002C00, V300R002C01, V300R003C00, V300R003C01, V300R003C02, V300R005C00, V300R005C01 | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | N   |
| NE80E       | V100R002C00, V300R001C00                                                                  | N         | N           | N        | N          | N           | N    | N   | N    | N    | N   |
|             | V300R002C00                                                                               | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | N   |
|             | V300R003C00, V300R003C01, V300R003C02                                                     | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |

| Device Type | Device Version                                             | ICMP Echo | ICMP Jitter | UDP Echo | UDP Jitter | TCP Connect | SNMP | DNS | DHCP | HTTP | FTP |
|-------------|------------------------------------------------------------|-----------|-------------|----------|------------|-------------|------|-----|------|------|-----|
|             | V300 R006 C00, V300 R006 C01, V600 R001 C00, V600 R001 C01 | Y         | Y           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| AR1200      | V200 R001 C00, V200 R001 C01, V200 R002 C00                | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| AR2200      | V200 R001 C00, V200 R001 C01, V200 R002 C00                | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| AR3200      | V200 R001 C00, V200 R001 C01, V200 R002 C00                | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| AR150       | V200 R002 C00                                              | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |
| AR200       | V200 R002 C00                                              | Y         | N           | Y        | Y          | Y           | Y    | Y   | Y    | Y    | Y   |

## Device Configuration

To perform test instances in eSight, you must perform the following settings listed in [Table 10-27](#).

**Table 10-27** Device configuration

| Test Instance | Device Configuration Requirements                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP ECHO     | The source and destination devices can ping successfully.                                                                                                                                                                                                                                                                                                     |
| ICMP JITTER   | The source and destination devices can ping successfully.                                                                                                                                                                                                                                                                                                     |
| UDP Echo      | <p>The UDP service must be enabled on the destination device.</p> <p>Run the following commands to start the UDP service:</p> <pre>&lt;Huawei&gt; system-view<br/>[Huawei] nqa-server udpecho 10.137.61.39 33434</pre> <p>In the command, <b>10.137.61.39</b> is the destination device IP address and <b>33434</b> is the UDP port number.</p>               |
| UDP Jitter    | <p>The UDP service must be enabled on the destination device.</p> <p>Run the following commands to start the UDP service:</p> <pre>&lt;Huawei&gt; system-view<br/>[Huawei] nqa-server udpecho 10.137.61.39 33434</pre> <p>In the command, <b>10.137.61.39</b> is the destination device IP address and <b>33434</b> is the UDP port number.</p>               |
| TCP Connect   | <p>The TCP service must be enabled on the destination device.</p> <p>Run the following commands to start the TCP service:</p> <pre>&lt;Huawei&gt; system-view<br/>[Huawei] nqa-server tcpconnect 10.137.61.39 33433</pre> <p>In the command, <b>10.137.61.39</b> is the destination device IP address and <b>33433</b> is the TCP port number.</p>            |
| SNMP          | None.                                                                                                                                                                                                                                                                                                                                                         |
| DNS           | <p>The DNS service must be enabled on the source device.</p> <p>Run the following commands to start the DNS service:</p> <pre>&lt;Huawei&gt; system-view<br/>[Huawei] dns resolve<br/>[Huawei] dns server 10.137.61.75<br/>[Huawei] dns domain net<br/>[Huawei] dns domain com</pre> <p>In the command, <b>10.137.61.75</b> is the DNS server IP address.</p> |
| DHCP          | <p>The DHCP server function must be enabled on the VLANIF interface of the destination device.</p> <p>Run the following command to enable the DHCP server function:</p>                                                                                                                                                                                       |

| Test Instance | Device Configuration Requirements                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <p>&lt;Huawei&gt; <b>system-view</b></p> <p>[Huawei] <b>interface Vlanif20</b></p> <p>[Huawei-Vlanif20] <b>ip address 70.2.1.2 255.255.255.0</b></p> <p>[Huawei-Vlanif20] <b>dhcp select interface</b></p> <p>In the commands, <b>Vlanif20</b> is the VLANIF interface, <b>70.2.1.2</b> is the DHCP server IP address, <b>225.255.255.0</b> is the subnet mask of the IP address.</p>                                                                                                                                                                                                                                                                                                          |
| HTTP          | None.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| FTP           | <p>The FTP service must be enabled on the destination device.</p> <p>Run the following commands to start the FTP service:</p> <p>&lt;Huawei&gt; <b>system-view</b></p> <p>[Huawei] <b>ftp server enable</b></p> <p>[Huawei] <b>ftp timeout 30</b></p> <p>[Huawei] <b>aaa</b></p> <p>[Huawei-aaa] <b>dns domain com</b></p> <p>[Huawei-aaa] <b>local-user admin admin password simple admin</b></p> <p>[Huawei-aaa] <b>local-user admin service-type ftp</b></p> <p>[Huawei-aaa] <b>local-user admin ftp-directory sd1:/</b></p> <p>[Huawei-aaa] <b>q</b></p> <p><b>sd1:/</b> specifies the working directory that the local user can access using the <b>dir</b> command in the user view.</p> |

## 10.4.2 Overview of SLA Management Operations

This topic describes the SLA management operations.

Figure 10-141 shows the overview of SLA management operations. For more details, click the operation in the overview.

**Figure 10-141** Overview of SLA management operations

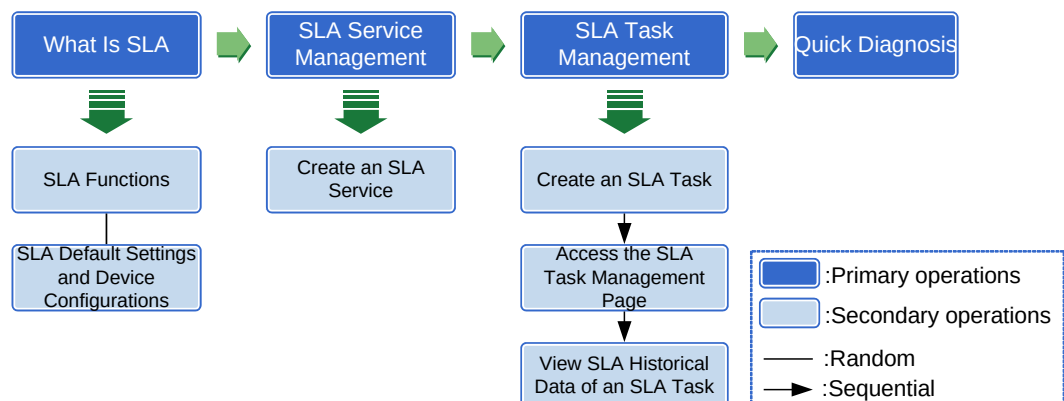




Table 10-28 describes the SLA management operations.

**Table 10-28** SLA management operations

| Operation                                                               | Description                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">10.4.1.2 SLA Functions</a>                                  | The service level agreement (SLA) is a network performance diagnosis tool. It sends packets between multiple NEs or links to evaluate the network performance.                                                                                                                                            |
| <a href="#">10.4.1.3 SLA Default Settings and Device Configurations</a> | Before using the SLA component, you must master the SLA terms and default settings to ensure smooth operations.                                                                                                                                                                                           |
| <a href="#">10.4.3.1 Creating an SLA Service</a>                        | An SLA service is the integration of common services, service quality, and test instances. Common services refer to voice and video applications. Test instances refer to diagnosis tests such as UDP Echo and FTP tests. Service quality refers to the thresholds configured for test instance counters. |
| <a href="#">10.4.3.2 Creating an SLA Task</a>                           | An SLA task is a test instance used to check the network link quality.                                                                                                                                                                                                                                    |
| <a href="#">10.4.3.3 Quick Diagnosis</a>                                | The quick diagnosis function is used to check links monitored by SLA tasks.                                                                                                                                                                                                                               |
| <a href="#">10.4.4.1 Accessing the SLA Task Management Page</a>         | This topic describes how to access the SLA Task Management page to monitor SLA tasks.                                                                                                                                                                                                                     |
| <a href="#">10.4.4.2 Viewing SLA Historical Data of an SLA Task</a>     | The SLA task details page displays the counter value graph in a specified period.                                                                                                                                                                                                                         |

## 10.4.3 Configuring SLA Tasks

This topic describes how to configure SLA tasks.

### 10.4.3.1 Creating an SLA Service

An SLA service is the integration of common services, service quality, and test instances. Common services refer to voice and video applications. Test instances refer to diagnosis tests such as UDP Echo and FTP tests. Service quality refers to the thresholds configured for test instance counters.

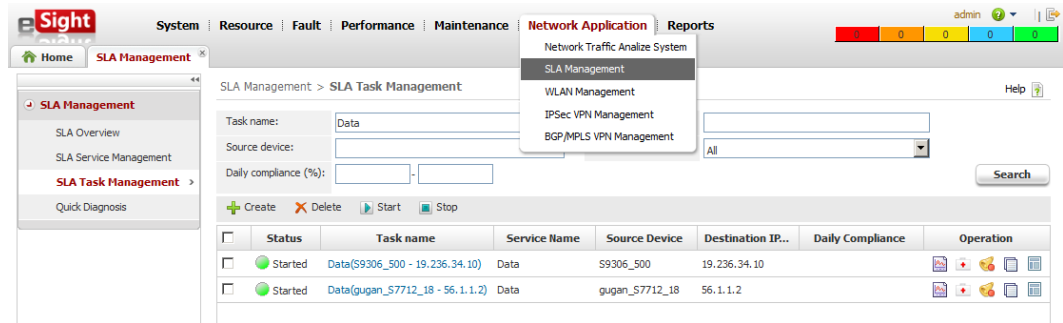
#### Context

SLA provides more than 10 predefined services. If the predefined services cannot meet your requirements, you can create SLA services as required.

#### Procedure

**Step 1** Choose **Network Application > SLA Management**.

Figure 10-142 SLA management



**Step 2** In the navigation tree, choose **SLA Service Management > Create**.

**Step 3** Set **Name**, **Description**, **Compliance threshold**, and **Rating**.

**Step 4** Select the corresponding test instance in the lower part, and set **Threshold** and **Weight**.

Figure 10-143 SLA service test instance

|                             |                                   |              |                                     |
|-----------------------------|-----------------------------------|--------------|-------------------------------------|
| * Name:                     | <input type="text" value="Data"/> | Description: | <input type="text" value="data"/>   |
| * Compliance threshold (%): | <input type="text" value="80"/>   | Rating:      | <input type="text" value="3-star"/> |

| Test Instance                        | Threshold | Weight |
|--------------------------------------|-----------|--------|
| <input type="checkbox"/> ICMP Echo   |           |        |
| <input type="checkbox"/> ICMP Jitter |           |        |
| <input type="checkbox"/> UDP Echo    |           |        |
| <input type="checkbox"/> UDP Jitter  |           |        |
| <input type="checkbox"/> TCP Connect |           |        |
| <input type="checkbox"/> SNMP        |           |        |
| <input type="checkbox"/> DNS         |           |        |
| <input type="checkbox"/> DHCP        |           |        |
| <input type="checkbox"/> HTTP        |           |        |
| <input type="checkbox"/> FTP         |           |        |

**NOTE**

SLA collects data of counters in the selected test instance. Only counters that are configured with thresholds are used to calculate the compliance.

SLA provides the default thresholds and weights for counters based on the **Rating** value.

**Step 5** Click **OK**.

----End

## Follow-up Procedure

The new SLA service is displayed on the **SLA Service Management** page.

### 10.4.3.2 Creating an SLA Task

An SLA task is a test instance used to check the network link quality.

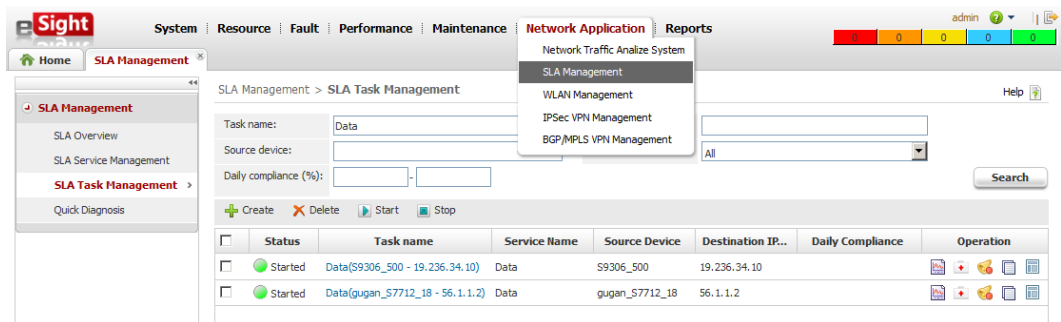
#### Prerequisites

An SLA service has been created.

#### Procedure

**Step 1** Choose **Network Application** > **SLA Management**.

**Figure 10-144** SLA management



**Step 2** In the navigation tree, choose **SLA Task Management** > **Create**.

**Step 3** Set the task basic parameters.

1. Set **Task** and **Description**.
2. Select an SLA service from the **Service name** drop-down list box. If no service meets your requirement, create a service on the **SLA Task Management** page.
3. Set **Source device** to the source device IP address and **Destination IP1** to the IP address and port number of the destination device.



#### NOTE

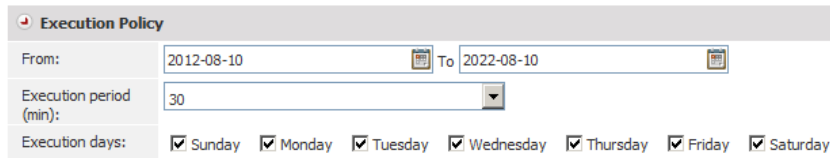
A maximum of five destination devices are supported. You can enter destination device information manually.

**Figure 10-145** Task basic settings

| Task Basic Settings |             |
|---------------------|-------------|
| * Task name:        | Data        |
| * Service name:     | Data        |
| * Destination IP1:  | 193.67.72.3 |
| Destination IP3:    |             |
| Destination IP5:    |             |
| Description:        | Data        |
| * Source device:    | AR2240_2200 |
| Destination IP2:    |             |
| Destination IP4:    |             |

**Step 4** Set the task execution policy.

1. Set the task execution start date and end date.
2. Set **Execution period** and **Execution days**.

**Figure 10-146** Execution policy

The 'Execution Policy' window shows the following settings:

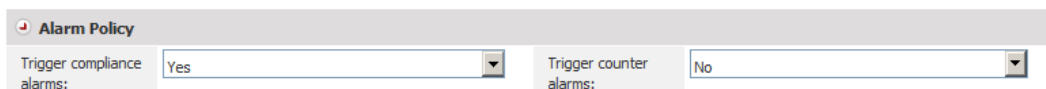
|                         |                                                                                                                                                                                                                                                                                                                      |     |            |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------|
| From:                   | 2012-08-10                                                                                                                                                                                                                                                                                                           | To: | 2022-08-10 |
| Execution period (min): | 30                                                                                                                                                                                                                                                                                                                   |     |            |
| Execution days:         | <input checked="" type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday |     |            |

**Step 5** Set the alarm policy.

1. Set **Trigger compliance alarms**. If the **Trigger compliance alarms** value is **Yes**, an alarm will be triggered when the compliance value is lower than the threshold.
2. Set **Trigger counter alarms**. If the **Trigger counter alarms** value is **Yes**, an alarm will be triggered when the counter value is lower than the threshold.

**NOTE**

Set the **Trigger compliance alarms** and **Trigger counter alarms** parameters with caution. If the network quality is poor, a large number of alarms will be triggered.

**Figure 10-147** Alarm policy

The 'Alarm Policy' window shows the following settings:

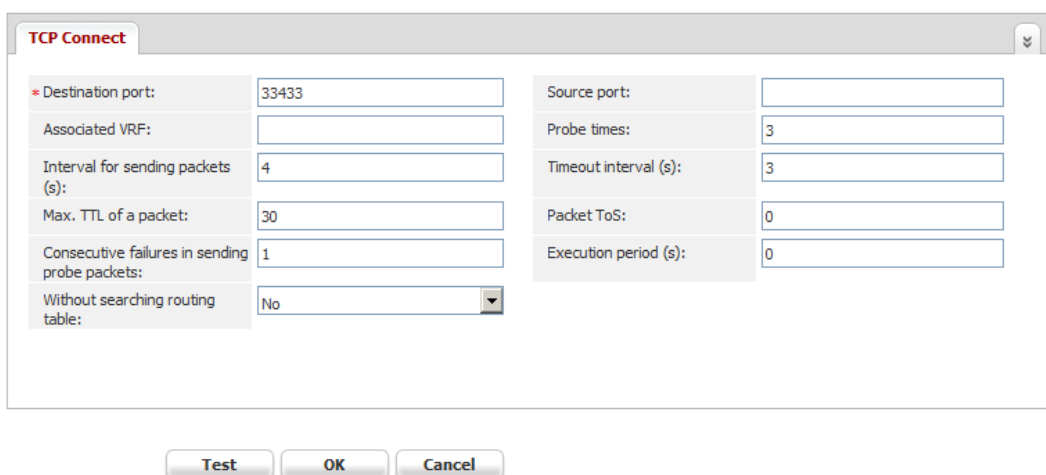
|                            |     |                         |    |
|----------------------------|-----|-------------------------|----|
| Trigger compliance alarms: | Yes | Trigger counter alarms: | No |
|----------------------------|-----|-------------------------|----|

**Step 6** Set test instance parameters.

The number of test instances depends on the tasks that are selected in the **Task Basic Settings** area and the test instances that are supported by the source device.

**NOTE**

For details about the device configuration requirement of each test case, see [Device configuration](#).

**Figure 10-148** Set test instance parameters

The 'TCP Connect' window shows the following settings:

|                                                |       |                       |   |
|------------------------------------------------|-------|-----------------------|---|
| * Destination port:                            | 33433 | Source port:          |   |
| Associated VRF:                                |       | Probe times:          | 3 |
| Interval for sending packets (s):              | 4     | Timeout interval (s): | 3 |
| Max. TTL of a packet:                          | 30    | Packet ToS:           | 0 |
| Consecutive failures in sending probe packets: | 1     | Execution period (s): | 0 |
| Without searching routing table:               | No    |                       |   |

Buttons: Test, OK, Cancel

**Step 7 Optional:** Click **Test** and verify that the new SLA task can be executed properly.

**Step 8** Click **OK**.

----End

### 10.4.3.3 Quick Diagnosis

The quick diagnosis function is used to check links monitored by SLA tasks.

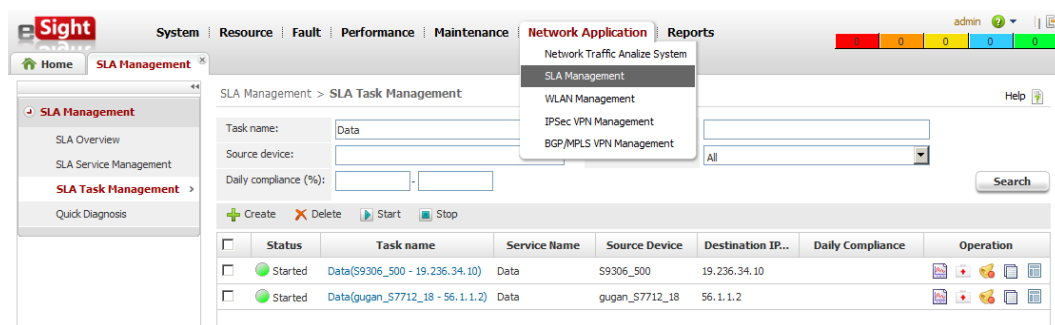
#### Prerequisites

An SLA task has been created.

#### Procedure

**Step 1** Choose **Network Application** > **SLA Management**.

**Figure 10-149** SLA management



**Step 2** In the navigation tree, click **Quick Diagnosis**.

**Step 3** Set parameters in the **Task Basic Settings** area.

1. Select an SLA service from the **Service name** drop-down list box. If no service meets your requirement, create a service on the **SLA Service Management** page.
2. Set **Source device** to the source device IP address and **Destination IP1** to the IP address and port number of the destination device.

Figure 10-150 Task task settings

SLA Management > Quick Diagnosis Help

Task Basic Settings

\* Service name:

Video

...

\* Source device:

S9303\_40

...

\* Destination IP:

10.137.61.40

...

Test Case Settings

ICMP Jitter

UDP Echo

UDP Jitter

Associated VRF:

Probe times:

3

Packets sent per probe:

20

Interval for sending packets (ms):

100

Consecutive failures in sending probe packets:

1

Type of packets sent:

Timestamp packet mode

Packet filling size (byte):

Packet filling content:

Max. TTL of a packet:

30

Packet TOS:

0

Diagnose

Step 4 Set test instance parameters.

The number of test instances to be configured depends on the service selected in **Task Basic Settings** and the test instances that are supported by the source device.

For details about test instance parameters, see the device feature description document.

Step 5 Click **Diagnosis**. The execution status, connection status, and other diagnosis parameters are displayed.

Figure 10-151 Diagnosis

Diagnosis

✓ Diagnose successful.

Details>

ICMP Jitter

UDP Echo

UDP Jitter

Execution status: Diagnose finished.

Connection status: Connected

Packet loss rate(%)

0

Average jitter(ms)

44

Number of timeouts

0

Average unidirectional delay from source to destination(ms)

28

Average unidirectional jitter from destination to source(ms)

1

Average RTD(ms)

29

Max. RTD(ms)

223

Average unidirectional delay from destination to source(ms)

0

Average unidirectional jitter from source to destination(ms)

64

OK

Stop

----End

## 10.4.4 Monitoring SLA Tasks

This topic describes how to monitor SLA tasks.

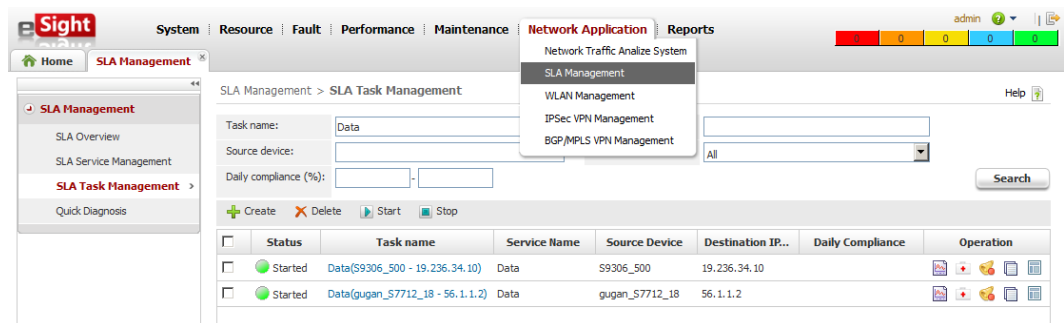
### 10.4.4.1 Accessing the SLA Task Management Page

This topic describes how to access the **SLA Task Management** page to monitor SLA tasks.

#### Procedure

**Step 1** Choose **Network Application** > **SLA Management**.

**Figure 10-152** SLA management



**Step 2** In the navigation tree, choose **SLA Management** > **SLA Task Management**.

**Step 3** In the upper part of the **SLA Task Management** page, you can set **Task name**, **Service name**, **Source device**, **Task Status**, or **Daily compliance** to specify the search criterion.

**Step 4** The **Create**, **Delete**, **Start**, and **Stop** buttons are provided on the toolbar.

Deletion, start, and stop operations can be performed in batches.

**Step 5** Task details are displayed in the table area in the middle of the **SLA Task Management** page. The **Status** and **Daily Compliance** values are updated in real time.

**Step 6** The **Historical data**, **Diagnosis**, **Copy**, and **Details** buttons are provided in the table operation area.

- **Historical data:** For details, see [10.4.4.2 Viewing SLA Historical Data of an SLA Task](#).
- **Diagnosis:** Click this button to check an SLA task. The function of this button is the same as that of **Quick Diagnosis** on the navigation bar.
- **Copy:** Click this button to copy SLA task data. An SLA task with a new name is created.
- **Details:** Click this button to view a task's basic parameters, execution policies, alarm policies, and test instance parameters.

----End

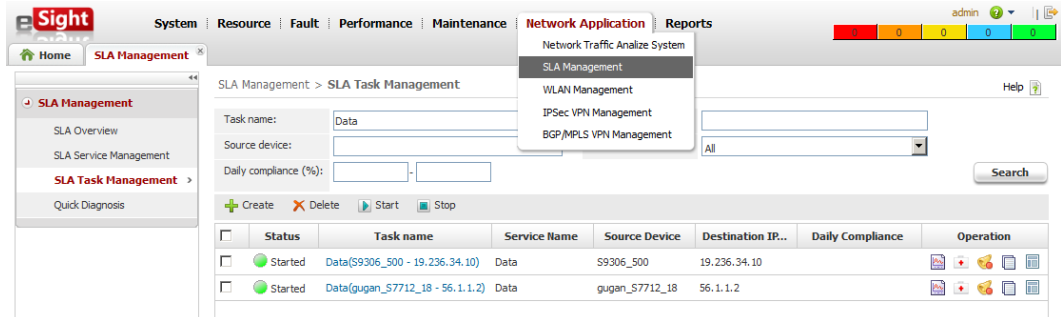
### 10.4.4.2 Viewing SLA Historical Data of an SLA Task

The SLA task details page displays the counter value graph in a specified period.

## Procedure

**Step 1** Choose **Network Application** > **SLA Management**.

**Figure 10-153** SLA management



**Step 2** In the navigation tree, choose **SLA Management** > **SLA Task Management**.

**Figure 10-154** Viewing historical data

| <input type="checkbox"/> | Status  | Task name                       | Service Name | Source Device  | Destination IP... | Daily Compliance | Operation                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------|---------------------------------|--------------|----------------|-------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Started | Data(S9306_500 - 19.236.34.10)  | Data         | S9306_500      | 19.236.34.10      |                  |         |
| <input type="checkbox"/> | Started | Data(gugan_S7712_18 - 56.1.1.2) | Data         | gugan_S7712_18 | 56.1.1.2          |                  |     |

**Step 3** In the table operation area on the right, click **Historical data** next to an SLA task. The counter value graph of the SLA task is displayed.

- You can set the counter value time span in the filter area in the upper part of the page.
- The **Compliance** area in the upper part of the page can be expanded and collapsed. In the **Compliance** area, you can view the comparison between the actual compliance value and the threshold. The line in blue indicates the actual compliance value, and the line in red indicates the threshold.
- The test instance counter display area in the lower part of the page also can be expanded and collapsed. If there are multiple test instances, SLA displays the test instances in multiple areas. Users can switch counters on the right of the display area. The line in blue indicates the actual counter value, and the line in red indicates the threshold configured for the corresponding service rating.
- SLA data in the compliance data area and counter display area can be exported.



### NOTE

Consolidation data saving policy:

- Original data: saved for one month
- Hourly data: saved for one year
- Daily data: saved for one year
- Weekly data: saved for three years
- Monthly data: saved permanently

----End



## 10.4.5 Typical SLA Applications

This topic describes two typical SLA applications.

### 10.4.5.1 Example: Creating a Predefined Task

This topic describes how to create a predefined task.

#### Prerequisites

- You have the operator right or a superior right.
- eSight has been connected to NEs using TCP/IP and can manage and maintain NEs.
- Devices support built-in Network Quality Analysis (NQA) probes.

#### Application Scenario

The service development requires one more device. The device has been installed and commissioned on the network and has been added to eSight. Now the administrator wants to test the video quality between the new device and the existing devices to locate and solve problems.

#### Procedure

**Step 1** Choose **Network Application > SLA Management**.

**Step 2** In the navigation tree, click **SLA Task Management**. Then click **Create**.

**Step 3** Set the task basic parameters.

1. Set **Task** and **Description**.
2. Set **Service name** to **Video**.
3. Set **Source device** to the new device IP address and **Destination IP1** to the IP address and port number of a neighboring device.

**Step 4** Retain the default task execution policy and alarm policy for the task, and click **OK**.

----End

### 10.4.5.2 Example: Creating a User-Defined Task

This topic describes how to create a user-defined task.

#### Prerequisites

- You have the operator right or a superior right.
- eSight has been connected to NEs using TCP/IP and can manage and maintain NEs.
- Devices support built-in Network Quality Analysis (NQA) probes.

#### Application Scenario

Employees in building B frequently complain about instant messaging interruptions. The administrator wants to test the instant messaging service to locate and solve the problem.

## Procedure

**Step 1** Choose **Network Application > SLA Management**.

**Step 2** Create an SLA service.

1. In the navigation tree, click **SLA Service Management**. Then click **Create**.
2. Set **Name** to instant messaging, **Description** to instant messaging service test, **Compliance threshold** to **80**, and **Rating** to **5-star**.
3. Select **ICMP Echo** and **UDP Echo**, and set the threshold and weight for the ICMP Echo and UDP Echo tests.
4. Click **OK**.

**Step 3** Create an SLA task.

1. In the navigation tree, click **SLA Task Management**. Then click **Create**.
2. Set **Task** and **Description**.
3. Set **Service name** to instant messaging.
4. Set **Source device** to the IP address of the egress device in building B and **Destination IP1** to the IP address and port number of the headquarters egress device.

**Step 4** Set the task execution policy.

1. Set the task execution start date and end date.
2. Set **Execution period** to **5** and **Execution days** to Monday to Friday.

**Step 5** Set the alarm policy.

1. Set **Trigger compliance alarms** to **Yes**.
2. Set **Trigger counter alarms** to **No**.

**Step 6** Set test instance parameters.

1. Set the parameters of the ICMP Echo test instance.
2. Set the parameters of the UDP Echo test instance.

**Step 7** Click **OK**.

After creating the task, you can click **Test** to verify that the SLA task can be executed properly.

----End

---

# 11 Smart Configuration Tool

---

## About This Chapter

This topic describes functions provided by the smart configuration tool and the procedure for configuring the smart configuration tool.

### [11.1 Overview](#)

This topic describes the Smart Configuration Tool operations.

### [11.2 Functions](#)

When establishing network environment, you must configure a large number of network elements (NEs). Generating scripts manually based on a network plan is time-consuming and may contain errors. With the smart configuration tool, you can configure a template and plan sheet, and send the same parameter settings to multiple NEs, greatly improving NE configuration efficiency.

### [11.3 Function Panorama](#)

This topic describes the delivery by template and delivery by plan sheet functions of the smart configuration tool.

### [11.4 Configuring Tasks](#)

This topic describes how to configure tasks using the smart configuration tool.

### [11.5 Examples](#)

This topic describes two typical applications to help network administrators better understand the smart configuration tool.

## 11.1 Overview

This topic describes the Smart Configuration Tool operations.

[Figure 11-1](#) shows the overview of Smart Configuration Tool operations. For details, click [operations in the overview](#).

## Overview of Smart Configuration Tool Operations

**Figure 11-1** Overview of Smart Configuration Tool Operations

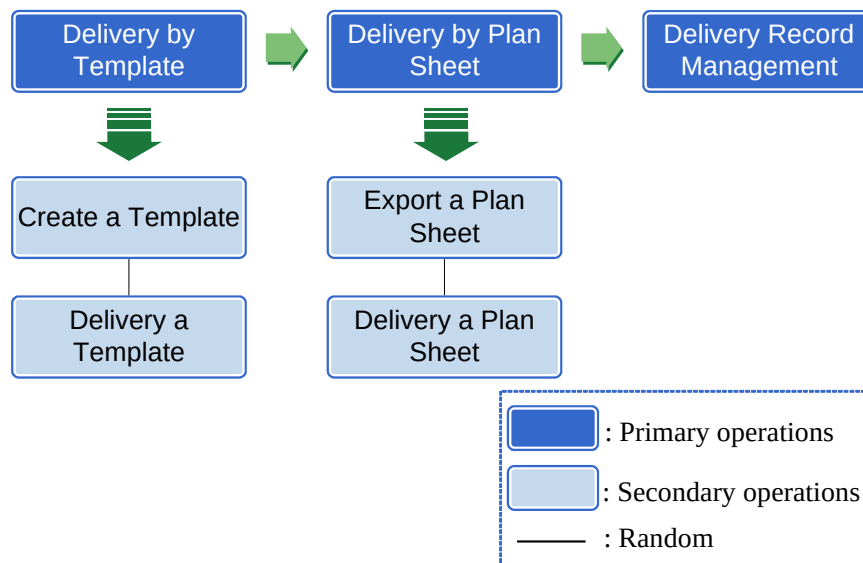


Table 11-1 describes the smart configuration tool operations.

**Table 11-1** Smart Configuration Tool Operations

| Operation                                            | Description                                                                                                                                                                    |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">11.3.1 Delivery by Template</a>          | The delivery by template function allows you to set parameters for a common or user-defined command line in a template and send the template to multiple devices.              |
| <a href="#">11.3.2 Delivery by Plan Sheet</a>        | The delivery by plan sheet function allows you to set parameters in a plan sheet to different values and deliver the plan sheet to corresponding devices. Process Description. |
| <a href="#">11.3.3 Delivery Record Management</a>    | This topic describes delivery record management operations.                                                                                                                    |
| <a href="#">11.4.1.1 Creating a Template</a>         | This topic describes how to create a template.                                                                                                                                 |
| <a href="#">11.4.1.2 Delivering a Template</a>       | This topic describes how to deliver a template to devices.                                                                                                                     |
| <a href="#">11.4.2.1 Exporting a Plan Sheet</a>      | This topic describes how to export a verified template. You can modify an exported template, and import the new template.                                                      |
| <a href="#">11.4.2.2 Delivering a Plan Sheet</a>     | You can use the plan sheet to deliver a template containing different parameter settings to multiple network devices.                                                          |
| <a href="#">11.5.1 Example: Delivery by Template</a> | This topic describes a typical application to help network administrators better understand how to delivery by template.                                                       |

| Operation                                              | Description                                                                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">11.5.2 Example: Delivery by Plan Sheet</a> | After a plan sheet is imported, the smart configuration tool automatically generates a configuration script for each device and delivers the configuration scripts to devices. |

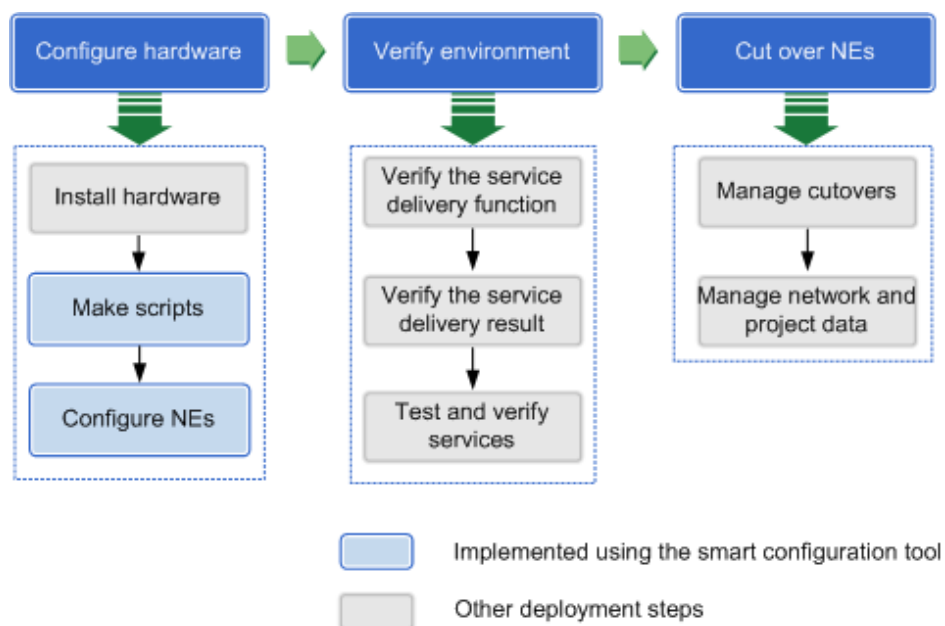
## 11.2 Functions

When establishing network environment, you must configure a large number of network elements (NEs). Generating scripts manually based on a network plan is time-consuming and may contain errors. With the smart configuration tool, you can configure a template and plan sheet, and send the same parameter settings to multiple NEs, greatly improving NE configuration efficiency.

- The smart configuration tool provides the template management function to quickly generate templates. In a template, you can configure a same command for multiple NEs in batches.
- The smart configuration tool provides the plan sheet delivery function to deliver parameters of a command to multiple NEs in batches.

Figure 11-2 shows the application scenario of the smart configuration tool.

**Figure 11-2** Application scenario of the smart configuration tool



The smart configuration tool is used to make scripts and configure devices during site deployment. It supports graphical command line interfaces (GCLIs) and currently supports only Huawei devices.

## 11.3 Function Panorama

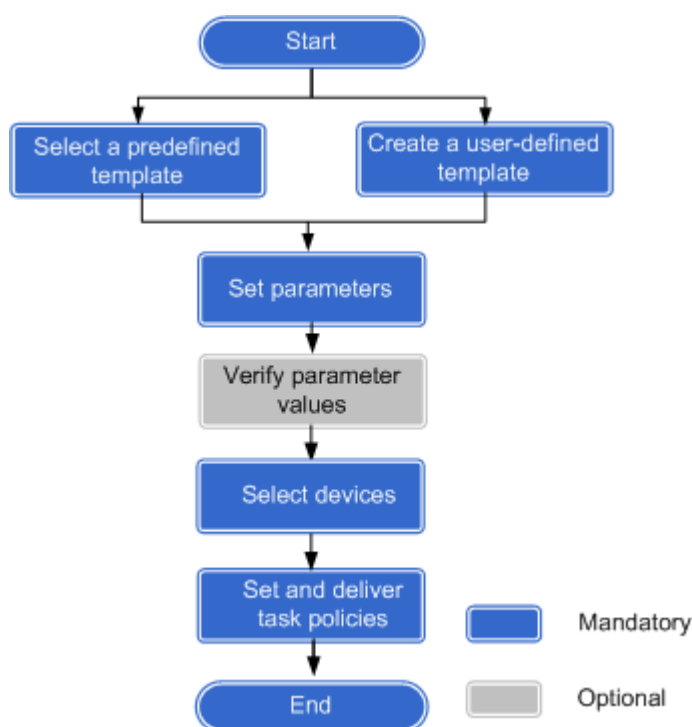
This topic describes the delivery by template and delivery by plan sheet functions of the smart configuration tool.

### 11.3.1 Delivery by Template

The delivery by template function allows you to set parameters for a common or user-defined command line in a template and send the template to multiple devices.

#### Process Description

Figure 11-3 Process of delivery by template



#### Function Description

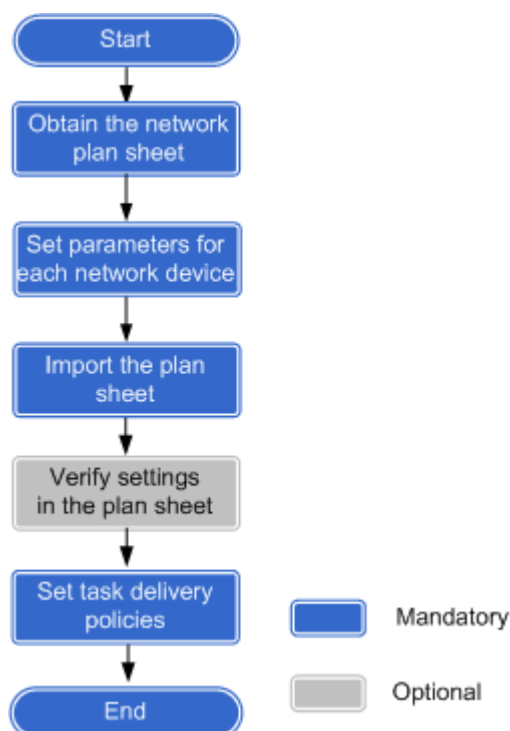
1. Template base
  - Predefined template: Displays predefined common templates.
  - User-defined template: Displays user-defined templates in the **User-defined** folder, and allows you to create, copy, move, modify, and delete templates, and create folders to classify templates to make the finding and management easy.
2. Delivery by template
  - **Deploy**: Select an existing template in the template base, set parameters, and send the template to multiple devices.
  - To deliver a template, perform the following steps: select a template, set parameters, select devices, and configure tasks.

## 11.3.2 Delivery by Plan Sheet

The delivery by plan sheet function allows you to set parameters in a plan sheet to different values and deliver the plan sheet to corresponding devices.

### Process Description

Figure 11-4 Process of delivery by plan sheet



### Function Description

The delivery by plan sheet function allows you to set parameters in a plan sheet to different values and deliver the plan sheet to corresponding devices.

1. Importing a plan sheet
  - Choose **Template Deploy** in the navigation tree, and click **Export Plan Sheet** to generate a plan sheet, or create a plan sheet manually on the local host.
  - Generate scripts based on network device names, IP addresses, and service parameters set in the plan sheet.
  - Plan sheets can only be Excel 2003 files. Excel 2007 files and later versions are not supported currently.
2. Verification
  - The verification function compares device command sets on eSight with parameter values entered by a current user.
  - If no device command set exists on eSight, eSight obtains device command sets from devices in real time.

## 11.3.3 Delivery Record Management

This topic describes delivery record management operations.

### Function Description

Delivery records enable you to view the execution status and result of all tasks.

1. The delivery record table lists task information including the task name, type, status, result, description, creation time, and execution time.
2. You can click **Operation** next to a task to view the task details including the device name, IP address, and device type, click **View Configuration Command** to view the delivered configuration command, and click **Delivery result** to view the command execution result.
3. You can click **Export Result** next to a task to save device execution information to the local host.
4. Tasks can be deleted in batches.
5. The operation logs of the smart configuration tool are recorded in the file in *eSight installation directory*\gcli\deploy\log\SctOperation-YEAR.MON.DAY-HOUR.MIN.SEC.log.

## 11.4 Configuring Tasks

This topic describes how to configure tasks using the smart configuration tool.

### 11.4.1 Template Management and Delivery

The delivery by template function allows you to set mandatory parameters for common or user-defined command lines and send the command lines to multiple devices.

#### 11.4.1.1 Creating a Template

This topic describes how to create a template.

### Context

The smart configuration tool provides multiple predefined templates. If the predefined templates cannot meet your requirements, you can create templates as required.

### Procedure

- Step 1** Choose **Maintenance > Smart Configuration Tool** from the main menu.

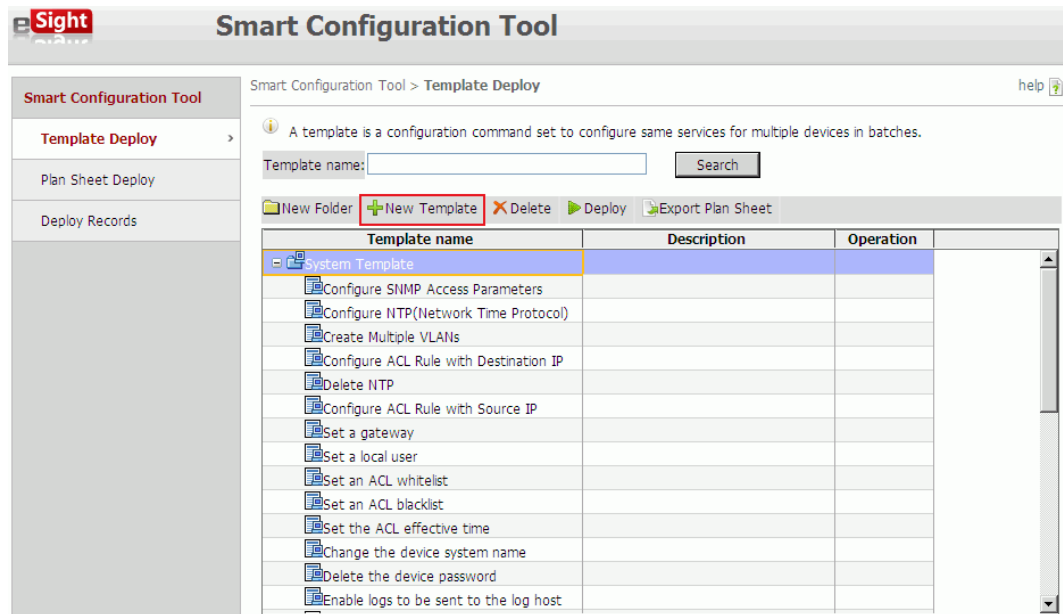
**Figure 11-5** Smart configuration tool





**Step 2** In the navigation tree, click **Template Deploy**. Then expand the **User-defined** folder.

**Figure 11-6** Creating template



**Step 3** Click **New Template**. The page for creating a template is displayed.

**Step 4** Set **Directory**, **Template name**, **Description**, and **Template Content**.

**Figure 11-7** Template basic information

Basic Information

Directory:

\*Template name:  Description:

\*Template Content

```
system-view
vlan batch 1 to 2
quit
```

**CAUTION**

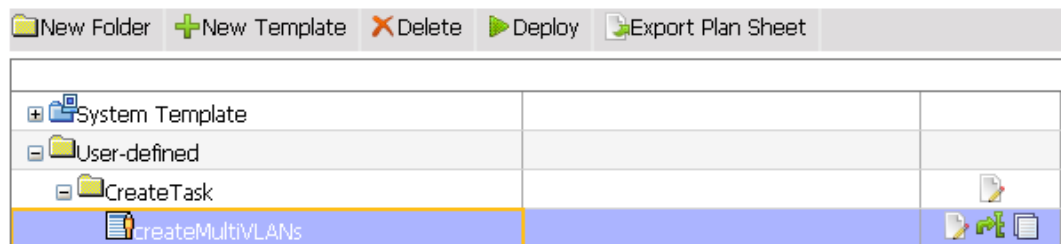
When copying a command, copy only information in the plain text format. For example, if you copy a command from a web page, the content may contain hidden special characters.

**NOTE**

Generally, prefix **system-view** to the **Template Content** value to enter the system view. You do not need to enter **quit** to the **Template Content** value. The smart configuration tool will automatically suffix **quit** based on command lines.

**Step 5** Click **OK**. The new template is displayed in the **User-defined** folder.

**Figure 11-8** User-defined templates

**NOTE**

If you want to generate a template, select a device to verify. If the template is verified, a table template is generated.

**Figure 11-9** Verification result

Basic Information

Directory:

\*Template name:  Description:

\*Template Content

Complete [Shift to command](#)

|                               | Shell |                                |
|-------------------------------|-------|--------------------------------|
| system-view                   |       | --                             |
| vlan batch INTEGER<1-4094> to |       | --                             |
| * INTEGER<1-4094>             |       | <input type="text" value="1"/> |
| * INTEGER<1-4094>             |       | <input type="text" value="2"/> |

----End

### 11.4.1.2 Delivering a Template

This topic describes how to deliver a template to devices.

## Procedure

**Step 1** Choose **Maintenance** > **Smart Configuration Tool** from the main menu.

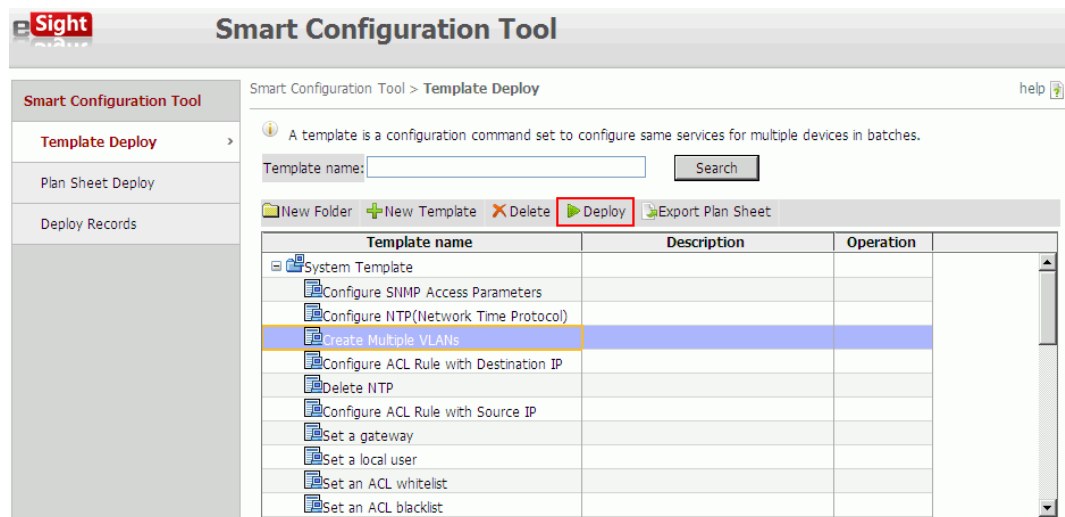
**Figure 11-10** Smart configuration tool



**Step 2** In the navigation tree, click **Template Deploy**, and select the template to be delivered.

**Step 3** Click **Deploy**. The page for delivering a template is displayed.

**Figure 11-11** Deploying template



**Step 4** Set parameters.

**Figure 11-12** Setting parameters

Smart Configuration Tool > **Template Deploy** help ?

Set parameters Select Device Set task

Parameter can be modified, it can be saved to the new template and can be used to deploy. [Shift to command](#)

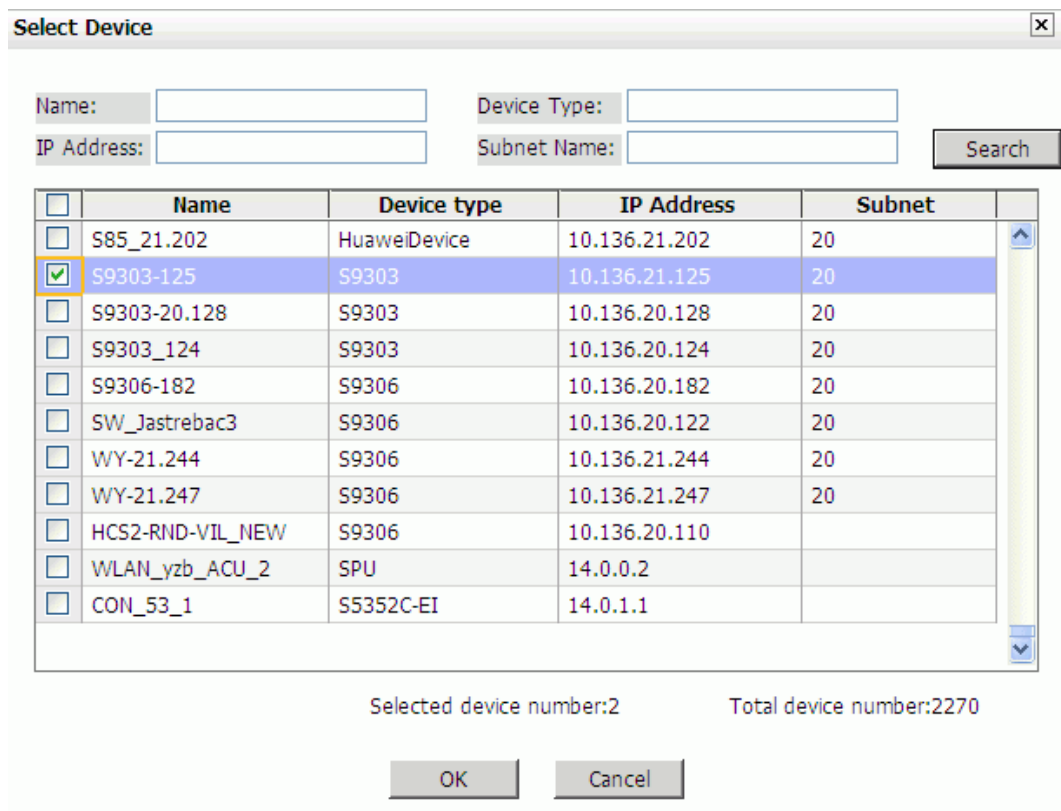
| Command                       | Command description              | Parameter value |
|-------------------------------|----------------------------------|-----------------|
| system-view                   | System view                      | --              |
| vlan batch INTEGER<1-4094> to | Create VLAN and access VLAN view | --              |
| * INTEGER<1-4094>             | VLAN ID                          | 5               |
| * INTEGER<1-4094>             | Last VLAN ID                     | 10              |

Save as Next Cancel

1. Set parameters in the command table.
2. Click **Next**.

**Step 5** Select devices.

1. Click **Add**.
2. Select devices in the **Select Device** dialog box that is displayed.

**Figure 11-13** Selecting devices

The 'Select Device' dialog box contains search filters and a table of available devices.

Search filters:

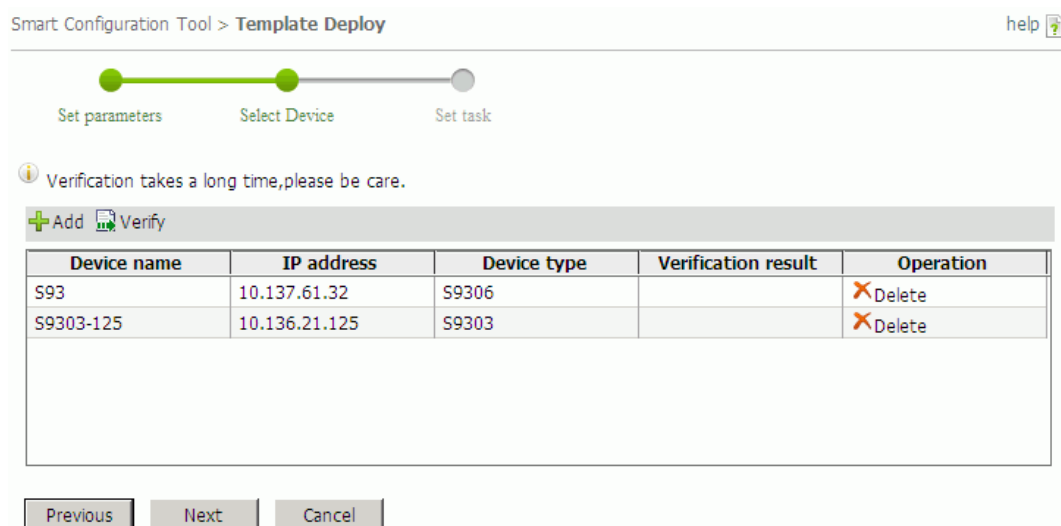
- Name:
- Device Type:
- IP Address:
- Subnet Name:
- Search button

| <input type="checkbox"/>            | Name             | Device type  | IP Address    | Subnet |
|-------------------------------------|------------------|--------------|---------------|--------|
| <input type="checkbox"/>            | S85_21.202       | HuaweiDevice | 10.136.21.202 | 20     |
| <input checked="" type="checkbox"/> | S9303-125        | S9303        | 10.136.21.125 | 20     |
| <input type="checkbox"/>            | S9303-20.128     | S9303        | 10.136.20.128 | 20     |
| <input type="checkbox"/>            | S9303_124        | S9303        | 10.136.20.124 | 20     |
| <input type="checkbox"/>            | S9306-182        | S9306        | 10.136.20.182 | 20     |
| <input type="checkbox"/>            | SW_Jastrebac3    | S9306        | 10.136.20.122 | 20     |
| <input type="checkbox"/>            | WY-21.244        | S9306        | 10.136.21.244 | 20     |
| <input type="checkbox"/>            | WY-21.247        | S9306        | 10.136.21.247 | 20     |
| <input type="checkbox"/>            | HCS2-RND-VIL_NEW | S9306        | 10.136.20.110 |        |
| <input type="checkbox"/>            | WLAN_yzb_ACU_2   | SPU          | 14.0.0.2      |        |
| <input type="checkbox"/>            | CON_53_1         | S5352C-EI    | 14.0.1.1      |        |

Selected device number:2      Total device number:2270

OK      Cancel

- Click **OK**.
- Click **Next**.

**Figure 11-14** Selected devices

The 'Smart Configuration Tool > Template Deploy' screen shows a progress bar with three steps: 'Set parameters' (completed), 'Select Device' (current), and 'Set task' (pending).

Verification takes a long time, please be care.

+ Add      Verify

| Device name | IP address    | Device type | Verification result | Operation |
|-------------|---------------|-------------|---------------------|-----------|
| S93         | 10.137.61.32  | S9306       |                     | ✗ Delete  |
| S9303-125   | 10.136.21.125 | S9303       |                     | ✗ Delete  |

Previous      Next      Cancel

**Step 6** Set task.

**Figure 11-15** Setting task

Set parameters      Select Device      Set task

Rollback need to reboot the device.

\*Task Name : createMultiVLANs

Description: Create Multiple VLANs

Execute: ☐ Instantly ☒ At 2012/04/19 21:00:00

Restore policy: ☒ Backup ☐ Rollback

Previous OK Cancel

1. Set **Task Name**, **Description** (optional), **Execute** and **Restore policy**(optional).
2. Click **Deploy/OK**.
3. In the **Confirm** dialog box, click **YES**.

----End

## Follow-up Procedure

In the navigation tree, click **Deploy Records**. The task execution progress and details about devices to which the task is delivered are displayed in the task list.

**Figure 11-16** Deployed records

Smart Configuration Tool > Deploy Records [help](#)

|                          |                    |          |          |         |     |                     |                     |        |
|--------------------------|--------------------|----------|----------|---------|-----|---------------------|---------------------|--------|
| Task Name:               |                    | Type:    | All      | Status: | All | Result:             | All                 | Search |
| <b>Delete</b>            |                    |          |          |         |     |                     |                     |        |
| <input type="checkbox"/> | task20120418203728 | Instance | Complete | Partial |     | 2012-04-18 20:37:36 | 2012-04-18 20:37:36 |        |
| <input type="checkbox"/> | createMultiVLANs   | Instance | Complete | Success |     | 2012-04-18 20:32:09 | 2012-04-18 20:32:09 |        |
| <input type="checkbox"/> | task20120324113054 | Instance | Complete | Success |     | 2012-03-24 11:29:22 | 2012-03-24 11:29:22 |        |

## 11.4.2 Plan Sheet Management and Delivery

You can use the plan sheet to deliver a template containing different parameter settings to multiple network devices.

### 11.4.2.1 Exporting a Plan Sheet

This topic describes how to export a verified template. You can modify an exported template, and import the new template.

## Prerequisites

Templates have been verified.

## Procedure

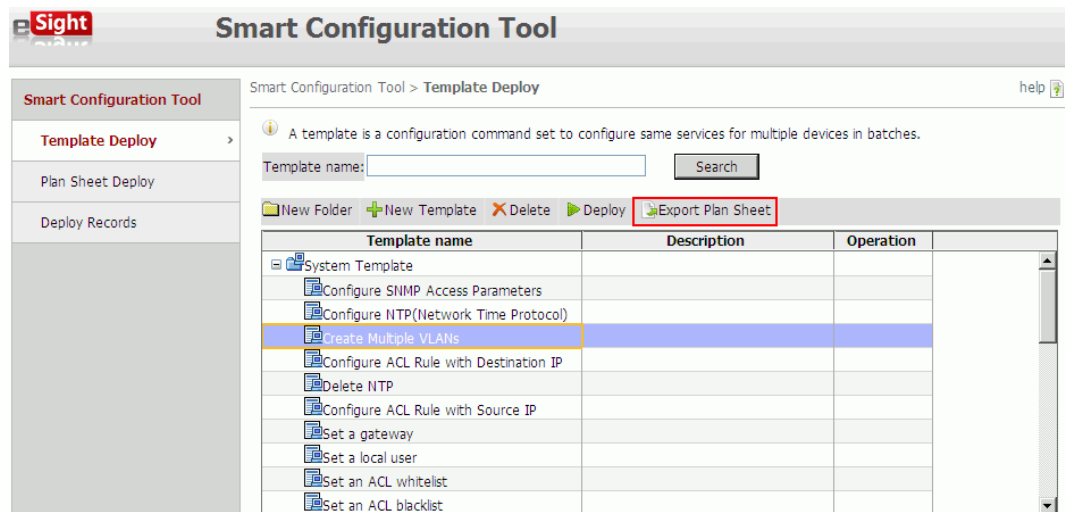
**Step 1** Choose **Maintenance > Smart Configuration Tool** from the main menu.

**Figure 11-17** Smart configuration tool



**Step 2** In the navigation tree, click **Template Deploy**, and search for a template to be exported.

**Figure 11-18** Selecting template



**Step 3** Select the template, and click **Export Plan Sheet**.

The **Export Plan Sheet** dialog box is displayed.

**Figure 11-19** Exporting plan sheet

**Export Plan Sheet**

Additional Columns

First Customized Column:  Last Customized Column:

Select Device

Name:  Device Type:

IP Address:  Subnet Name:

| <input type="checkbox"/>            | Name          | Device type  | IP Address    | Subnet |
|-------------------------------------|---------------|--------------|---------------|--------|
| <input type="checkbox"/>            | S5752EI-83    | S5700-52C-EI | 10.136.21.83  | 20     |
| <input type="checkbox"/>            | S6324EI-114   | S6324-EI     | 10.136.21.114 | 20     |
| <input type="checkbox"/>            | S6506R_21.201 | HuaweiDevice | 10.136.21.201 | 20     |
| <input type="checkbox"/>            | S6724         | S6700-24-EI  | 10.136.20.234 | 20     |
| <input type="checkbox"/>            | S85_21.202    | HuaweiDevice | 10.136.21.202 | 20     |
| <input checked="" type="checkbox"/> | S9303-125     | S9303        | 10.136.21.125 | 20     |
| <input type="checkbox"/>            | S9303-20.128  | S9303        | 10.136.20.128 | 20     |
| <input type="checkbox"/>            | S9303-124     | S9303        | 10.136.20.124 | 20     |

Selected device number:2      Total device number:2270

**Step 4 Optional:** Set **First Customized Column** and **Last Customized Column**.**NOTE**

The plan sheet is exported to an Excel file. You can add a column before the first column and a column after the last column to the Excel file to specify device flags such as locations and remarks, which facilitates maintenance.

**Step 5 Optional:** Select the devices.**Step 6** Click **OK**. Save the plan sheet to the local host.**Step 7** Close the **Export Plan Sheet** dialog box.

----End

### 11.4.2.2 Delivering a Plan Sheet

This topic describes how to deliver a plan sheet to multiple network devices.

#### Prerequisites

- A network data plan sheet has been obtained. You can export a plan sheet or manually create a plan sheet on the local host.



**NOTE**

If a cell in a plan sheet indicates time, for example, **12:15**, set the cell format to **Text**.

- All mandatory parameters in the plan sheet have been set, and device names in the plan sheet exist on eSight (if device names do not exist on eSight, the import fails).

## Procedure

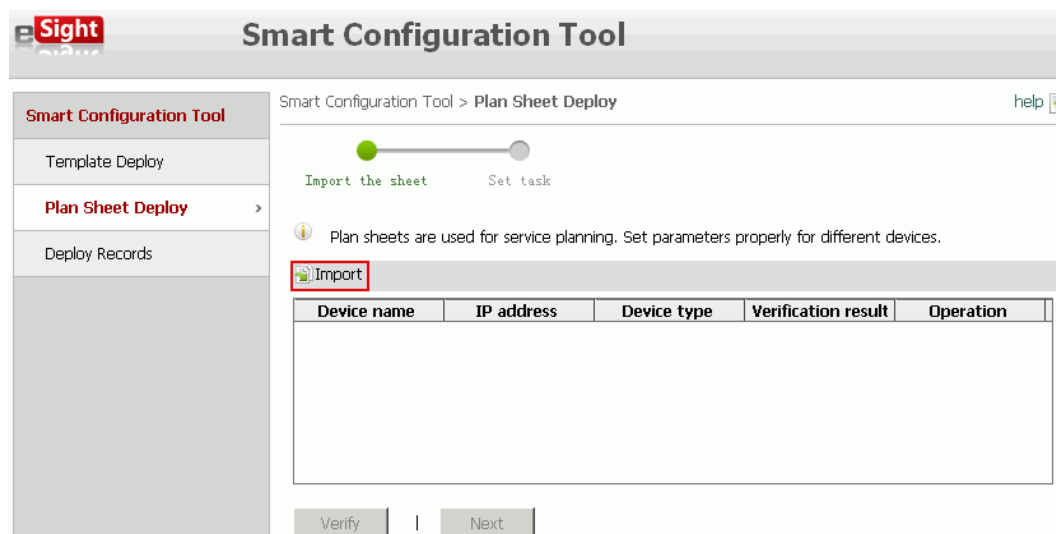
**Step 1** Choose **Maintenance > Smart Configuration Tool** from the main menu.

**Figure 11-20** Smart configuration tool

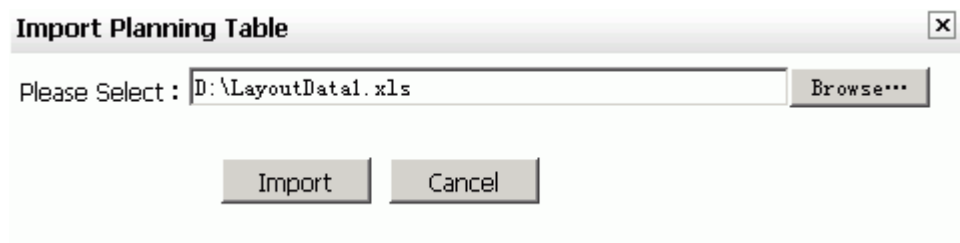


**Step 2** In the navigation tree, click **Plan Sheet Deploy**. The wizard for delivery by plan sheet is displayed.

**Figure 11-21** Import wizard

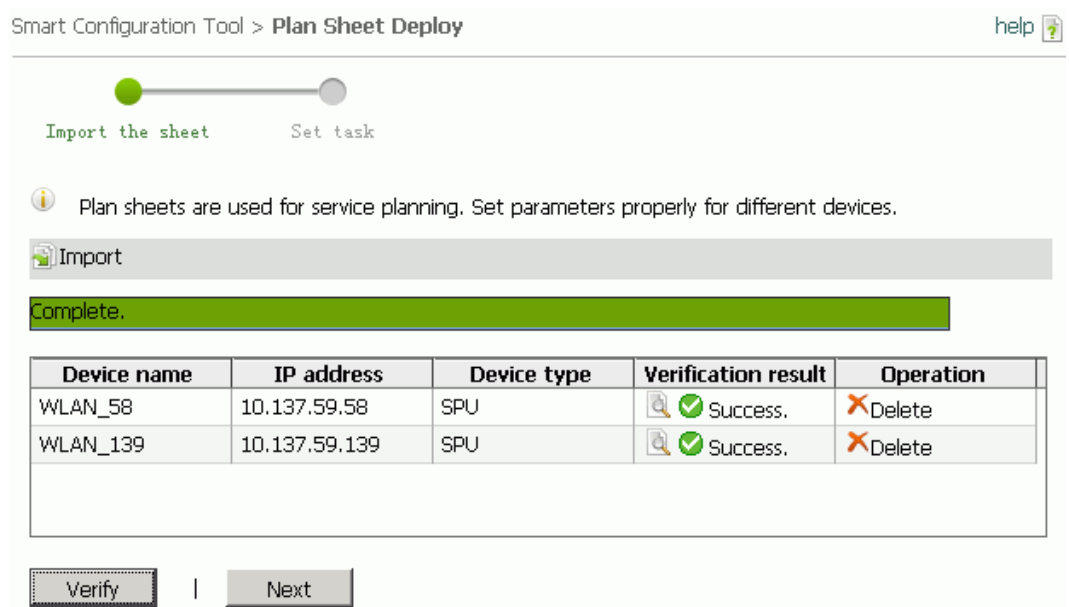


**Step 3** Click **Import**, and select the file to be imported in the **Import Planning Table** dialog box that is displayed.

**Figure 11-22** Importing planning table

**Step 4** Click **Import**. Information such as the device name, IP address, and device type in the plan sheet is displayed.

**Step 5 Optional:** Click **Verify**. The verification result is displayed.

**Figure 11-23** Verification result

**Step 6 Optional:** Click **Delete** to delete devices that fail to be verified.

**Step 7** Click **Next**. The **Set task** page is displayed.

**Step 8** Set task.

**Figure 11-24** Setting task

Smart Configuration Tool > Plan Sheet Deploy help ?



Import the sheet      Set task

 Rollback need to reboot the device.

\*Task Name :

Description:

Execute: ☒ Instantly    ☐ At     

Restore policy: ☐ Backup    ☐ Rollback

1. Set **Task Name**, **Description** (optional), **Execute** and **Restore policy**(optional).
2. Click **Deploy/OK**.
3. In the **Confirm** dialog box, click **YES**.

**NOTE**

On the current page, you can view the task execution progress and details about devices to which the task is delivered. You can also view the task execution details on the **Deploy Records** tab page.

**Figure 11-25** Deployed result

Smart Configuration Tool > Plan Sheet Deploy help ? Back

 When a task is stopped, the Telnet connection on a device remains until the script deploy is complete.

 A task cannot be executed again after being stopped. For details about task execution, see task details.

Complete.100%

| Device name | IP address    | Device type | Template Content                                                                    | Deploy result                                                                                  |
|-------------|---------------|-------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| WLAN_139    | 10.137.59.139 | SPU         |  |  Failure. |
| WLAN_58     | 10.137.59.58  | SPU         |  |  Success. |

----End

## 11.5 Examples

This topic describes two typical applications to help network administrators better understand the smart configuration tool.

## 11.5.1 Example: Delivery by Template

### Context

A user wants to deliver a command line to one or more devices and execute the deployment task immediately based on the specified sequence. For example, the user wants to deliver the command line **Create Multiple VLANs** to devices whose IP addresses are 10.138.35.43 and 10.38.35.60. The command line contains the following parameters: start VLAN ID and end VLAN ID.

### Procedure

**Step 1** Choose **Maintenance > Smart Configuration Tool** from the main menu.

**Step 2** In the navigation tree, click **Template Deploy**, and search for the template **Create Multiple VLANs**.

**Step 3** Click **Deploy**. The template delivery wizard is displayed.

**Step 4** Modify the start and end VLAN IDs as required, and click **Next**.



#### NOTE

- Parameters marked with an asterisk (\*) are mandatory. If a parameter marked with an asterisk (\*) is left blank, the template will not contain this command.
- The smart configuration tool provides default settings. You can modify parameters based on the site scenario.

**Step 5** Click **Add**, select the devices whose IP addresses are 10.38.35.43 and 10.138.35.60 from the device list in the **Select Device** dialog box that is displayed, and click **OK**. Then click **Next**.



#### NOTE

- After selecting the devices, you can verify the commands. The verification takes a long period and cannot be interrupted. Therefore, verify commands with caution.
- You can verify the command line syntax based on command sets even if the device is disconnected from eSight.

**Step 6** Set **Task Name**, **Description** (optional), **Execute** and **Restore policy**, and click **Deploy**.

----End

### Follow-up Procedure

In the navigation tree, click **Deploy Records**. The task execution progress and details about devices to which the task is delivered are displayed in the task list.

## 11.5.2 Example: Delivery by Plan Sheet

After a plan sheet is imported, the smart configuration tool automatically generates a configuration script for each device and delivers the configuration scripts to devices.

### Prerequisites

- A network data plan sheet has been obtained. You can export a plan sheet or manually create a plan sheet on the local host.
- All mandatory parameters in the plan sheet have been set, and device names in the plan sheet exist on eSight (if device names do not exist on eSight, the import fails).

## Context

Predefined templates can be directly exported as plan sheets, and self-defined templates must be verified before they are exported as plan sheets.

## Procedure

- Step 1** Choose **Maintenance > Smart Configuration Tool** from the main menu.
- Step 2** In the navigation tree, click **Plan Sheet Deploy**. The wizard for delivery by plan sheet is displayed.
- Step 3** Click **Import**, and select the file to be imported in the **Import Planning Table** dialog box that is displayed.
- Step 4** Click **Import**. Information such as the device name, IP address, and device type in the plan sheet is displayed.
- Step 5** (Optional) Click **Verify**. The verification result is displayed.
- Step 6** Click **Next**. The **Set task** page is displayed.
- Step 7** Set **Task Name**, **Description** (optional), **Execute** and **Restore policy**, and click **Deploy**.

----End

## Follow-up Procedure

1. Click the **Deploy Records** tab.
2. The task execution progress and details about devices to which the task is delivered are displayed in the task list.

# 12 Device Configuration File Management

---

## About This Chapter

Device configuration files vary based on the service configuration on devices. To ensure the security of device configuration files, eSight provides the functions of backing up and restoring device configuration files.

### [12.1 Overview of Device Configuration File Management Operations](#)

This topic describes the device configuration file management operations.

### [12.2 Setting FTP Parameters](#)

Before backing up or restoring a device configuration file, ensure that FTP parameters are set correctly. If they are set incorrectly, you cannot transfer files between NEs and eSight properly.

### [12.3 Backing Up NE Configuration Files](#)

You can back up NE configuration files to the eSight server to avoid NE data damage or loss due to upgrade, rollback, or other exceptions.

### [12.4 Managing NE Configuration Files](#)

This topic describes common operations for managing NE configuration files.

### [12.5 Restoring NE Configuration Files](#)

When an NE is faulty, you can upload an NE configuration file to the NE to restore NE configuration data.

## 12.1 Overview of Device Configuration File Management Operations

This topic describes the device configuration file management operations.

[Figure 12-1](#) shows the overview of device configuration file management operations. For more details, click the operation in the overview.

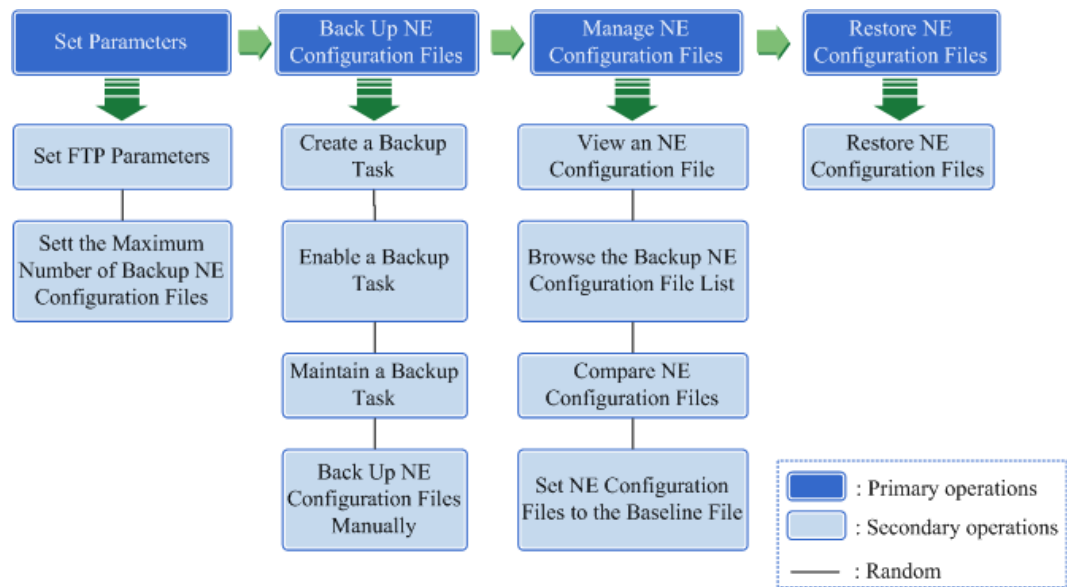
**Figure 12-1** Overview of device configuration file management operations

Table 12-1 lists the device configuration file management operations.

**Table 12-1** Device Configuration File Management Operations

| Operation                                                   | Description                                                                                                                                                                                       |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Setting FTP Parameters                                      | Before backing up or restoring a device configuration file, ensure that FTP parameters are set correctly. If they are set incorrectly, you cannot transfer files between NEs and eSight properly. |
| Setting the Maximum Number of Backup NE Configuration Files | You must set the maximum number of backup NE configuration files to avoid excessive space usage.                                                                                                  |
| Creating a Backup Task                                      | You can create a backup task for a type of NEs.                                                                                                                                                   |
| Enabling a Backup Task                                      | When a configuration file backup task is disabled, you must enable the backup task for execution.                                                                                                 |
| Maintaining a Backup Task                                   | You can browse and maintain a backup task as required.                                                                                                                                            |
| Backing Up NE Configuration Files Manually                  | You can back up NE configuration files manually for instant backup.                                                                                                                               |
| Viewing an NE Configuration File                            | This topic describes how to view a backup NE configuration file and a configuration file that is in use.                                                                                          |
| Browsing the Backup NE Configuration File List              | After backing up an NE configuration file, you need to browse all the NE's backup                                                                                                                 |

| Operation                                                           | Description                                                                                                                                                            |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | configuration files to verify that the configuration file is backed up successfully.                                                                                   |
| <a href="#">Comparing NE Configuration Files</a>                    | You can know differences between NE configuration files by comparing them.                                                                                             |
| <a href="#">Setting NE Configuration Files to the Baseline File</a> | After a configuration file that is being used by an NE is backed up to eSight, you can set the NE configuration file to the baseline file for subsequent file restore. |
| <a href="#">Restoring NE Configuration Files</a>                    | When an NE is faulty, you can upload an NE configuration file to the NE to restore NE configuration data.                                                              |

## 12.2 Setting FTP Parameters

Before backing up or restoring a device configuration file, ensure that FTP parameters are set correctly. If they are set incorrectly, you cannot transfer files between NEs and eSight properly.

### Context



#### NOTE

You can start only the eSight FTP service to ensure that the backup and restore functions are normal.

The default username of FTP is admin and password is Changeme123.

The default path where transfer-in files are stored is **eSight installation directory**/AppBase/var/runtime.center/data/ftp.

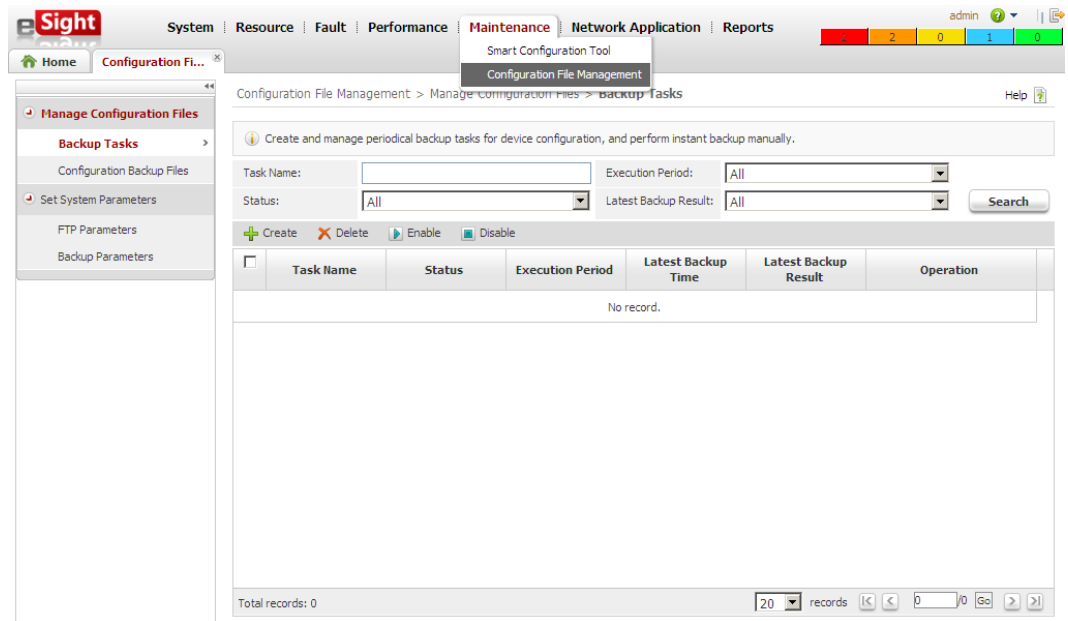
The default FTP type is **FTP**. The system supports FTP and SFTP.

The default FTP port is **21**, and the default SFTP port is **31022**.

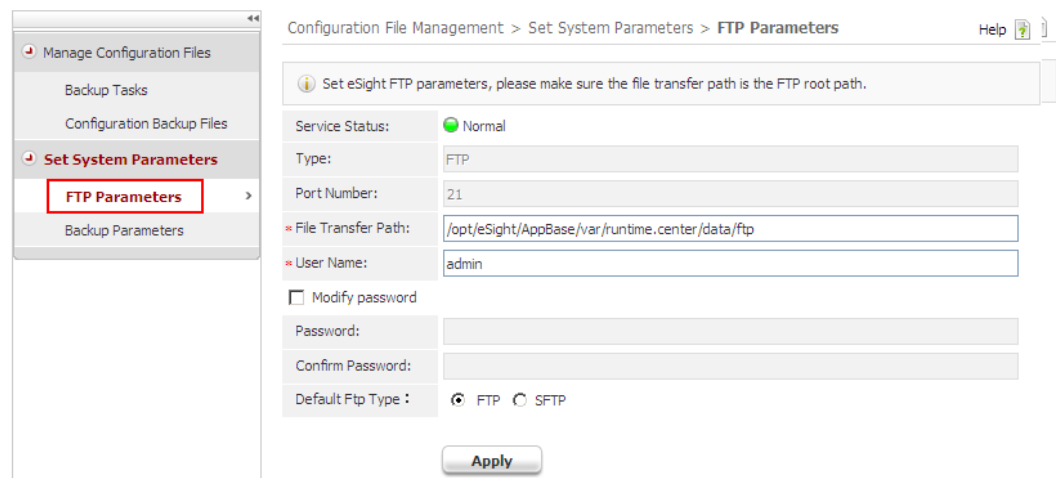
### Procedure

**Step 1** Choose **Maintenance > Configuration File Management**.



**Figure 12-2** Configuration File Management

**Step 2** In the navigation tree on the left, choose **Set System Parameters** > **FTP Parameters**.

**Figure 12-3** FTP Parameters

**Step 3** Set the FTP parameters and click **Apply**.

----End

## Follow-up Procedure

| Operation                  | Procedure                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------|
| Batch change the FTP type. | 1. In the navigation tree, choose <b>Set System Parameters</b> > <b>Configuration Backup Files</b> . |

| Operation | Procedure                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <ol style="list-style-type: none"><li>2. Select one or more pieces of data.</li><li>3. Click <b>Ftp Type</b> and select the FTP type.</li></ol> |

## 12.3 Backing Up NE Configuration Files

You can back up NE configuration files to the eSight server to avoid NE data damage or loss due to upgrade, rollback, or other exceptions.

### 12.3.1 Backing Up NE Configuration Files Automatically

eSight can automatically and periodically back up NE configuration files using backup tasks.

#### 12.3.1.1 Creating a Backup Task

You can create a backup task for a type of NEs.

#### Prerequisites

eSight communicates with NEs normally.

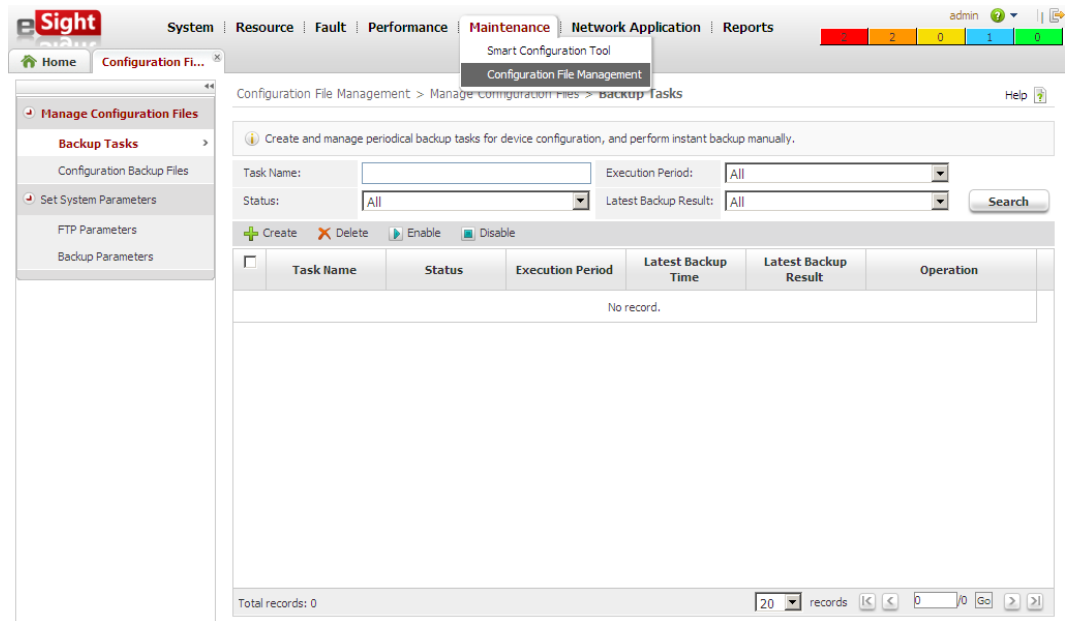
The FTP service is configured and started. For details on how to configure the FTP service, see [12.2 Setting FTP Parameters](#).

For the user-defined device, the Telnet parameters on eSight and the NE are set to be the same.

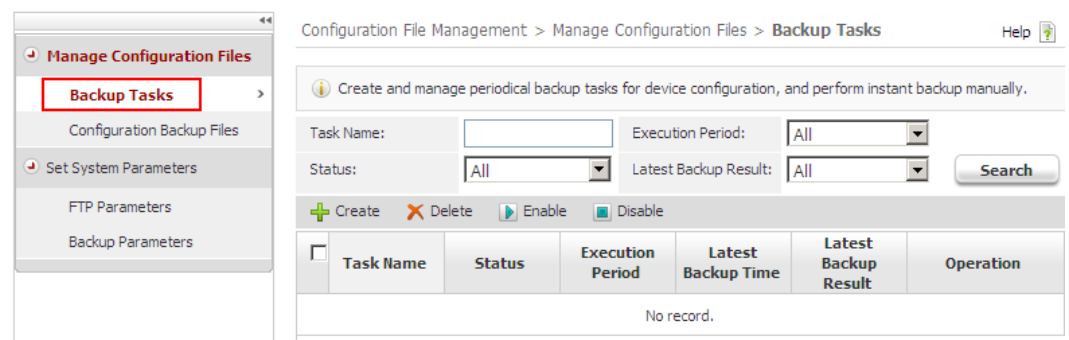
SNMP write permission is set.

#### Procedure

**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-4** Configuration File Management

**Step 2** Choose **Manage Configuration Files > Backup Tasks** from the navigation tree on the left.

**Figure 12-5** Backing Up Tasks

**Step 3** Click **Create** to set backup task parameters.

**Figure 12-6** Creating Backup Task

Configuration File Management > Manage Configuration Files > Backup Tasks > **Create Backup Task**

| * Task name:              | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |                |                          |             |            |             |            |  |  |  |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------|--------------------------|-------------|------------|-------------|------------|--|--|--|
| Task Description:         | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |                |                          |             |            |             |            |  |  |  |
| * Executed At:            | Daily                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 00         | Hour 00 Minute |                          |             |            |             |            |  |  |  |
| * Save Even If No Update: | <input checked="" type="radio"/> No <input type="radio"/> Yes <div>Save configuration file if no updates since last save.</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |                |                          |             |            |             |            |  |  |  |
| * Apply to Device:        | <div> <input checked="" type="button"/> Add Device           <input type="button"/> Delete Device           <input type="button"/> Delete All         </div> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Device Name</th> <th>IP Address</th> <th>Device Type</th> </tr> </thead> <tbody> <tr> <td colspan="4">No record.</td> </tr> </tbody> </table> <div>           Total records: 0           <div>20 records</div> <div> <input type="button"/> &lt;             <input type="button"/> &lt;&lt;             <input type="button"/> &gt;&gt;             <input type="button"/> &gt;             <input type="button"/> Go             <input type="text"/> / 0           </div> </div> |            |                | <input type="checkbox"/> | Device Name | IP Address | Device Type | No record. |  |  |  |
| <input type="checkbox"/>  | Device Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | IP Address | Device Type    |                          |             |            |             |            |  |  |  |
| No record.                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |                |                          |             |            |             |            |  |  |  |

OK
  Cancel

**Step 4** Click **Add Device** next to **Apply to Device**, select a device, and click **OK** to apply the backup task to the device.

**Figure 12-7** Adding Device

| <input type="checkbox"/> | Device Name         | IP Address    | Device Type      |
|--------------------------|---------------------|---------------|------------------|
| <input type="checkbox"/> | AR 1220-10          | 10.137.59.10  | AR 1220          |
| <input type="checkbox"/> | AR2240_2200         | 10.137.59.220 | AR2240           |
| <input type="checkbox"/> | S5700-52C-PWR-EI-78 | 10.137.59.78  | S5700-52C-PWR-EI |
| <input type="checkbox"/> | S93                 | 10.137.61.37  | S9312            |
| <input type="checkbox"/> | VASP_204            | 10.137.59.204 | SPU              |
| <input type="checkbox"/> | WLAN_58             | 10.137.59.58  | SPU              |
| <input type="checkbox"/> | ar 1220_20          | 10.137.59.208 | AR 1220VW        |
| <input type="checkbox"/> | gugan_S7703_15      | 10.137.59.15  | S7703            |
| <input type="checkbox"/> | gugan_S7703_16      | 10.137.59.16  | S7703            |

Total records: 12    20 records    1 / 1    Go

Select All    OK    Cancel

**Step 5 Optional:** Select a device in the **Apply to Device** pane as required and click **Delete Device** to cancel the application of the backup task.

**Step 6** Click **OK**.

----End

### 12.3.1.2 Enabling a Backup Task

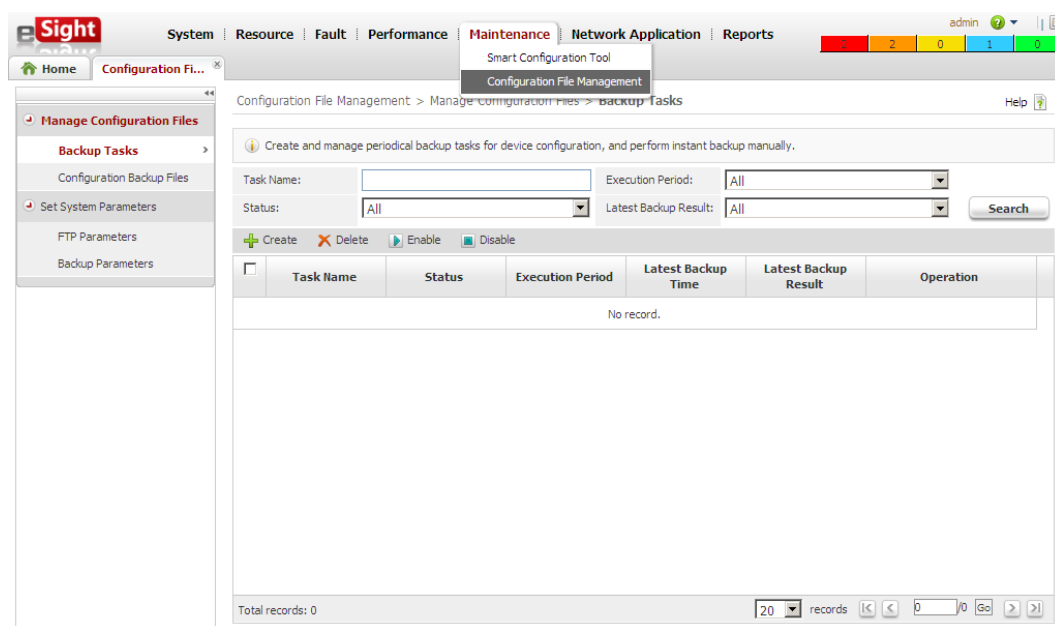
When a configuration file backup task is disabled, you must enable the backup task for execution.

#### Prerequisites

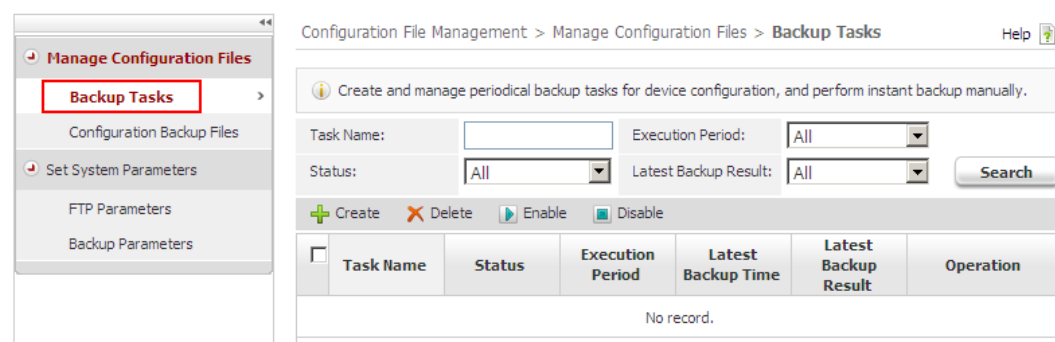
SNMP write permission is set.

#### Procedure

**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-8** Configuration File Management

**Step 2** Choose **Manage Configuration Files > Backup Tasks** from the navigation tree on the left.

**Figure 12-9** Backing Up Tasks

**Step 3** Set **Status** to **Disable** and click **Search**.

**Step 4** Select a backup task and click **Enable**.

----End

### 12.3.1.3 Maintaining a Backup Task

You can browse and maintain a backup task as required.

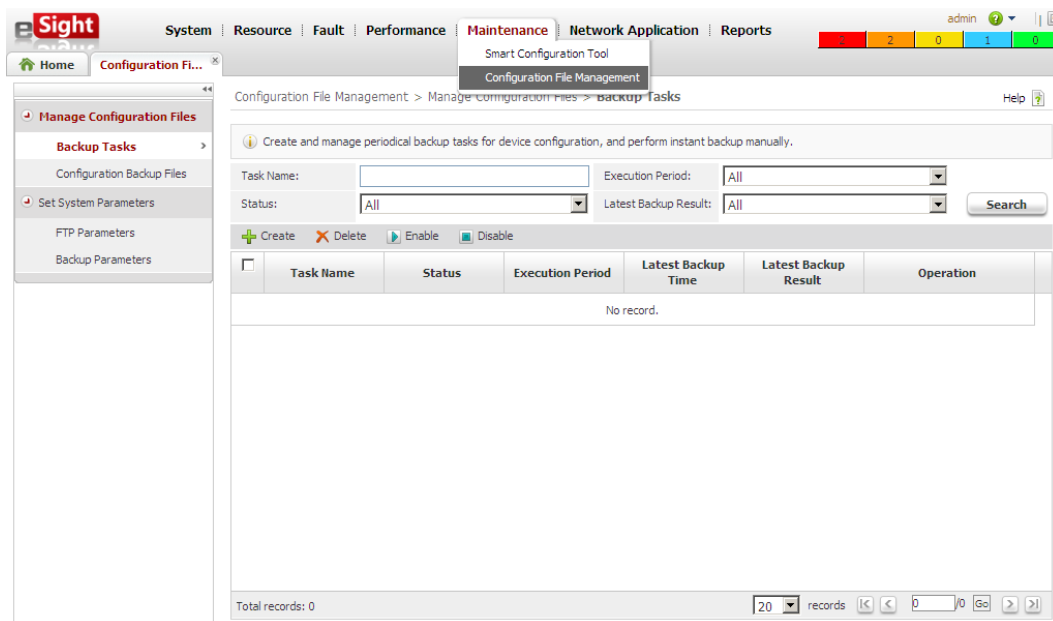
#### Prerequisites

SNMP write permission is set.

## Procedure

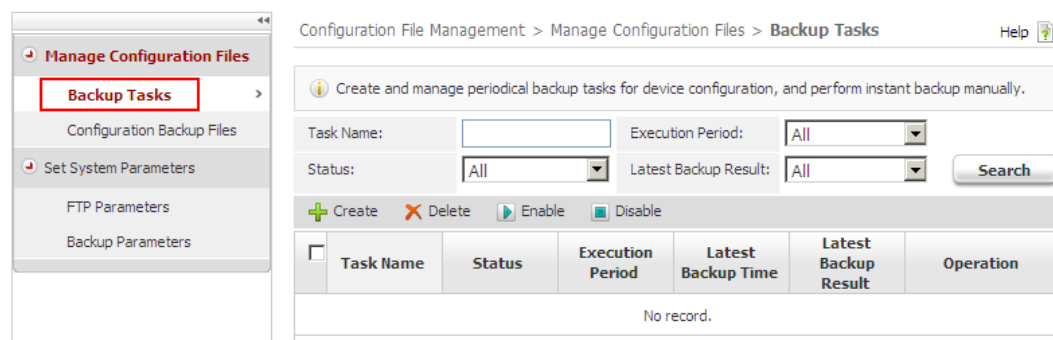
**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-10** Configuration File Management



**Step 2** Choose **Manage Configuration Files > Backup Tasks** from the navigation tree on the left.

**Figure 12-11** Backing Up Tasks



**Step 3** Set filter parameters at the top of the pane and click **Search**.

**Step 4** **Optional:** If **Latest Backup Result** is **Failure** or **Partially successful**, click **Failure** or **Partially successful** to view backup records. After faults are rectified, select the device and click **Back Up**.

**Step 5** **Optional:** Perform the following operations as required:

- In a backup task, click  to modify its parameters.
- In a backup task, click  to start backup.

- Select a backup task and click **Disable** to disable it.
- Select a backup task and click **Delete** to delete it.

----End

## 12.3.2 Backing Up NE Configuration Files Manually

You can back up NE configuration files manually for instant backup.

### Prerequisites

eSight communicates with NEs normally.

The FTP service is configured and started. For details on how to configure the FTP service, see [12.2 Setting FTP Parameters](#).

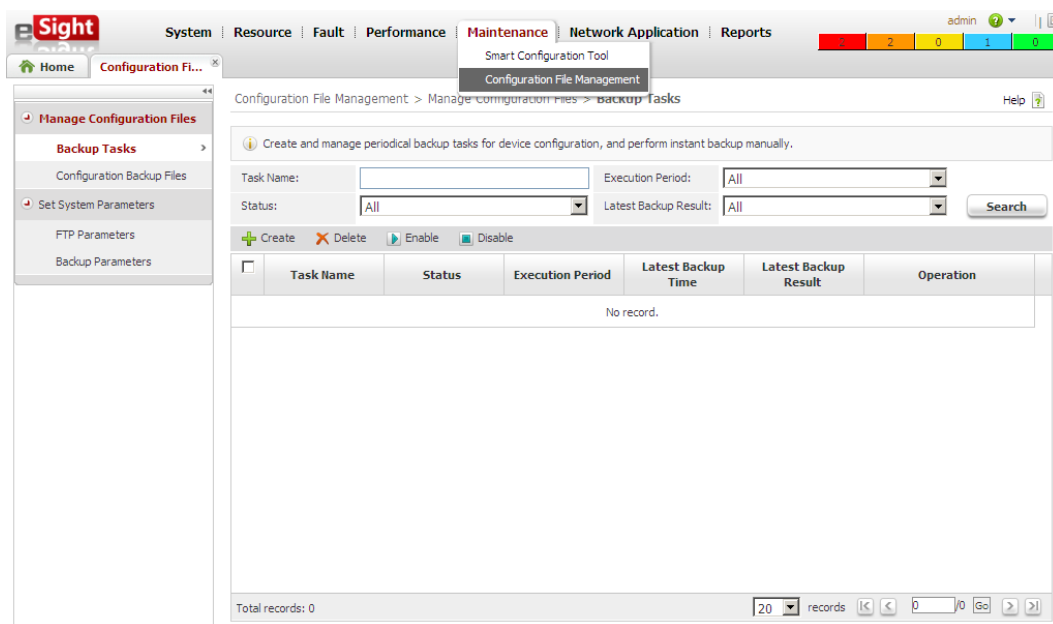
The Telnet parameters on eSight and the NE are set to be the same.

SNMP write permission is set.

### Procedure

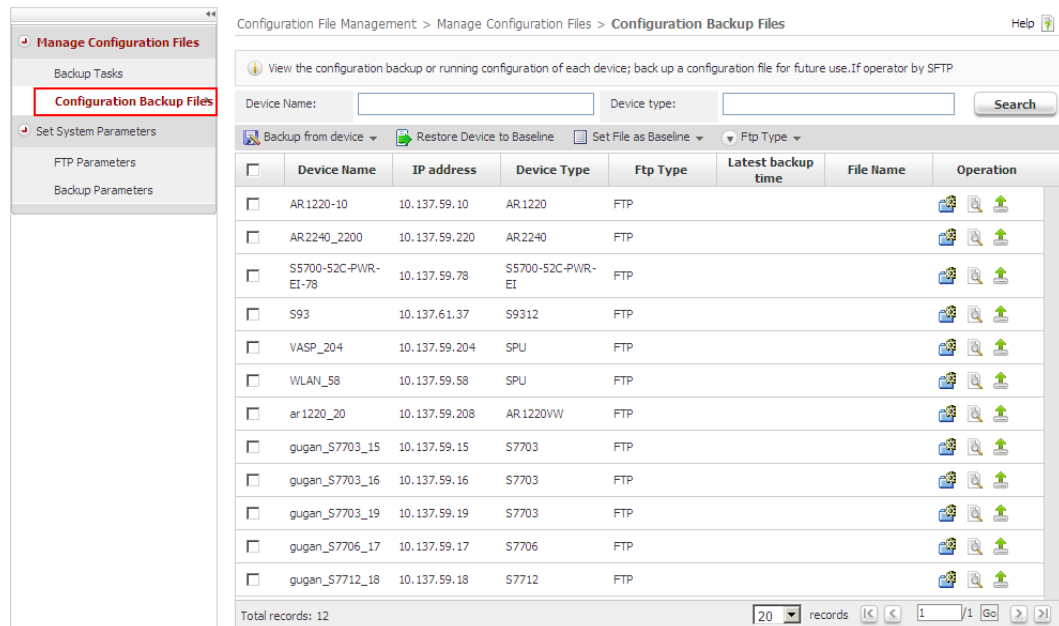
**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-12** Configuration File Management



**Step 2** In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.



**Figure 12-13** Configuration Backup Files

**Step 3** Select one or more devices and choose **Backup from device > Backup Select** to back up the device information; If you want to back up all devices, choose **Backup from device > Backup All**. If you set search criteria, only the devices meeting the search criteria can be backed up.

----End

## Result

When the configuration file used by an NE is the same as the backup configuration file, eSight remains the configuration file in use and discards the backup configuration file by default.

When the configuration file used by an NE is different from each backup configuration file and the number of backup configuration files reaches the maximum, eSight discards the earliest non-baseline configuration file by default.

## 12.4 Managing NE Configuration Files

This topic describes common operations for managing NE configuration files.

### 12.4.1 Viewing an NE Configuration File

This topic describes how to view a backup NE configuration file and a configuration file that is in use.

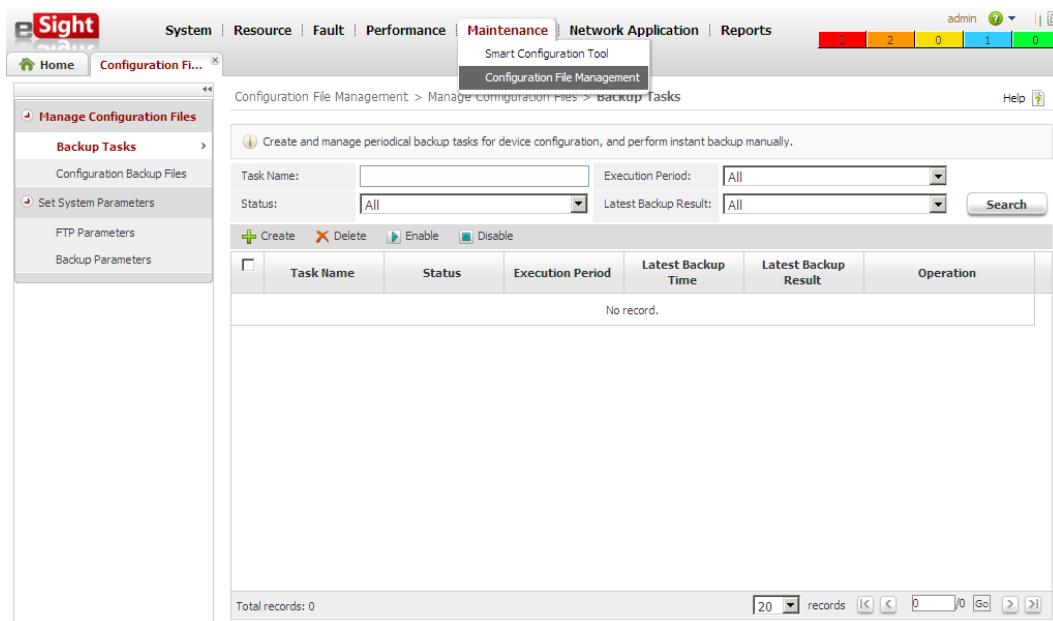
## Prerequisites

A backup file is in .cfg format.

## Procedure

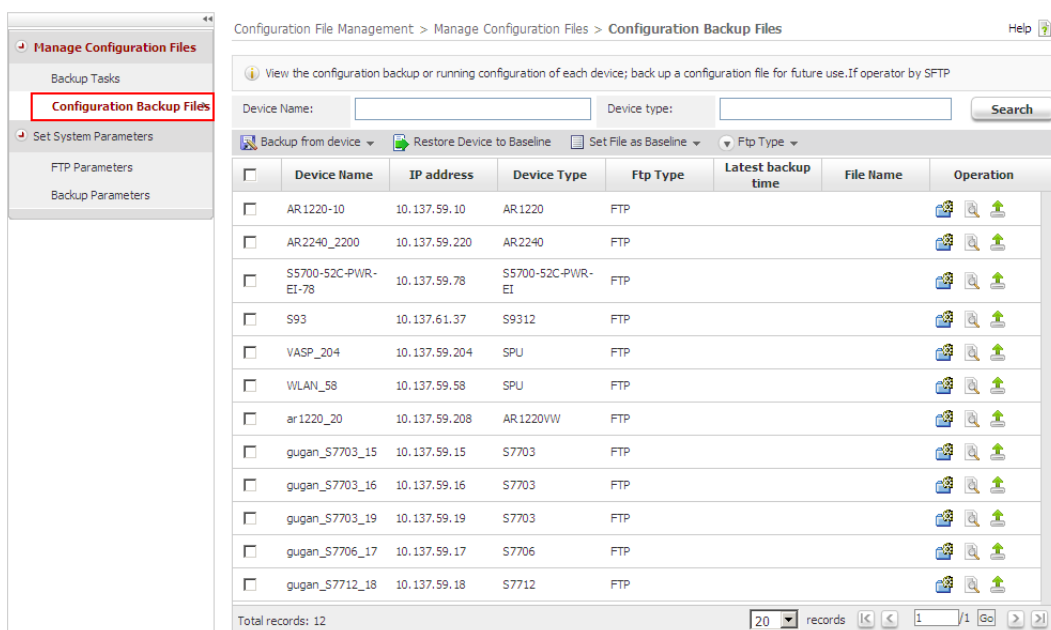
**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-14** Configuration File Management



**Step 2** In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.

**Figure 12-15** Configuration Backup Files



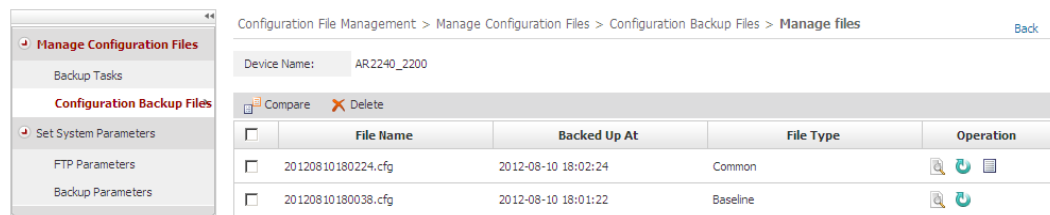
**Step 3** View the configuration file that is being used by the NE. Click  next to an NE.

**Step 4** Click **File Name** to view the latest backup configuration file.

**Step 5** View the backup NE configuration file.

1. Click  on the right to access the NE configuration file management page.

**Figure 12-16** Managing Files



2. Click  next to a configuration file to view details.

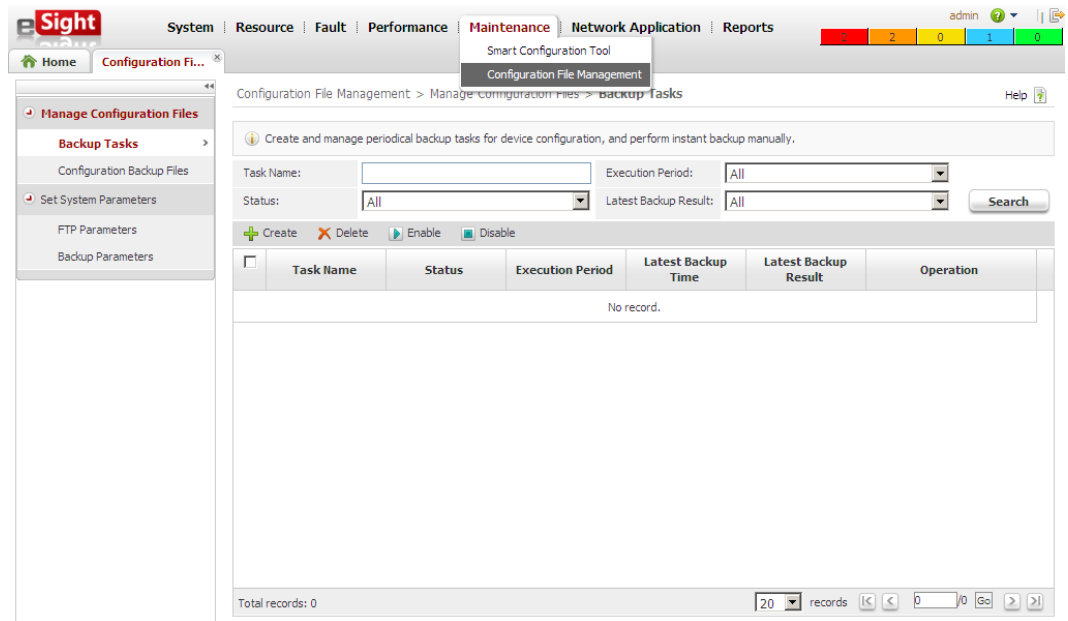
----End

## 12.4.2 Browsing the Backup NE Configuration File List

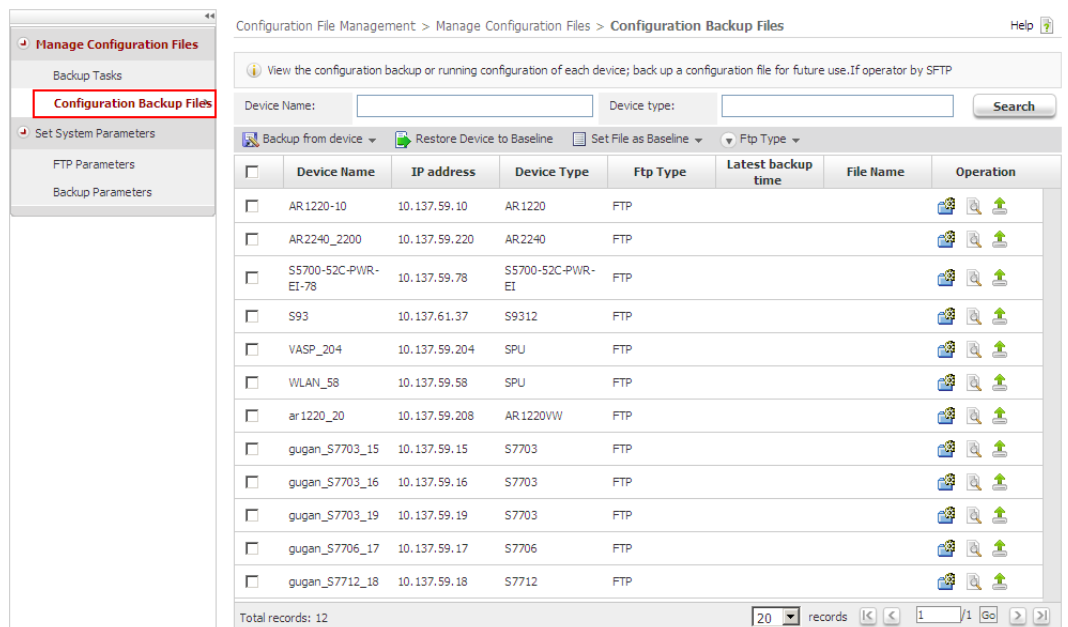
After backing up an NE configuration file, you need to browse all the NE's backup configuration files to verify that the configuration file is backed up successfully.

### Procedure

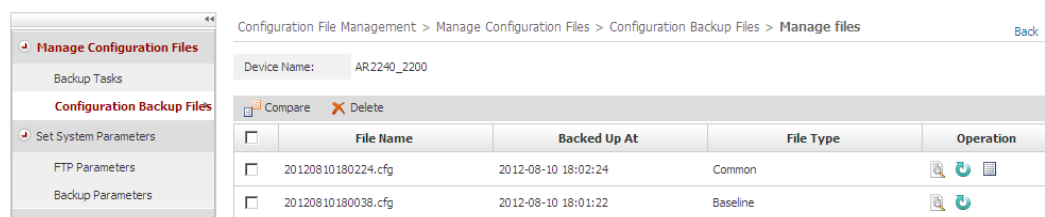
**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-17** Configuration File Management

**Step 2** In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.

**Figure 12-18** Configuration Backup Files

**Step 3** Click  on the right and view backup NE configuration files on the file management page.

**Figure 12-19 Managing Files**

----End

## 12.4.3 Comparing NE Configuration Files

You can know differences between NE configuration files by comparing them.

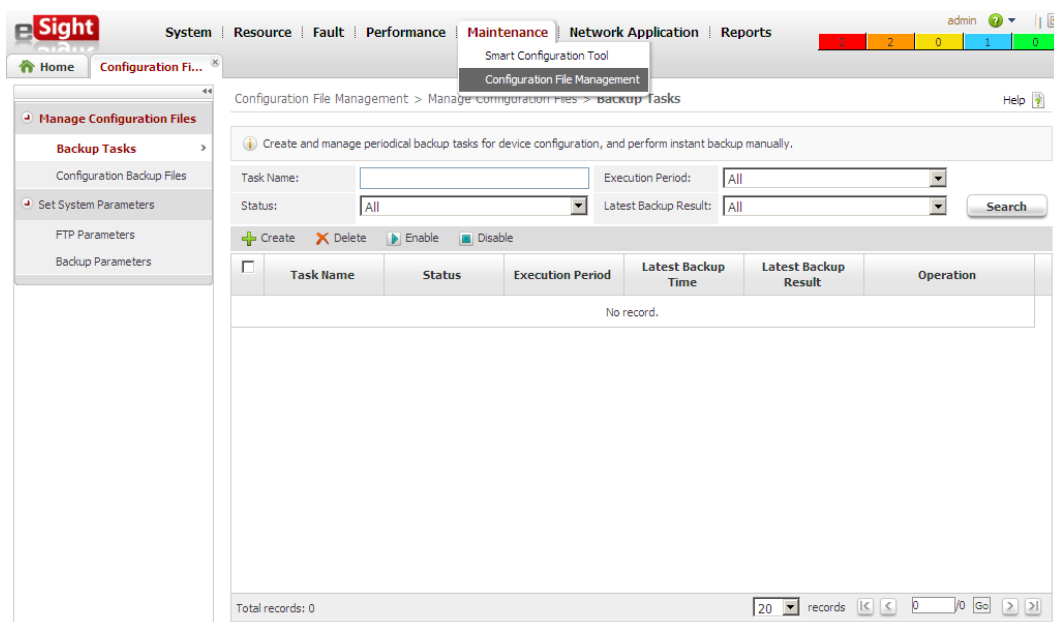
### Prerequisites

An NE has two or more NE configuration files on eSight.

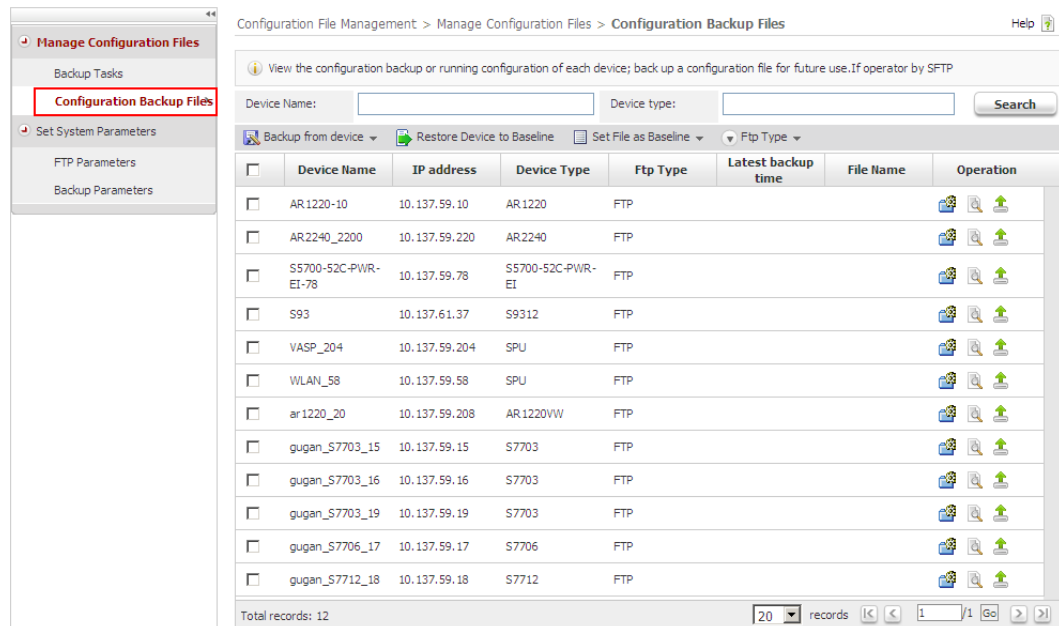
SNMP write permission is set.

### Procedure

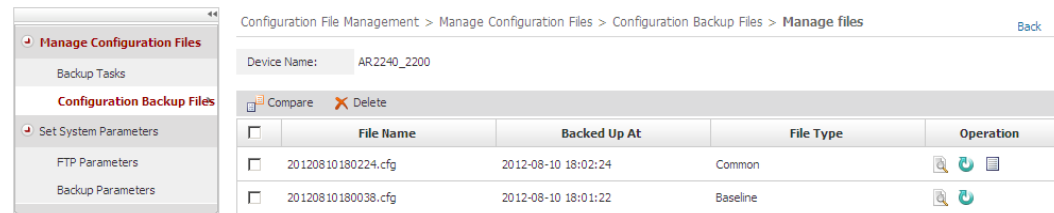
**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-20 Configuration File Management**

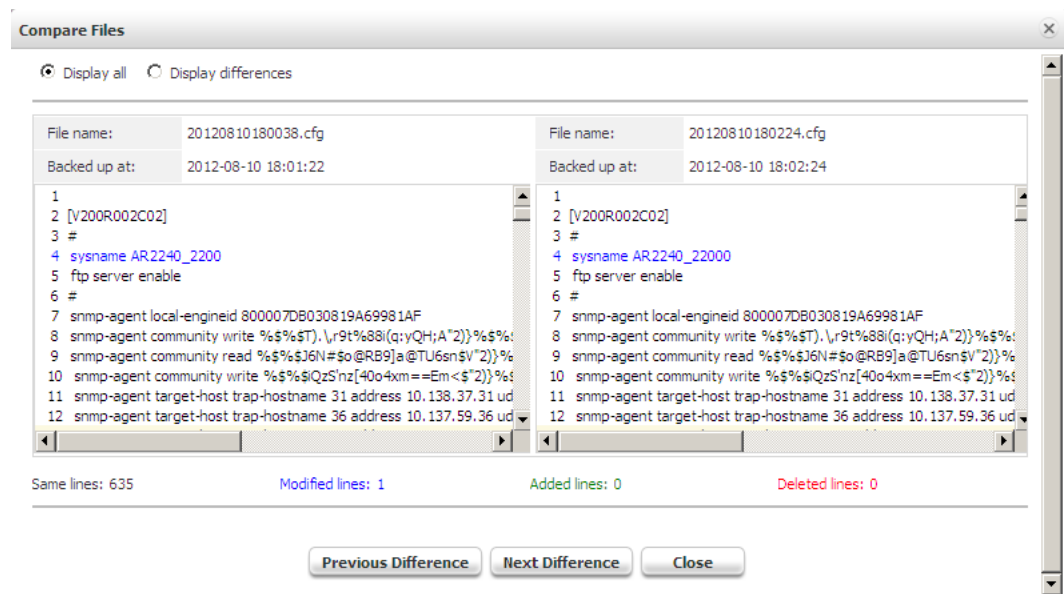
**Step 2** In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.

**Figure 12-21** Configuration Backup Files

**Step 3** Click  on the right to access the NE configuration file management page.

**Figure 12-22** Managing Files

**Step 4** Select two configuration files and click **Compare** to view the comparing result.

**Figure 12-23** Comparing Files

- Select **Display all** or **Display differences** to customize result displaying.
- In the lower part of the page, view **Same lines**, **Modified lines**, **Added lines**, and **Deleted lines** to find differences between the two configuration files.
- Click **Previous Difference** or **Next Difference** to highlight the previous or next difference.

----End

## 12.4.4 Setting NE Configuration Files to the Baseline File

After a configuration file that is being used by an NE is backed up to eSight, you can set the NE configuration file to the baseline file for subsequent file restore.

### Prerequisites

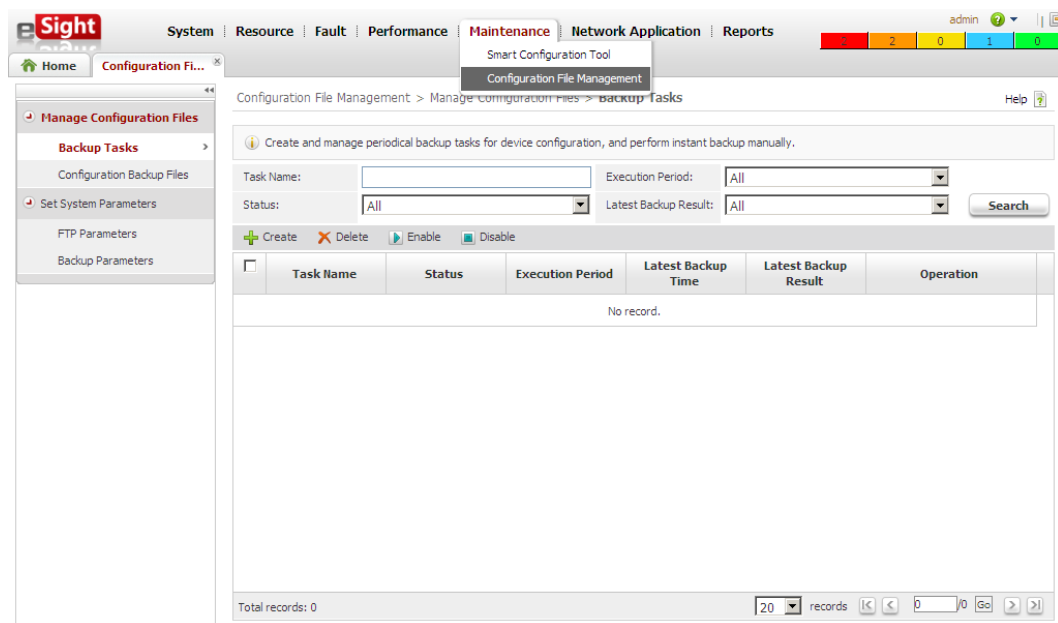
The NE configuration file is backed up to eSight successfully.

### Context

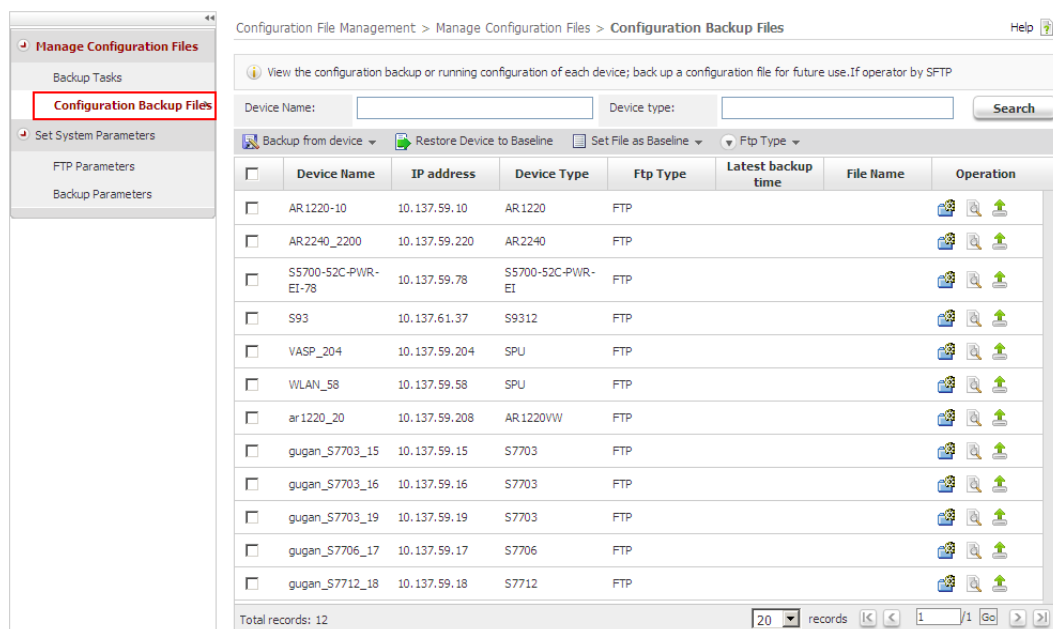
By default, the firstly backed up NE configuration file is the baseline file. Each NE has only one baseline file.

### Procedure

**Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-24** Configuration File Management

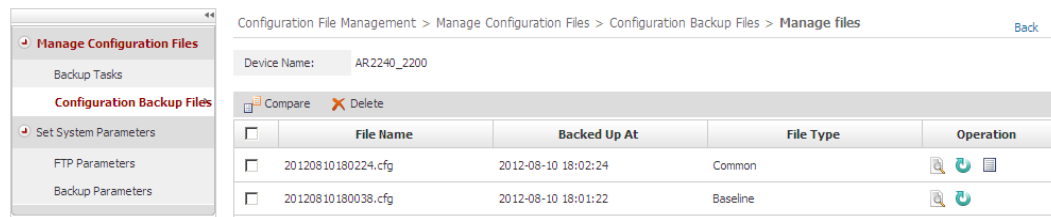
**Step 2** In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.

**Figure 12-25** Configuration Backup Files

**Step 3** Set an NE configuration file to the baseline file.

1. Click  on the right to access the NE configuration file management page.

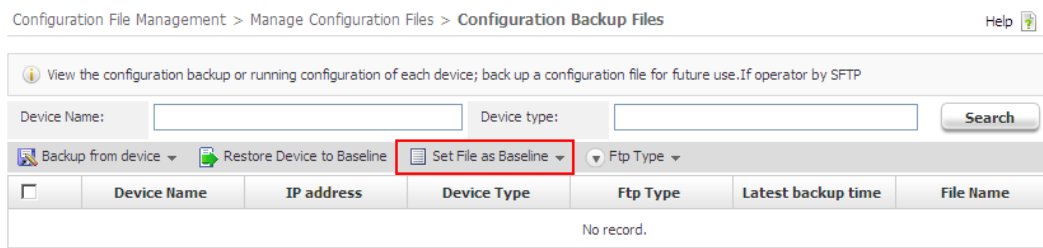


**Figure 12-26 Managing Files**

- Click next to the configuration file. The value of **File Type** is changed to **Baseline**, indicating that the configuration file is set to the baseline file successfully.

**Step 4 Optional:** Set the latest backup configuration files on NEs to baseline files in batches.

- Select multiple NEs and click **Set File as Baseline**.

**Figure 12-27 Setting File as Baseline**

- If the operation fails or partially fails, you can click **Details** in the **Prompt** dialog box that is displayed to view the cause.
- In the **Prompt** dialog box that is displayed, click **OK**.

----End

## 12.4.5 Setting the Maximum Number of Backup NE Configuration Files

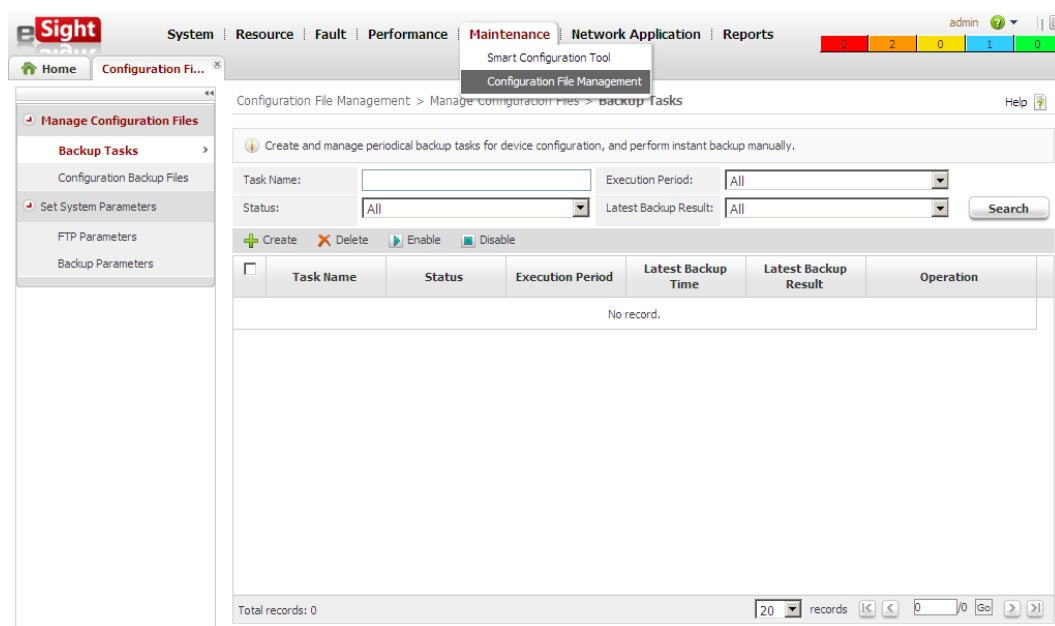
You must set the maximum number of backup NE configuration files to avoid excessive space usage.

### Context

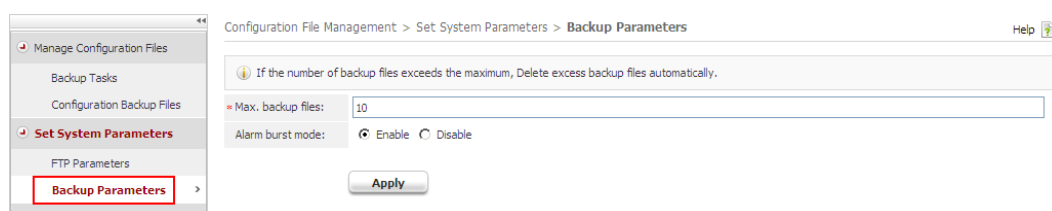
When the number of backup NE configuration files reaches the maximum, eSight deletes the earliest backup NE configuration files by default.

### Procedure

- Step 1** Choose **Maintenance > Configuration File Management**.

**Figure 12-28** Configuration File Management

**Step 2** In the navigation tree on the left, choose **Set System Parameters** > **Backup Parameters**.

**Figure 12-29** Backup Parameters

**Step 3** Set **Max. backup files**.

**Step 4** Enable or disable **Alarm burst mode**.

**NOTE**

- When **Alarm burst mode** is enabled, the configuration file module automatically backs up device configuration files when eSight receives configuration update alarms from devices.
- When **Alarm burst mode** is disabled, the configuration file module does not back up device configuration files when eSight receives configuration update alarms from devices.

**Step 5** Click **Apply**.

----End

## 12.5 Restoring NE Configuration Files

When an NE is faulty, you can upload an NE configuration file to the NE to restore NE configuration data.

## Prerequisites

SNMP write permission is set.

## Context



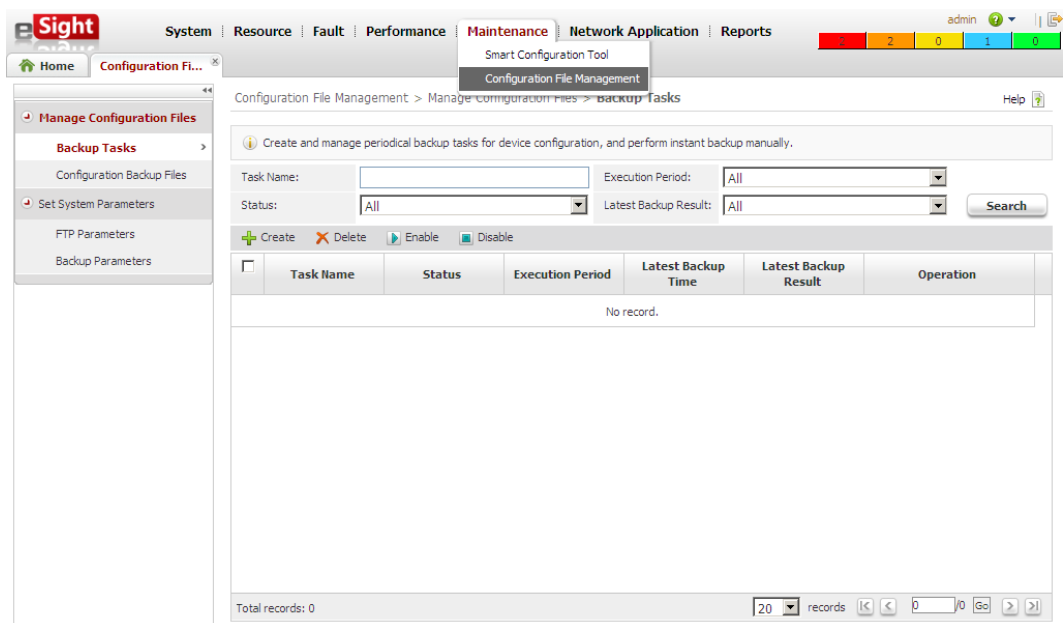
### WARNING

NE configuration file restore may result in service interruption.

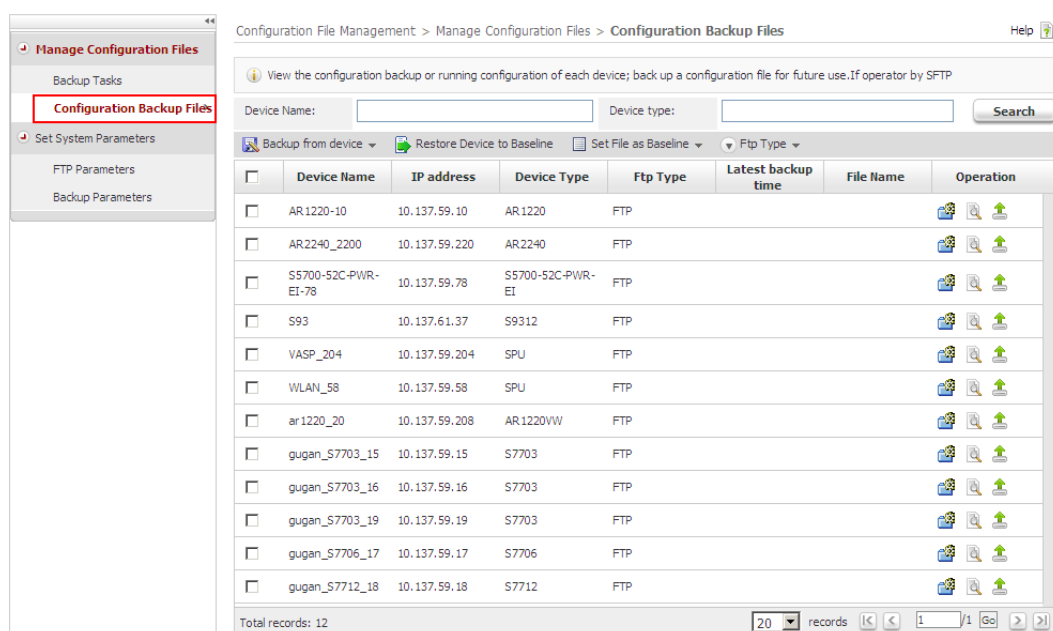
## Procedure

**Step 1** Choose **Maintenance > Configuration File Management**.

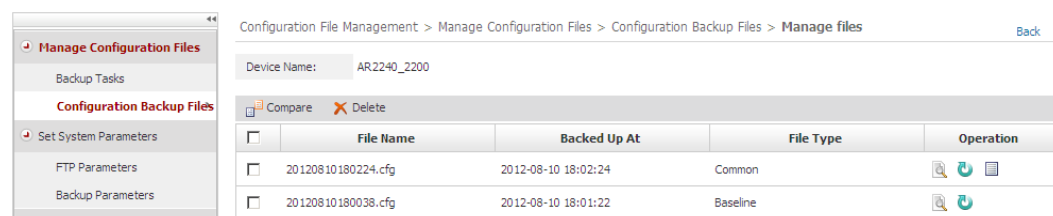
**Figure 12-30** Configuration File Management



**Step 2** In the navigation tree on the left, choose **Manage Configuration Files > Configuration Backup Files**.

**Figure 12-31** Configuration Backup Files**Step 3** Restore an NE configuration file.

1. Click  on the right to access the NE configuration file management page.

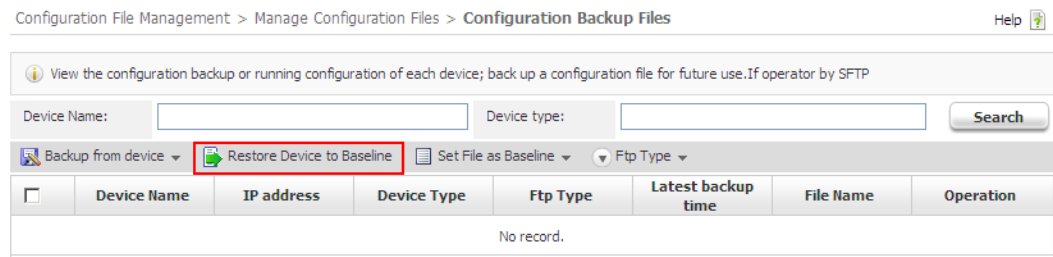
**Figure 12-32** Managing Files

2. Select an NE configuration file and click  to restore NE configuration data.

**Step 4 Optional:** Restore NE configuration files in batches.

1. Select multiple NEs and click **Restore Device to Baseline**.

**Figure 12-33** Restoring Device to Baseline



2. Click **Yes** in the **Prompt** dialog box that is displayed.
3. In the **Prompt** dialog box that is displayed, click **OK**.

----End

# 13 User-Defined Device Management

## About This Chapter

When managing a network containing devices from multiple manufacturers, eSight allows you to customize devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types to reduce operation and maintenance costs.

### [13.1 Overview of user-defined device management](#)

This topic describes the user-defined devices management operations.

### [13.2 User-defined Device Functions](#)

eSight provides a management platform, allowing you to add devices supporting SNMP to eSight. eSight provides complete management capabilities for pre-integrated devices. You can customize user-defined devices (devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types) as required to manage and monitor them on eSight.

### [13.3 Customization Process](#)

To customize a user-defined device, you can perform the following steps for quicker and accurate configuration.

### [13.4 Discovering a User-defined Device](#)

eSight allows you to add a user-defined device to eSight using three methods and manage it on eSight.

### [13.5 Customizing the Vendor Name and Device Type](#)

eSight cannot recognize vendor names and device types of some non-Huawei devices. You must customize the vendor name and device type as required in eSight.

### [13.6 NE Management Capability](#)

### [13.7 Checking the Network Status of User-Defined Devices](#)

You can check the network status of user-defined devices periodically to obtain the status of communication between eSight and user-defined devices in real time.

### [13.8 Invoking the Web NMS of User-Defined Devices](#)

eSight supports invocation of the Web NMS function of user-defined devices. eSight can configure services of user-defined devices on the Web NMS page.

## 13.1 Overview of user-defined device management

This topic describes the user-defined devices management operations.

Figure 13-1 shows the overview of user-defined device management operations. For more details, click the operation in the overview.

**Figure 13-1** Overview of user-defined device management operations

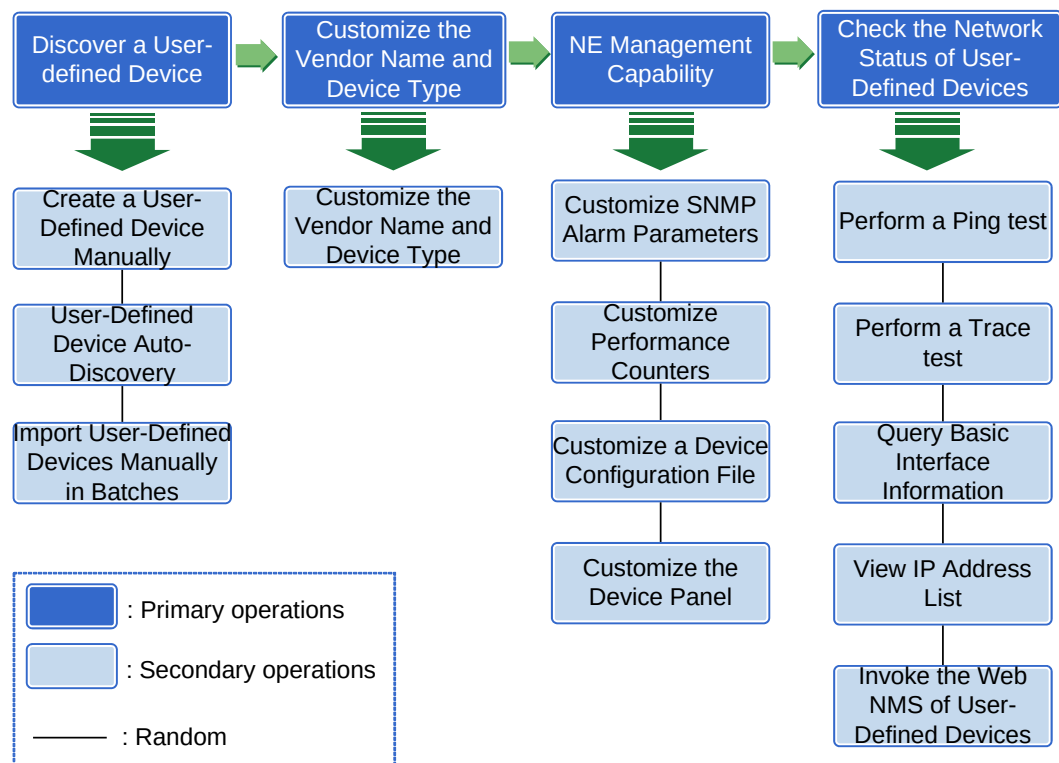


Table 13-1 describes the user-defined device management operations.

**Table 13-1** User-defined device management operations

| Operation                                                          | Description                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Creating a User-Defined Device Manually</a>            | If you want a few different types of NEs to access the eSight, you can create these NEs one by one.                                                                                                                                                                                 |
| <a href="#">User-Defined Device Auto-Discovery</a>                 | The system automatically searches for NEs in a specified network segment based on the specified SNMP and adds the found NEs. When the NEs in a specified network segment will be added, the NE auto-discovery function helps you to perform the operation in batches and save time. |
| <a href="#">Importing User-Defined Devices Manually in Batches</a> | When the system has a lot of managed objects during deployment or device expansion, you can add NEs in batches by using this function.                                                                                                                                              |
| <a href="#">Customizing the Vendor</a>                             | eSight cannot recognize vendor names and device types of                                                                                                                                                                                                                            |

| Operation                                                    | Description                                                                                                                                                                                |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Name and Device Type</a>                         | some third-party devices. You must customize the vendor name and device type as required in eSight.                                                                                        |
| <a href="#">Customizing SNMP Alarm Parameters</a>            | You can customize SNMP alarm parameters in eSight so that non-Huawei devices can report SNMP alarms to eSight.                                                                             |
| <a href="#">Customizing Performance Counters</a>             | This topic describes how to customize performance counters, including device temperature, interface packet error rate, and CPU usage.                                                      |
| <a href="#">Customizing a Device Configuration File</a>      | You must customize restart commands and commands for backing up and restoring configuration files for devices from different vendors as required.                                          |
| <a href="#">Customizing the Device Panel</a>                 | You can upload a device panel photo or draw a device panel in eSight to customize the device panel. This topic describes how to upload a device panel photo to customize the device panel. |
| <a href="#">Performing a Ping Test</a>                       | Perform a Ping test on a user-defined device in the NE manager to check the communication status of eSight and the device.                                                                 |
| <a href="#">Performing a Trace Test</a>                      | Perform a Trace test on a user-defined device in the NE manager to check the communication status of eSight and the device.                                                                |
| <a href="#">Query Basic Interface Information</a>            | eSight supports query of information on an interface.                                                                                                                                      |
| <a href="#">Viewing IP Address List</a>                      | When performing service configuration and network planning, you must query the IP addresses of an NE and the interface. eSight supports query of IP addresses of an NE and the interface.  |
| <a href="#">Invoking the Web NMS of User-Defined Devices</a> | eSight supports invocation of the Web NMS function of user-defined devices. eSight can configure services of user-defined devices on the Web NMS page.                                     |

## 13.2 User-defined Device Functions

eSight provides a management platform, allowing you to add devices supporting SNMP to eSight. eSight provides complete management capabilities for pre-integrated devices. You can customize user-defined devices (devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types) as required to manage and monitor them on eSight.

### Application Scenario

The application scenario of user-defined devices is described as follows:

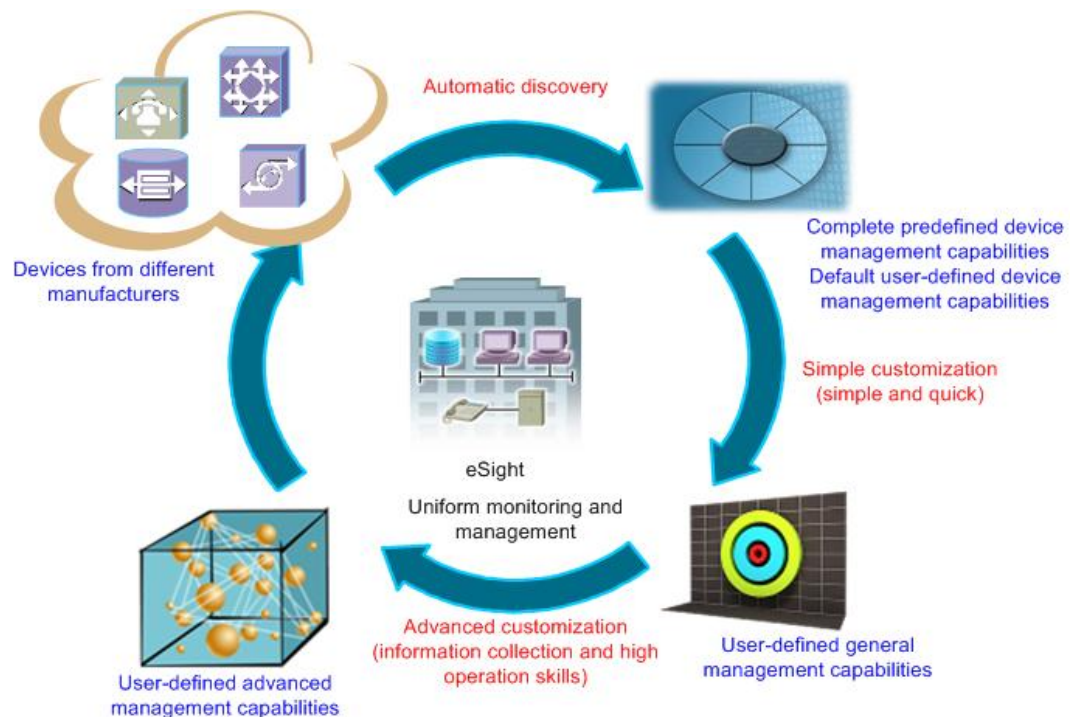
1. Add all devices on the live network to eSight.



2. Manage devices on eSight and determine whether the devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types need customization based on the default functions provided by eSight.
3. Perform simple customization (customize the manufacturer name and device type for a device on eSight). Then eSight has general capabilities to manage the device.
4. Collect related information and perform advanced customization for eSight to have advanced capabilities to manage the device.

Customize other devices from different manufacturers flexibly on eSight for different management capabilities. Then you can manage devices from all manufacturers on eSight.

**Figure 13-2** Application scenario



## Default and Customizable Functions

**Table 13-2** Default and customizable functions

| Device                                      | Default Functions After Discovery                                                                                                                                                                                   | New Functions After Customization                                                                                                    |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Huawei Device, H3C Device, and Cisco Device | <ul style="list-style-type: none"> <li>Basic information</li> <li>Device panel</li> <li>SNMP parameters</li> <li>Public alarm (alarm menu and NE manager)</li> <li>IP address</li> <li>Interface manager</li> </ul> | <ul style="list-style-type: none"> <li>Private alarm</li> <li>Performance indicator</li> <li>Panel</li> <li>Topology icon</li> </ul> |

| Device  | Default Functions After Discovery                                                                                                             | New Functions After Customization                                                                                                                                                                                                                                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"><li>Telnet parameters</li><li>Performance indicator</li><li>Configuration file backup and restore</li></ul> |                                                                                                                                                                                                                                                                                                                                                                                                       |
| Unknown | <ul style="list-style-type: none"><li>Basic information</li><li>Device panel</li><li>SNMP parameters</li></ul>                                | <ul style="list-style-type: none"><li>IP address</li><li>Interface manager</li><li>Telnet parameters</li><li>Alarm</li><li>Performance indicator</li><li>Topology icon</li><li>Configuration file backup and restore</li></ul> <p>After customizing a device, you can back up and restore the device's configuration file. You must restart the device for the configuration file to take effect.</p> |

## User-defined Device Customization Based on Scenario

**Table 13-3** User-defined device customization based on scenario

| Customization Item               | Description                                                                                                                                           | Information to Collect                                                                                                                    | Application Scope                                    |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| General management capabilities  |                                                                                                                                                       |                                                                                                                                           |                                                      |
| IP address                       | Manufacturer name and device type.<br>Workload: 0.2 person/day<br>For details, see <a href="#">13.5 Customizing the Vendor Name and Device Type</a> . | <ul style="list-style-type: none"><li>Manufacturer name (Only <b>Unknown</b> is available.)</li><li>NE type</li><li>NE category</li></ul> | Unknown                                              |
| Interface manager                |                                                                                                                                                       |                                                                                                                                           | Unknown                                              |
| Telnet parameters                |                                                                                                                                                       |                                                                                                                                           | Unknown                                              |
| Topology icon                    |                                                                                                                                                       |                                                                                                                                           | Huawei Device, H3C Device, Cisco Device, and Unknown |
| Advanced management capabilities |                                                                                                                                                       |                                                                                                                                           |                                                      |
| Alarm                            | Alarms for NE monitoring and management<br>Workload: 1 item/hour                                                                                      | <ul style="list-style-type: none"><li>Trap OID of the alarm to add</li><li>VB (MIB node information)</li></ul> <b>NOTE</b>                | Huawei Device, H3C Device, Cisco Device, and Unknown |

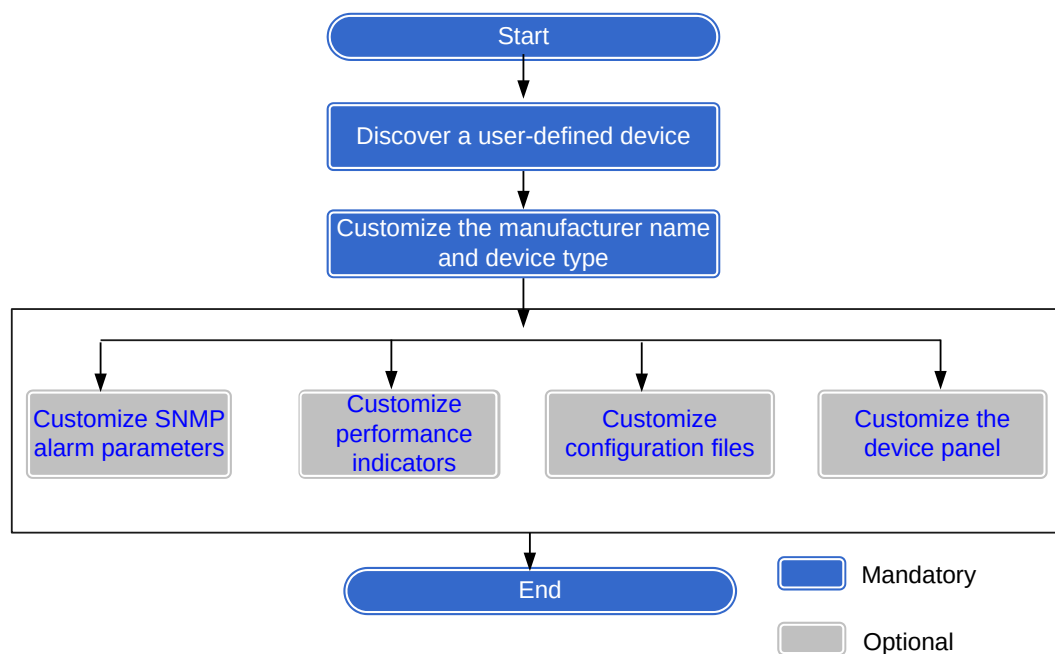
| Customization Item         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Information to Collect                                                                                                                                                                                    | Application Scope                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | For details, see <a href="#">13.6.1 Customizing SNMP Alarm Parameters</a> .                                                                                                                                                                                                                                                                                                                                                                                                                        | Obtain the preceding information from the manufacturer.                                                                                                                                                   |                                                                                                                                                                                                                    |
| Performance Indicator      | <p>Performance indicators supported by devices of the <b>Huawei Device</b>, <b>H3C Device</b>, and <b>Cisco Device</b> types are the same as those of predefined devices from Huawei, H3C, and Cisco respectively.</p> <p>By default, devices of the <b>Unknown</b> type do not support performance indicators. Therefore, you must customize performance indicators for them.</p> <p>Workload: 0.5 item/hour</p> <p>For details, see <a href="#">13.6.2 Customizing Performance Counters</a>.</p> | <ul style="list-style-type: none"><li>Performance indicator OID</li><li>Formula</li><li>Measurement object index</li></ul> <p><b>NOTE</b><br/>Obtain the preceding information from the manufacturer.</p> | <ul style="list-style-type: none"><li>Huawei Device, H3C Device, and Cisco Device: support customization but do not need customization unless otherwise specified.</li><li>Unknown: needs customization.</li></ul> |
| Configuration backup files | <p>Devices only of the <b>Unknown</b> type need customization. After customizing a device, you can back up and restore the device's configuration file. (The displayed operation result may differ from the actual result.)</p> <p>Workload: 0.2 person/day</p> <p>For details, see <a href="#">13.6.3 Customizing a Device Configuration File</a>.</p>                                                                                                                                            | <ul style="list-style-type: none"><li>Backup command</li><li>Restore command</li><li>Restart command</li></ul> <p><b>NOTE</b><br/>Obtain the preceding information from the manufacturer.</p>             | Unknown                                                                                                                                                                                                            |

| Customization Item | Description                                                                                                                                                                                                                                                                                                                  | Information to Collect                                                                                                                                                                               | Application Scope                           |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| NE panel           | <p>Devices of the <b>Huawei Device</b>, <b>H3C Device</b>, <b>Cisco Device</b>, and <b>Unknown</b> types can be displayed on the NE panel. (The displayed device panel may differ from the actual situation.)</p> <p>Workload: 1 person/day</p> <p>For details, see <a href="#">13.6.4 Customizing the Device Panel</a>.</p> | <ul style="list-style-type: none"><li>• Actual appearance</li><li>• Device hierarchy</li><li>• Device's <b>vendortype</b>, which is unique identifier of each device</li><li>• Start index</li></ul> | Huawei Device<br>H3C Device<br>Cisco Device |

## 13.3 Customization Process

To customize a user-defined device, you can perform the following steps for quicker and accurate configuration.

## Customization Flowchart



## 13.4 Discovering a User-defined Device

eSight allows you to add a user-defined device to eSight using three methods and manage it on eSight.

### 13.4.1 Creating a User-Defined Device Manually

If you want a few different types of NEs to access the eSight, you can create these NEs one by one.

#### Prerequisites

You have the operation rights for **Access Resource**.

#### Procedure

**Step 1** Choose **Resource > Add Device** from the main menu.

**Figure 13-3** Adding Device

**Step 2** On the **Add Device** page, configure basic information about the NE to be created and SNMP parameters.

**NOTE**

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. To add an SNMP template, see [3.9 Creating an SNMP Template](#).

**Figure 13-4** Setting SNMP parameters

**Step 3** Click **OK**.

**NOTE**

Click **Apply** to create more NEs.

- If the NE is created successfully, the NE is displayed in the list.
- If the NE cannot be created, the **Error** dialog box is displayed, indicating the reason for the failure. Click **OK** to set the parameters again.

----End

## 13.4.2 User-Defined Device Auto-Discovery

The system automatically searches for NEs in a specified network segment based on the specified SNMP and adds the found NEs. When the NEs in a specified network segment will be added, the NE auto-discovery function helps you to perform the operation in batches and save time.

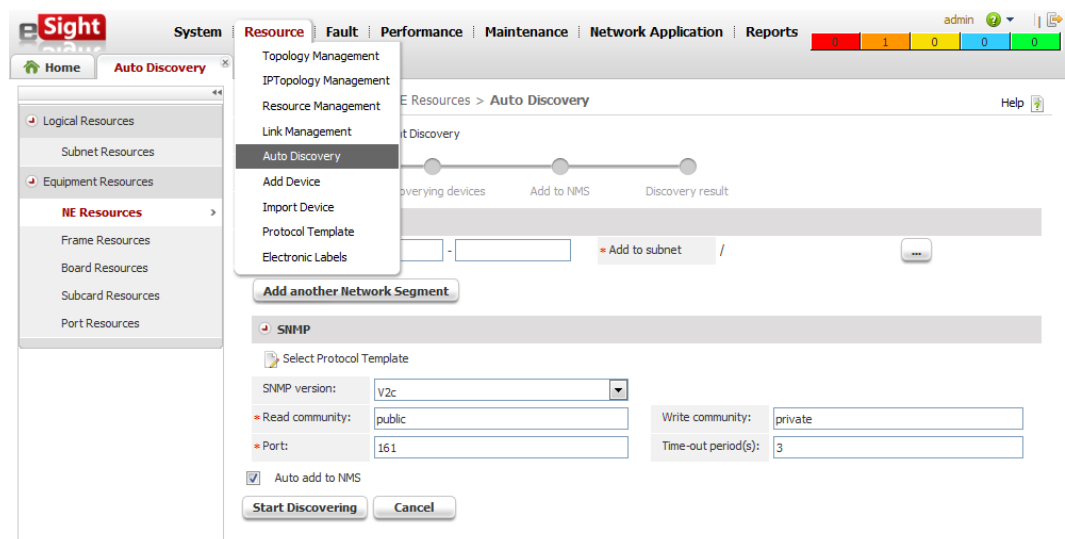
### Prerequisites

- You have the operation rights for **Access Resource**.
- NEs support the SNMP version specified by the eSight.

### Procedure

**Step 1** Choose **Resource > Auto Discovery** from the main menu.

**Figure 13-5** Discovering NEs automatically



**Step 2** On the **Network Segment Discovery** page, set network segment discovery parameters and SNMP parameters.



#### NOTE

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. To add an SNMP template, see [3.9 Creating an SNMP Template](#).

**Figure 13-6** Setting automatic discovery parameters

Set Param Discovering devices Add to NMS Discovery result

**Network Segment**

Network Segment: 10.137.59.11 - 10.137.59.33 \* Add to subnet / ...

Add another Network Segment

**SNMP**

Select Protocol Template

SNMP version: V2c

\* Read community: public Write community: private

\* Port: 161 Time-out period(s): 3

☒ Auto add to NMS

Start Discovering Cancel

**Step 3 Optional:** Select **Auto add to NMS**.

**NOTE**

- If **Auto add to NMS** is selected, the discovered NEs are automatically added. The [Step 5](#) is skipped.
- If **Auto add to NMS** is not selected, you need to execute the [Step 5](#) to add the discovered NEs.

**Step 4** Click **Start Discovering**.

The discovered NEs are displayed in the list.

**NOTE**

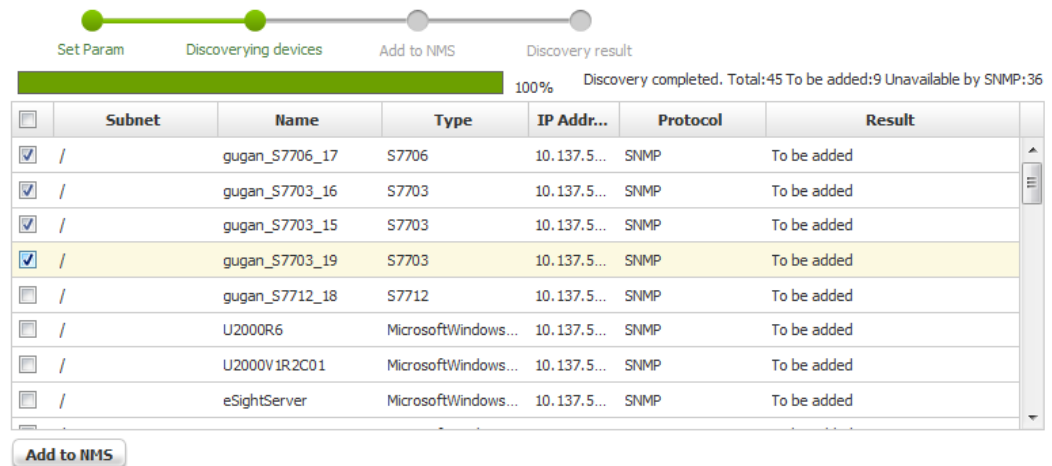
You can click **Stop Discovering** to stop the discover operation.

**Step 5** Select NEs in the list and click **Create**.

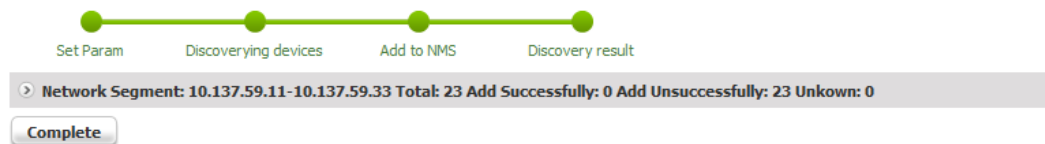
If **Auto add to NMS** is selected, this step is skipped.

- If the NE is created successfully, the **Result** column is **Add success**.
- If the NE fails to be created, the **Result** column displays **Add fail** and the reason for the failure.



**Figure 13-7** Adding the NEs

**Step 6** Click **Show Discovery Result** to view details about NE addition.

**Figure 13-8** Discovery Result

**Step 7** Click **Complete**.

----End

### 13.4.3 Importing User-Defined Devices Manually in Batches

When the system has a lot of managed objects during deployment or device expansion, you can add NEs in batches by using this function.

#### Prerequisites

You have the operation rights for **Access Resource**.

#### Context

Manually importing NEs is to add NEs by importing the .xls template.

Table 13-4 describes every fields in Excel template.

**Table 13-4** Excel template

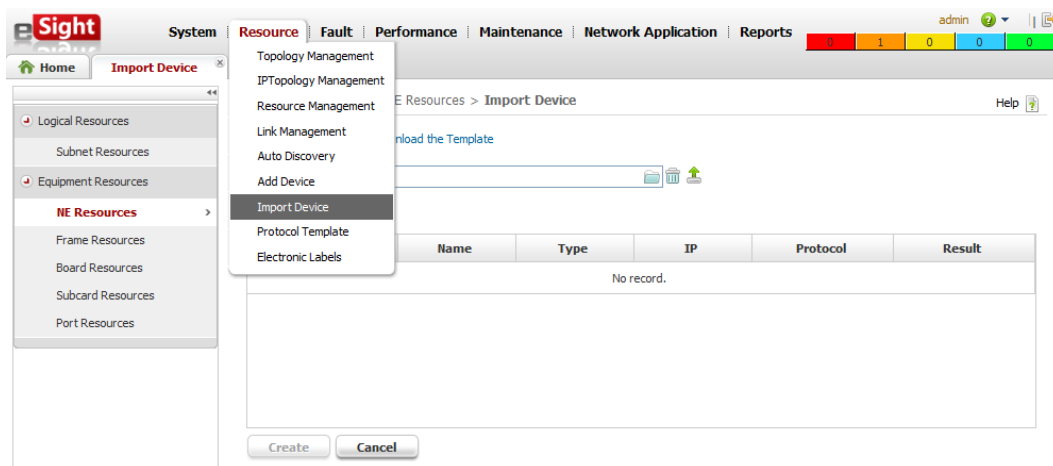
| Field name | Description                          |
|------------|--------------------------------------|
| IP Address | For example, <b>10.123.124.115</b> . |

| Field name       | Description                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------|
| NE Name          | 1 to 128 characters. The NE name cannot contain the following characters # % & + / ; < = > ? \.            |
| Protocol Type    | Set to <b>SNMP</b> .                                                                                       |
| Protocol Version | The protocol version must be the same as the SNMP protocol version in the device, for example, <b>V1</b> . |
| Port             | This parameter must be the same as the port number of the SNMP protocol, for example, <b>161</b> .         |
| Read Community   | This parameter must be the same as the read community of the SNMP protocol, for example, <b>public</b> .   |
| Write Community  | This parameter must be the same as the write community of the SNMP protocol, for example, <b>private</b> . |

## Procedure

**Step 1** Choose **Resource > Import Device** from the main menu.

**Figure 13-9** Importing Device



**Step 2** Click  and download the **.xls** template to the local computer.

**Step 3** Open the template, fill in NE information, and save the template.

**Step 4** On the **Import Device** page, click  next to **Upload Resource File** and select the saved Excel file.

If you want to import other files, click  to clear the selected files.

**Step 5** Click  to upload a file.

NE information and NE check results are displayed on the right of the page. If is **Result** empty, NE check succeeds.

**Figure 13-10** Uploading the file

Template to download: [Download the Template](#)

\* Upload Resource File: C:\SZ\_B.xls  

Select Subnet

| <input checked="" type="checkbox"/> | Subnet                                                                                  | Name | Type | IP           | Protocol | Result |
|-------------------------------------|-----------------------------------------------------------------------------------------|------|------|--------------|----------|--------|
| <input checked="" type="checkbox"/> |  /AA/B |      |      | 10.137.61.32 | SNMP     |        |

Create Cancel

**Step 6** Select an NE and click **Create**.

The system starts to import the NEs.

- If the NE is created successfully, the **Result** column is **The resource is created successfully**.
- If the NE cannot be created, the reason for the failure is displayed in the **Result** column. You can attempt to resolve the problem and import NEs again based on the failure reason. If the fault persists, contact the technical support personnel.

**Figure 13-11** Result

Template to download: [Download the Template](#)

\* Upload Resource File:   

100%

Select Subnet

| <input checked="" type="checkbox"/> | Subnet                                                                                    | Name | Type  | IP           | Protocol | Result                                |
|-------------------------------------|-------------------------------------------------------------------------------------------|------|-------|--------------|----------|---------------------------------------|
| <input checked="" type="checkbox"/> |  /AA/B | S93  | S9306 | 10.137.61.32 | SNMP     | The resource is created successfully. |

Create Cancel

----End

## 13.5 Customizing the Vendor Name and Device Type

eSight cannot recognize vendor names and device types of some non-Huawei devices. You must customize the vendor name and device type as required in eSight.

## Procedure

**Step 1** Access the **Vendor Information** page.

1. Choose **Resource > Resource Management**.
2. In the navigation tree on the left, choose **Equipment Resources > NE Resources**, click **Name** in device list, the page for configuring the basic device information is displayed.
3. On the **Basic Information** tab page, click **User-defined device type** next to **Model**. The **Vendor Information** page is displayed.

**Figure 13-12** User-defined device type

The screenshot shows a web interface for configuring a device. At the top, there is a toolbar with icons for Modify, Refresh, Telnet, Ping, Trace, and Synchronize Device Data. Below the toolbar, the device information is displayed in a table-like format:

|              |                                                   |
|--------------|---------------------------------------------------|
| Name:        | H3C_S1626                                         |
| Model:       | Unknown/H3CDevice <b>User-defined device type</b> |
| Host name:   | H3C_S1626                                         |
| IP address:  | 10.137.59.237                                     |
| MAC address: | 3C-E5-A6-BF-AC-E7                                 |

**Step 2** Click **Create**, and customize vendor information in the window that is displayed.

**Figure 13-13** New vendor

The screenshot shows a 'New Vendor' dialog box with the following fields:

- \* Vendor Name:** ZZZ
- Vendor Description:** (empty text area)
- Vendor Phone:** (empty text field)
- Vendor Contact:** (empty text area)

At the bottom of the dialog box, there are two buttons: **OK** and **Cancel**.

**Step 3** Click **OK**. The **Vendor Information** page is displayed.

**Step 4** Select the vendor **ZZZ**, and click **Next**.

**Step 5** Set **NE Type**, **NE Category**, and **Current NE Icon**, and click **Complete**.

**Figure 13-14** Customize a NE type

|                  |                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * NE Type:       | 9000                                                                                                                                                                |
| * Vendor Name:   | ZZZ                                                                                                                                                                 |
| * System OID:    | 1.3.6.1.4.1.25506.1.472                                                                                                                                             |
| * NE Category:   | Switch                                                                                                                                                              |
| Web NMS URL:     |                                                                                                                                                                     |
| Current NE Icon: |   |

**Step 6** In the dialog box indicating operation success, click **OK**.

----End

## Follow-up Procedure

1. Choose **Resource > Resource Management**.
2. In the navigation tree on the left, choose **Equipment Resources > NE Resources**, click a user-defined device in the device list. The page for configuring the basic device information is displayed.
3. Verify that the device type is customized successfully in the **Model**.

## 13.6 NE Management Capability

### 13.6.1 Customizing SNMP Alarm Parameters

You can customize SNMP alarm parameters in eSight so that non-Huawei devices can report SNMP alarms to eSight.

#### Context

You must obtain alarms' trap IDs and MIB node information for locating alarm parameters from the manufacturer.

You can use a tool (for example, MIB Browser) to obtain alarm trap packets. According to the packet structure, you can obtain parameters related to alarm customization.

SNMPv1 packet structure:

```
Simple Network Management Protocol
Version: 1 (0)
Community: public
PDU type: TRAP-V1 (4)
Enterprise: 1.3.6.1.4.1.2011.2.87.7.2 (SNMPv2-SMI::enterprises.2011.2.87.7.2) — Enterprise ID
Agent address: 10.137.127.3 (10.137.127.3)
Trap type: LINK DOWN (2) — Generic
Specific trap type: 0 — Specific
Timestamp: 84854133
Object identifier 1: 1.3.6.1.2.1.2.2.1.1.201332352 (IF-MIB::ifIndex.201332352)
Value: INTEGER: 201332352
Object identifier 2: 1.3.6.1.2.1.2.2.1.7.201332352 (IF-MIB::ifAdminStatus.201332352)
Value: INTEGER: up(1)
Object identifier 3: 1.3.6.1.2.1.2.2.1.8.201332352 (IF-MIB::ifOperStatus.201332352)
Value: INTEGER: down(2)
Object identifier 4: 1.3.6.1.2.1.2.2.1.2.201332352 (IF-MIB::ifDescr.201332352)
```

Location  
Parameter OID

SNMPv2 packet structure:

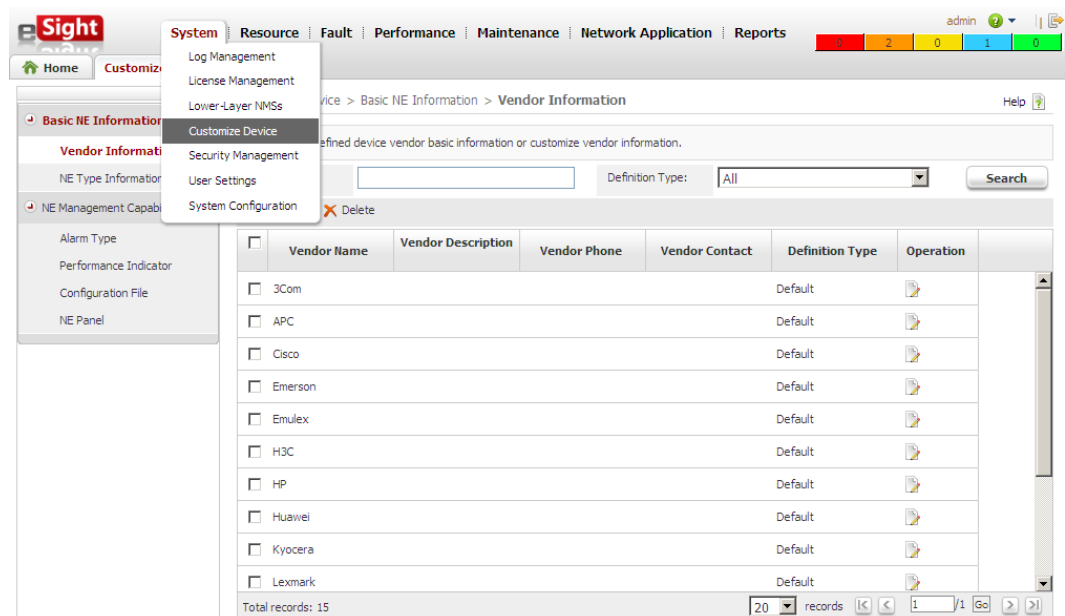
```
Simple Network Management Protocol
Version: 2C (1)
Community: public
PDU type: TRAP-V2 (7)
Request Id: 0x69aadf54
Error Status: NO ERROR (0)
Error Index: 0
Object identifier 1: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
Value: Timeticks: (20118615) 2 days, 7:53:06.15
Object identifier 2: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0) — Alarm OID, unique identifier of an alarm
Value: OID: IF-MIB::linkDown
Object identifier 3: 1.3.6.1.2.1.2.2.1.1.84609 (IF-MIB::ifIndex.84609)
Value: INTEGER: 84609
Object identifier 4: 1.3.6.1.2.1.2.2.1.7.84609 (IF-MIB::ifAdminStatus.84609)
Value: INTEGER: down(2)
Object identifier 5: 1.3.6.1.2.1.2.2.1.8.84609 (IF-MIB::ifOperStatus.84609)
Value: INTEGER: down(2)
Object identifier 6: 1.3.6.1.2.1.2.2.1.2.84609 (IF-MIB::ifDescr.84609)
Value: STRING: GigabitEthernet2/0/1
Object identifier 7: 1.3.6.1.2.1.2.2.1.8.84609 (IF-MIB::ifOperStatus.84609)
Value: INTEGER: down(2)
```

Location  
Parameter OID

## Procedure

**Step 1** Choose **System > Customize Device** from the main menu.

**Figure 13-15** Customize Device



**Step 2** In the navigation tree on the left, choose **NE Management Capability > Alarm Type**.

**Figure 13-16** Alarm Type**Step 3** Customize an alarm.

1. On the **Alarm Type** page, click **Create**. The **Create Alarm Type** tab page is displayed.
2. Set the parameters for customizing alarms, and click **OK**.

**Figure 13-17** Creating alarm type**Table 13-5** Parameters for customizing alarms

| Parameter     | Description                                                                                                                                                                                                                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP Version  | SNMP versions supported by eSight, including SNMPv1, SNMPv2c, and SNMPv3. <ul style="list-style-type: none"><li>• Set the alarm OID for devices supporting SNMPv2c or SNMPv3.</li><li>• For devices supporting SNMPv1, set <b>Generic</b>, <b>Specific</b>, and <b>Enterprise ID</b>.</li></ul> |
| Generic       | The combination of <b>Generic</b> , <b>Specific</b> , and <b>Enterprise ID</b> is the unique identifier of an SNMPv1 alarm.                                                                                                                                                                     |
| Specific      |                                                                                                                                                                                                                                                                                                 |
| Enterprise ID |                                                                                                                                                                                                                                                                                                 |
| Alarm OID     | Trap OID supporting                                                                                                                                                                                                                                                                             |

| Parameter     |                         | Description                                                                                                              |
|---------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------|
|               |                         | SNMPv2c, which is the unique identifier of an alarm.                                                                     |
| New Parameter | Location Parameter Name | Name of an alarm location parameter.<br>For example, <b>Port index</b> is used to locate the port that reports an alarm. |
|               | Location Parameter OID  | MIB node of an alarm location parameter.                                                                                 |

**Step 4** Customize a clear alarm.

1. On the **Alarm Type** page, click **Create**. The **Create Alarm Type** tab page is displayed.
2. Set **Vendor Name** to the vendor of a device where an alarm is generated and **Notification Type** to **Recovery alarm**.
3. Click **Select**, select an alarm, and click **OK**.
4. Set **Alarm OID**, and click **OK**.

----End

## Follow-up Procedure

When the user-defined alarm occurs on a device, choose **Fault** > **Current Alarms** to view the alarm information.

## 13.6.2 Customizing Performance Counters

This topic describes how to customize performance counters, including device temperature, interface packet error rate, and CPU usage.

### Context

- User-defined device performance counter group: contains performance counters of devices, for example, device temperature. The monitoring object is each device.
- User-defined interface performance counter group: contains performance counters of interfaces, for example, interface traffic. The monitoring object is interface.
- Group of performance counters without specified monitoring objects: indicates private performance counters of devices from different manufacturers. After customizing a performance counter, you must specify the monitoring object for it.

**NOTE**

You must obtain the user-defined performance counter MIB information from manufacturers.

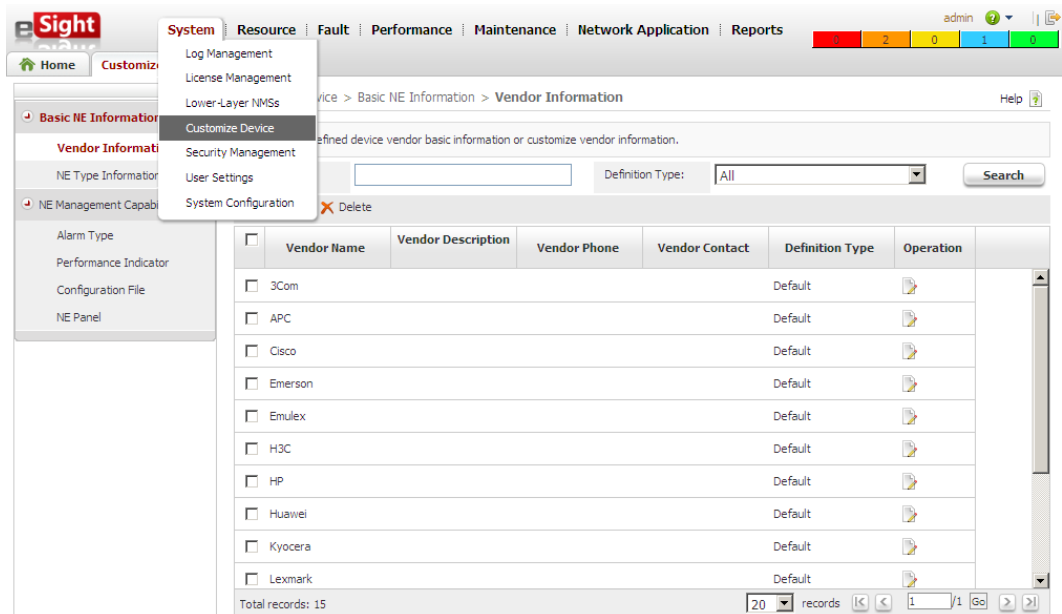


- The performance counter formula is an expression for computing performance counters for the MIB object to be monitored.
- The expression consists of the MIB OID value, and any of the following characters: \$ + - \* / == period ' ( ) When customizing counters for user-defined devices, suffix .0 to the MIB OID. Two \$ characters are used to quote an MIB OID. The single quotation mark (') follows the MIB OID, indicating the last performance counter that a device reports to eSight (the reported performance counter is used for difference calculation). The **period** value indicates the report interval. The symbol == is used for judgment.

## Procedure

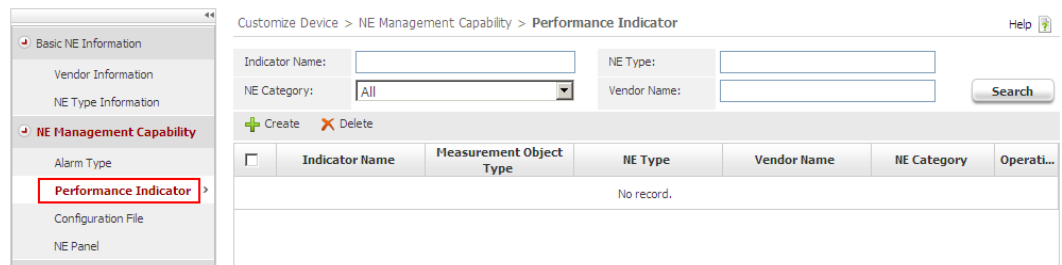
**Step 1** Choose **System > Customize Device** from the main menu.

**Figure 13-18** Customize Device



**Step 2** In the navigation tree on the left, choose **NE Management Capability > Performance Indicator**.

**Figure 13-19** Performance Indicator



**Step 3** Create user-defined devices, user-defined interfaces, and performance counters whose monitoring objects are unspecified.

1. Create user-defined device counters. Click **Create**, set device performance counter parameters on the **Create Performance Indicator** tab page, and click **OK**.

**Figure 13-20** Creating user-defined device counters

|                            |                          |
|----------------------------|--------------------------|
| * Indicator Name:          | Device Temperature       |
| * Measurement Object Type: | User-defined devices     |
| * NE Type:                 | 9000 <span>Select</span> |
| * Vendor Name:             | ZZZ                      |
| * Indicator Unit:          | Degree Fahrenheit        |
| * Calculation Formula:     | \$1.3.6.1.2.1.11.1.0\$   |



**NOTE**

Set **Calculation Formula** of a device performance counter to *MIB ID* followed by **.0**.

2. Create user-defined interface counters. Click **Create**, set interface performance counter parameters on the **Create Performance Indicator** tab page, and click **OK**.

**Figure 13-21** Creating user-defined interface counters

|                            |                                                     |
|----------------------------|-----------------------------------------------------|
| * Indicator Name:          | Interface packet error rate                         |
| * Measurement Object Type: | User-defined interfaces                             |
| * NE Type:                 | 9000 <span>Select</span>                            |
| * Vendor Name:             | ZZZ                                                 |
| * Indicator Unit:          | %                                                   |
| * Calculation Formula:     | (\$1.3.6.1.2.1.11.1-\$1.3.6.1.2.1.11.1')/\$period\$ |

3. Create object counters whose monitoring objects are unspecified. Click **Create**, set object performance counter parameters on the **Create Performance Indicator** tab page, and click **OK**.

**Figure 13-22** Creating object counters whose monitoring objects are unspecified

|                            |                               |
|----------------------------|-------------------------------|
| * Indicator Name:          | CPU usage                     |
| * Measurement Object Type: | Unspecified measuring objects |
| * NE Type:                 | 9000 <span>Select</span>      |
| * Vendor Name:             | ZZZ                           |
| * Indicator Unit:          | %                             |
| * Calculation Formula:     | \$1.3.6.1.2.1.11.2\$          |

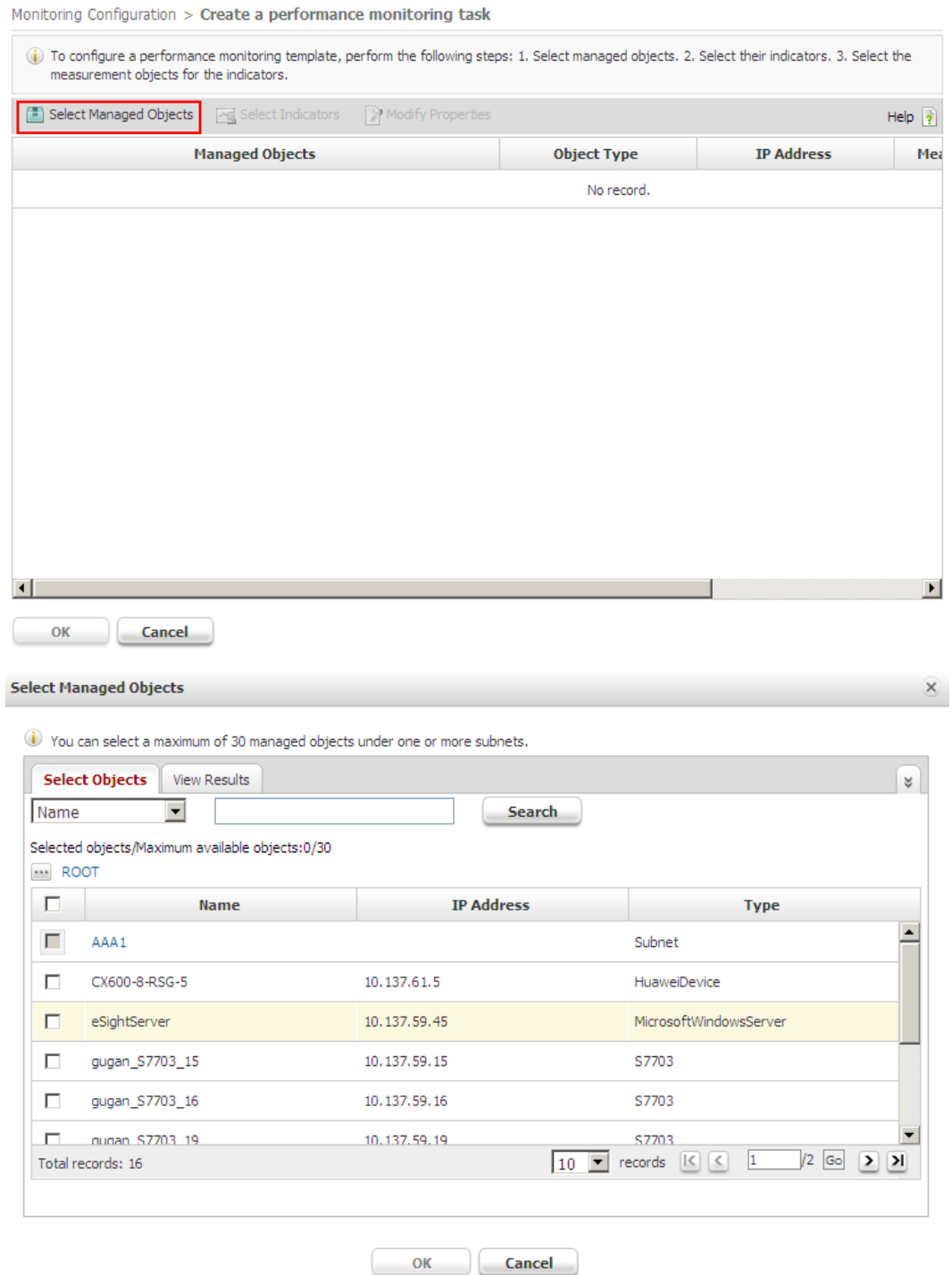
**Step 4** Create a performance monitoring instance.

1. On the main menu, choose **Performance > Monitoring Configuration**, and click **Create**.

**Figure 13-23 Monitoring Configuration**

| Managed Object | Indicator Name                  | Measurement Object | Collection Status | Critical | Major | Minor | Warning | Collection Period | Data Graph |
|----------------|---------------------------------|--------------------|-------------------|----------|-------|-------|---------|-------------------|------------|
| AR1220-10      | CPU usage                       | Slot:SRU Board 0   | Normal            | >90 %    |       |       |         | 15 minutes        |            |
| AR1220-10      | Memory usage                    | Slot:SRU Board 0   | Normal            | >90 %    |       |       |         | 15 minutes        |            |
| AR1220-10      | Responding duration             |                    | Normal            |          |       |       |         | 15 minutes        |            |
| AR1220-10      | Unreachable percentage in a day |                    | Normal            |          |       |       |         | 15 minutes        |            |
| CX600-8-RSG-5  | CPU usage                       | Slot:LPU 8         | Normal            | >90 %    |       |       |         | 15 minutes        |            |
| CX600-8-RSG-5  | CPU usage                       | Slot:SFP 11        | Normal            | >90 %    |       |       |         | 15 minutes        |            |
| CX600-8-RSG-5  | CPU usage                       | Slot:SFP 12        | Normal            | >90 %    |       |       |         | 15 minutes        |            |
| CX600-8-RSG-5  | CPU usage                       | Slot:SRU 9         | Normal            | >90 %    |       |       |         | 15 minutes        |            |

2. Click **Select Managed Objects**. In the **Select Managed Objects** window that is displayed, select a subnet and then select a user-defined device.

**Figure 13-24** Select Managed Objects

3. Click **Select Indicators**, select user-defined device performance counters, and click **OK**.
4. Click  on the right of **Unspecified measuring objects** and **User-defined interfaces**, set a measurement object, and click **OK**.

**NOTE**

You must manually specify monitoring objects for the performance counters without specified monitoring objects.

- Click **OK**. In the **Operation Results** dialog box displaying the operation success message, click **Complete**.

----End

## Follow-up Procedure

Choose **Performance > Monitoring Configuration**, click an NE in the NE list, and click **Performance Status** in the NE manager that is displayed to view the status of the user-defined performance counter.

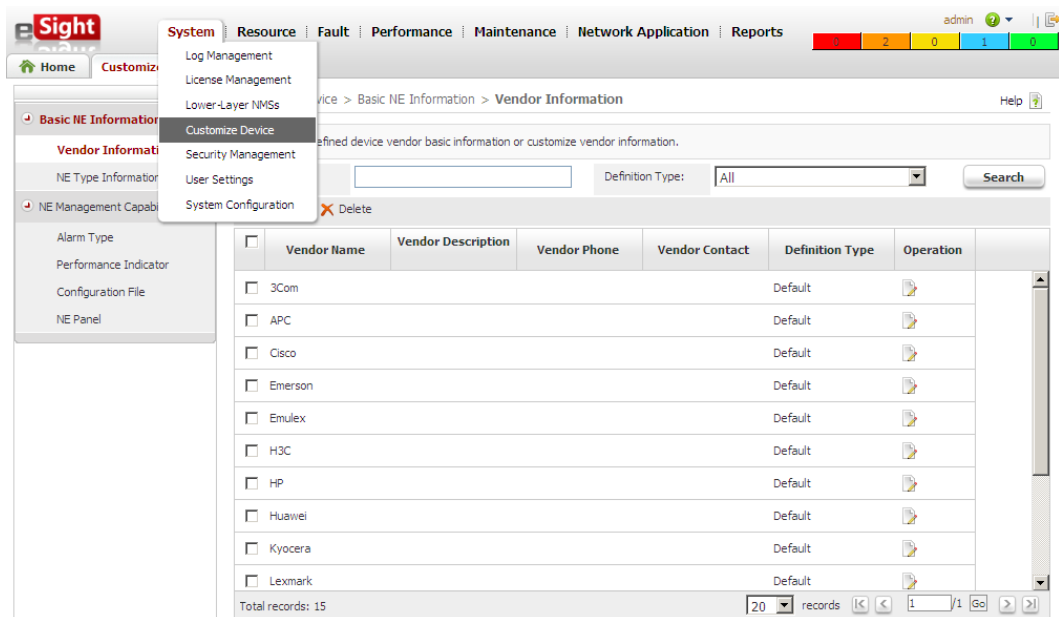
## 13.6.3 Customizing a Device Configuration File

You must customize restart commands and commands for backing up and restoring configuration files for devices from different vendors as required.

### Procedure

- Step 1** Choose **System > Customize Device** from the main menu.

Figure 13-25 Customize Device



- Step 2** In the navigation tree on the left, choose **NE Management Capability > Configuration File**.

**Figure 13-26** Configuration File

The screenshot shows the 'Configuration File' management page. On the left is a navigation tree with 'Configuration File' highlighted. The main area has a breadcrumb 'Customize Device > NE Management Capability > Configuration File' and a 'Help' icon. Below the breadcrumb are input fields for 'NE Type', 'Vendor Name', 'NE Category' (set to 'All'), and 'Definition Type' (set to 'All'), with a 'Search' button. There are '+ Create' and '- Delete' buttons. A table lists existing configuration files:

| <input type="checkbox"/> | NE Type      | Vendor Name | NE Category | Definition Type | Operations |
|--------------------------|--------------|-------------|-------------|-----------------|------------|
| <input type="checkbox"/> | CiscoDevice  | Cisco       | Unknown     | Default         | [Icon]     |
| <input type="checkbox"/> | H3CDevice    | H3C         | Unknown     | Default         | [Icon]     |
| <input type="checkbox"/> | HuaweiDevice | Huawei      | Unknown     | Default         | [Icon]     |
| <input type="checkbox"/> | WS6603       | Huawei      | Switch      | Default         | [Icon]     |

At the bottom, it shows 'Total records: 4' and a pagination control set to '20' records per page.

**Step 3** Click **Create**, click **Select** next to **NE Type**, and select a desired device type.

**Figure 13-27** Creating Configuration File

The 'Create Configuration File' dialog box is shown. It has a breadcrumb 'Customize Device > NE Management Capability > Configuration File > Create Configuration File'. The 'NE Type' field has a 'Select' button. There are three text areas for 'Backup command:', 'Restore command:', and 'Restart command:'. To the right, a help message explains the command format: 'Enter the required command (backup, restore, or restart) for the device vendor and model. Replace specific values with variables. For example, in command `ip ftp username name1`, "name1" is replaced by \$username: `ip ftp username $username`'. It lists available variables: \$username (FTP user name), \$password (FTP password), \$serviceIP (FTP server IP address), \$neFile (backup configuration file name saved on a device), and \$networkFile (backup configuration file name in eSight). At the bottom are 'OK' and 'Cancel' buttons.

**Step 4** Set **Backup command**, **Restore command**, and **Restart command**, and click **OK**.

**Figure 13-28** Customizing a Device Configuration File

|                  |                                                            |                                       |
|------------------|------------------------------------------------------------|---------------------------------------|
| * NE Type:       | <input type="text" value="9000"/>                          | <input type="button" value="Select"/> |
| Backup command:  | <div>save 1.cfg<br/>y<br/>ftp<br/>open 10.137.25.669</div> |                                       |
| Restore command: | <div>ftp<br/>open 10.138.25.36<br/>admin<br/>admin</div>   |                                       |
| Restart command: | <div>restart</div>                                         |                                       |

**Step 5** Create a backup task for the configuration file.

1. Choose **Maintenance > Configuration File Management**.

**Figure 13-29** Configuration File Management

Configuration File Management > Manage Configuration Files > Backup Tasks

Create and manage periodical backup tasks for device configuration, and perform instant backup manually.

Task Name:  Execution Period:   
Status:  Latest Backup Result:

| <input type="checkbox"/> | Task Name | Status | Execution Period | Latest Backup Time | Latest Backup Result | Operation |
|--------------------------|-----------|--------|------------------|--------------------|----------------------|-----------|
| No record.               |           |        |                  |                    |                      |           |

Total records: 0  records

2. Choose **Manage Configuration Files > Backup Tasks** from the navigation tree on the left.

**Figure 13-30** Backing Up Tasks

3. Click **Create** and set parameters related to the backup task.

**Figure 13-31** Creating Backup Task

4. Click **Add Device** next to **Apply to Device**, select the device type, and click **OK** to apply the backup task to devices of this type.



**Figure 13-32** Adding Device

| <input type="checkbox"/> | Device Name         | IP Address    | Device Type      |
|--------------------------|---------------------|---------------|------------------|
| <input type="checkbox"/> | AR 1220-10          | 10.137.59.10  | AR 1220          |
| <input type="checkbox"/> | AR2240_2200         | 10.137.59.220 | AR2240           |
| <input type="checkbox"/> | S5700-52C-PWR-EI-78 | 10.137.59.78  | S5700-52C-PWR-EI |
| <input type="checkbox"/> | S93                 | 10.137.61.37  | S9312            |
| <input type="checkbox"/> | VASP_204            | 10.137.59.204 | SPU              |
| <input type="checkbox"/> | WLAN_58             | 10.137.59.58  | SPU              |
| <input type="checkbox"/> | ar 1220_20          | 10.137.59.208 | AR 1220VW        |
| <input type="checkbox"/> | gugan_S7703_15      | 10.137.59.15  | S7703            |
| <input type="checkbox"/> | gugan_S7703_16      | 10.137.59.16  | S7703            |

Total records: 12    20 records    1 / 1    Go

Select All    OK    Cancel

**NOTE**

- When configuring the backup and restore functions for devices from non-Huawei vendors, you must set Telnet parameters.
- Currently, you can customize commands for backing up and restoring configuration files for Huawei, Cisco, and H3C devices in eSight. Backup and restore may fail on devices from the other vendors.

----End

## 13.6.4 Customizing the Device Panel

You can upload a device panel photo or draw a device panel in eSight to customize the device panel.

### Context

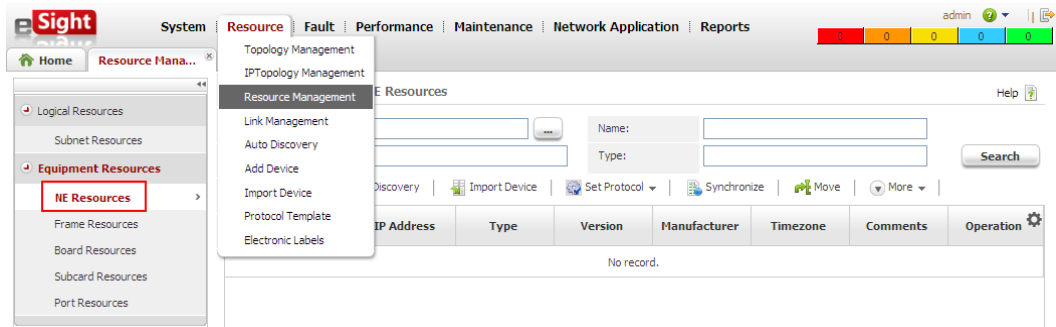
- When customizing the device panel in the NE manager, you do not need to collect devices' vendor type or start index.
- Devices of the **Unknown** type have default device panels and do not support customization.

### Procedure

**Step 1** Access the NE manager page.

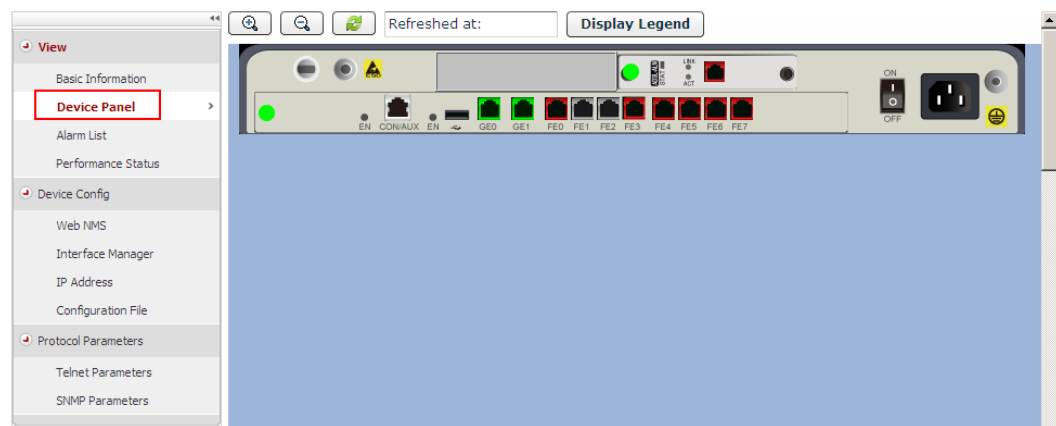
1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 13-33 Resource Management**



**Step 2** In the navigation tree on the left, choose **View > Device Panel**.

**Figure 13-34 Device Panel**



**Step 3** Customize a subrack.

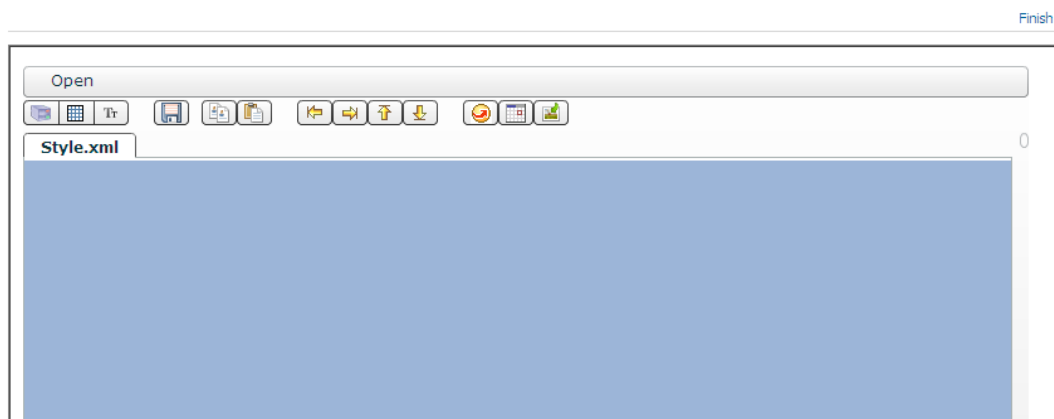
1. Right-click a subrack, and choose **Create New Style**.

**Figure 13-35 Creating New Style**



2. Set the subrack size. Click the slot icon  on the menu bar, drag it to the editor, and set the slot image size based on the subrack image size.

**Figure 13-36** Customize A Subrack



3. Drag the subrack icon  to the slot created in [Step 3.2](#).
4. (Optional) Click , upload a subrack image from the local host, and select the subrack image in the **Extended Attributes** area.



**NOTE**

When you want to log in to eSight using Internet Explorer 8, use Internet Explorer 8 official version. If Internet Explorer 8 preview release is used to log in to eSight and upload an image, the display of the image is incorrect and the system prompts an error.

5. Drag the slot icon  to the subrack image, set the slot size and index ID based on the site scenario. A slot must map a board.
6. Click , set the subrack template name, and click **Save**.
7. Click **OK** in the upper right corner.

**Step 4** Customize a board.

1. On the **Device Panel** tab page in the NE manager, right-click a board, and choose **Create New Style**.
2. Drag the slot icon  to the editor, and set the slot image size based on the board image size.
3. Drag the board icon  to the slot created in [Step 4.2](#).
4. (Optional) Click , upload a board image from the local host, and select the board image in the **Extended Attributes** area.



**NOTE**

When you want to log in to eSight using Internet Explorer 8, use Internet Explorer 8 official version. If Internet Explorer 8 preview release is used to log in to eSight and upload an image, the display of the image is incorrect and the system prompts an error.

To ensure that the port layout is the same as that on the device, drag the slot icon  to the board image, set the slot size and index ID, and arrange slots based on the port layout on the device.

5. Click , set the board template name, and click **Save**.
6. Click **OK** in the upper right corner.

**Step 5** Customize a port template.

1. On the **Device Panel** tab page in the NE manager, right-click a port, and choose **Create New Style**.

 **NOTE**

When you move the pointer to a port, the port type is displayed in a tip. Create different port templates for different port types.

2. Drag the slot icon  to the editor, and set the slot image size based on the port image size.
3. Drag the port icon  to the slot created in [Step 5.2](#).
4. (Optional) Click , upload a port image from the local host, and select the port image in the **Extended Attributes** area.

 **NOTE**

When you want to log in to eSight using Internet Explorer 8, use Internet Explorer 8 official version. If Internet Explorer 8 preview release is used to log in to eSight and upload an image, the display of the image is incorrect and the system prompts an error.

5. Click , set the port template name, and click **Save**.
6. Click **OK** in the upper right corner.

----End

## Follow-up Procedure

To verify the device panel customization, choose **View > Device Panel** in the NE manager to refresh the device panel.

## 13.7 Checking the Network Status of User-Defined Devices

You can check the network status of user-defined devices periodically to obtain the status of communication between eSight and user-defined devices in real time.

### 13.7.1 Performing a Ping Test

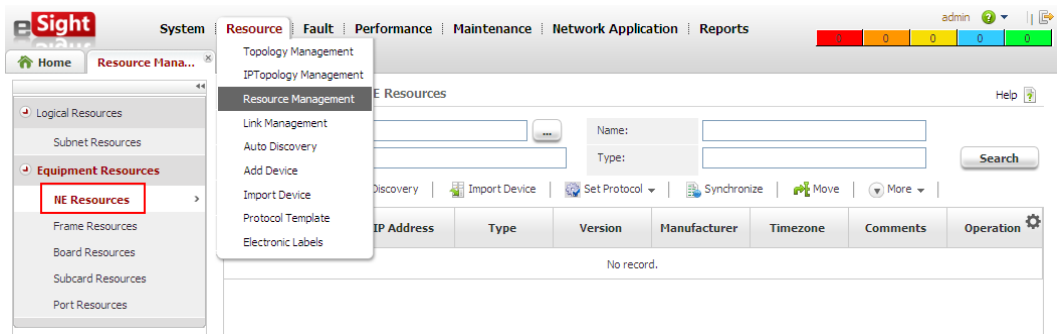
Perform a Ping test on a user-defined device in the NE manager to check the communication status of eSight and the device.

#### Procedure

**Step 1** Access the NE manager page.

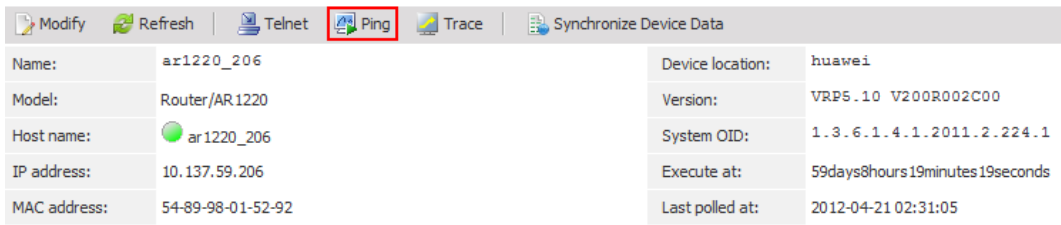
1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.

Figure 13-37 Resource Management



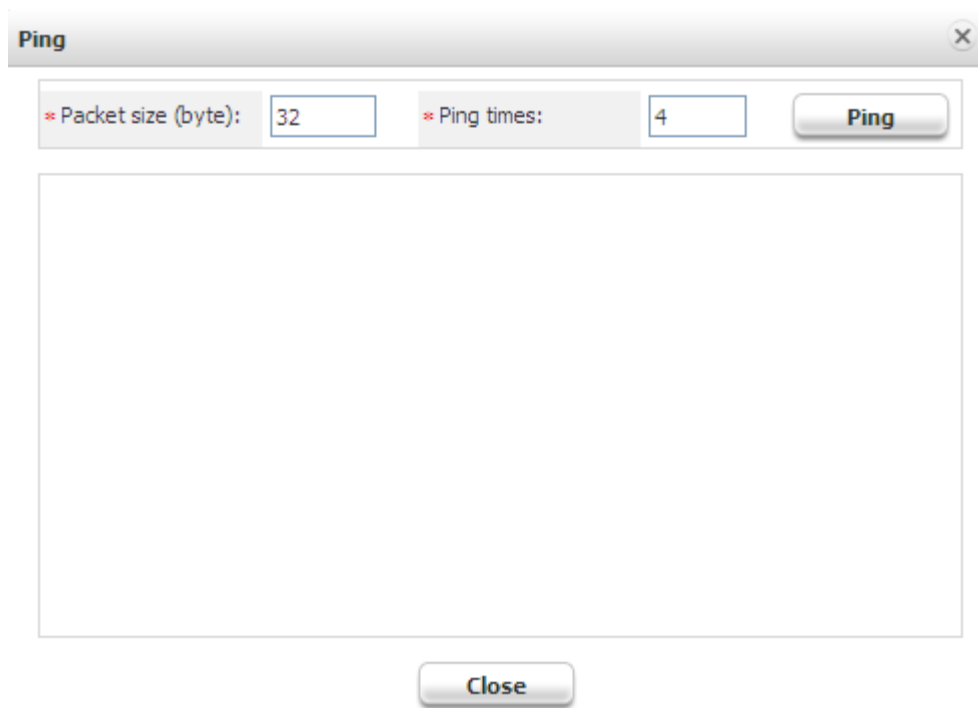
**Step 2** In the navigation tree on the left, choose **View > Basic Information**. In the pane on the right, click **Ping**.

Figure 13-38 Ping



**Step 3** In the displayed **Ping** window, set the Ping test parameters and click **Ping**.

**Figure 13-39** Ping Test



**Step 4** In the **Ping** window, view the Ping test result and click **Close**.  
----End

## 13.7.2 Performing a Trace Test

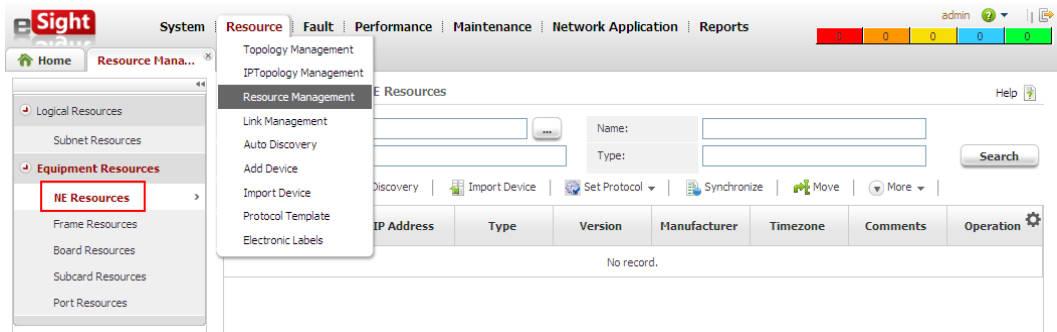
Perform a Trace test on a user-defined device in the NE manager to check the communication status of eSight and the device.

### Procedure

**Step 1** Access the NE manager page.

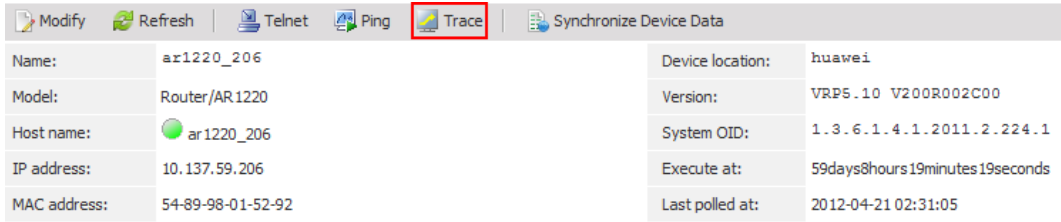
1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

Figure 13-40 Resource Management



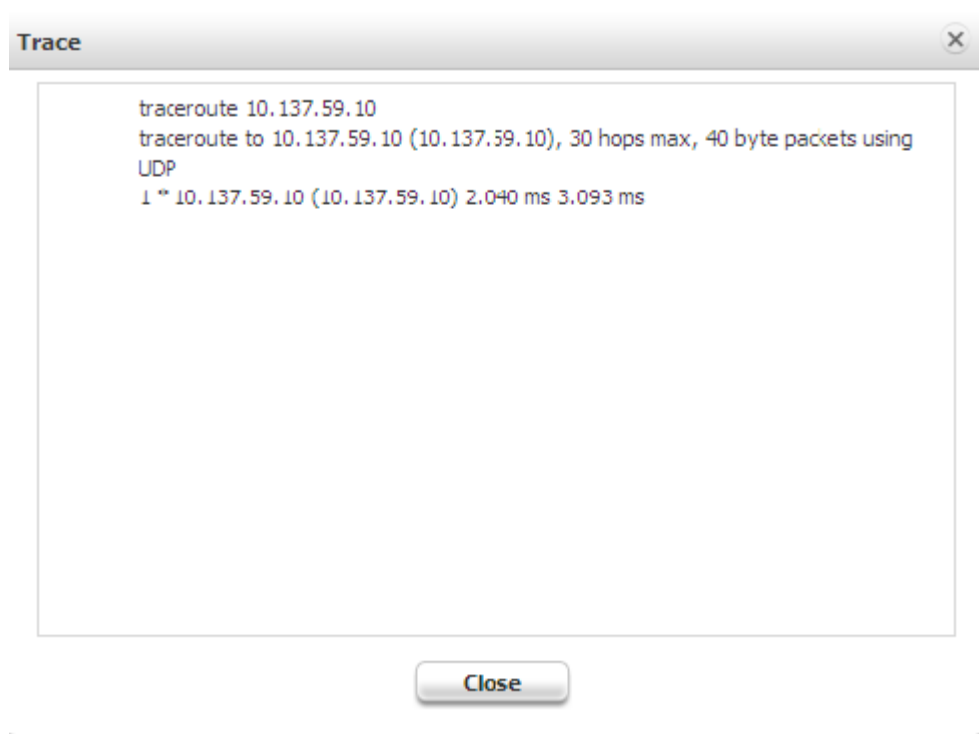
**Step 2** In the navigation tree on the left, choose **View > Basic Information**. In the pane on the right, click **Trace**.

Figure 13-41 Trace



**Step 3** In the displayed **Trace** window, view the Trace test result.

**Figure 13-42** Trace Test



**Step 4** Click **Close**.

----End

### 13.7.3 Query Basic Interface Information

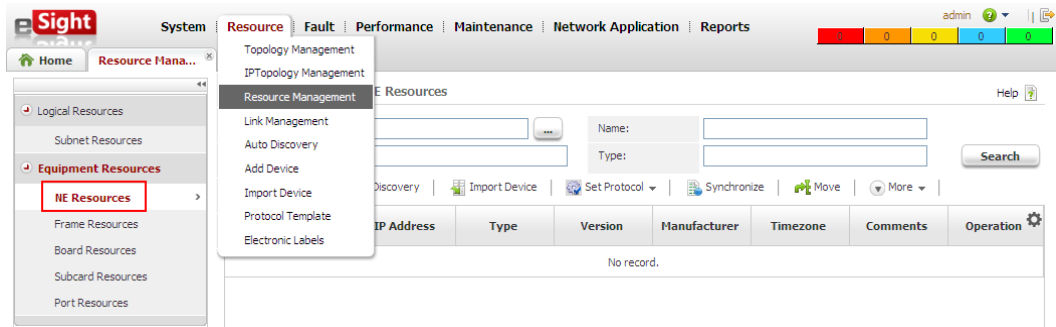
eSight allows users to query interface information.

#### Procedure

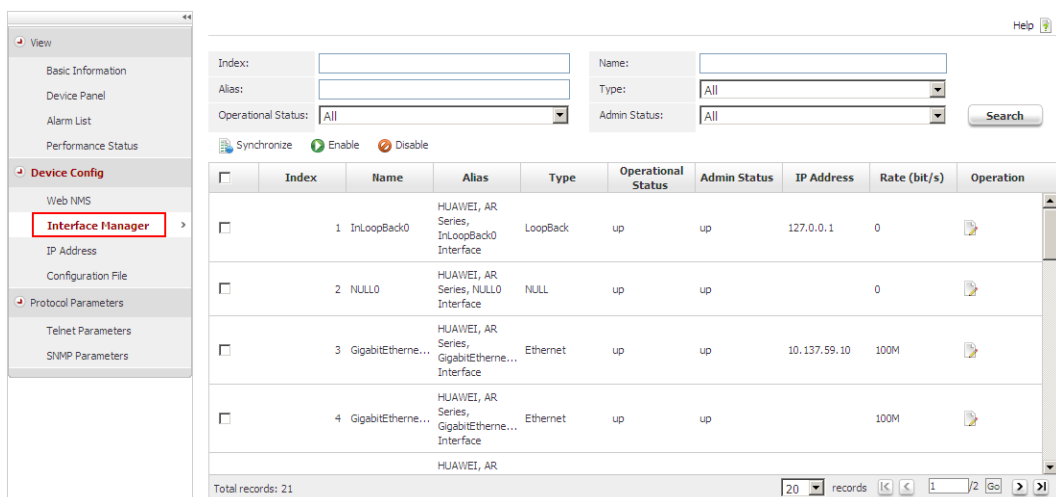
**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.
3. Click the NE name.



**Figure 13-43 Resource Management**

**Step 2** In the navigation tree on the left, choose **Device Config > Interface Manager**.

**Figure 13-44 Interface Manager**

**Step 3** Set filter parameters at the top of the pane and click **Search**.

**Step 4** On the lower part of the right pane of the window, view the interface parameters.

----End

## 13.7.4 Viewing IP Address List

When performing service configuration and network planning, you must query the IP addresses of an NE and the interface. eSight supports query of IP addresses of an NE and the interface.

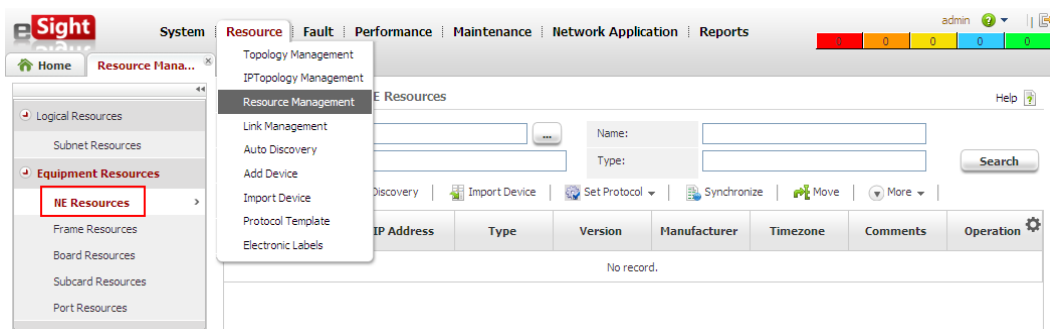
### Procedure

**Step 1** Access the NE manager page.

1. Choose **Resource > Resource Management** from the main menu.
2. Choose **Equipment Resources > NE Resources** from the navigation tree on the left.

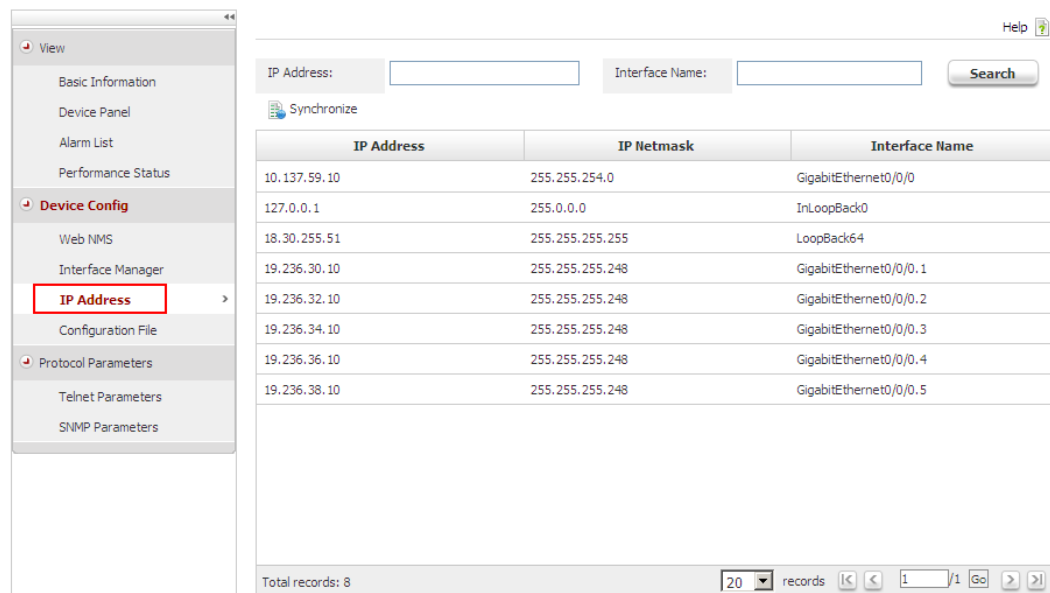
3. Click the NE name.

**Figure 13-45** Resource Management

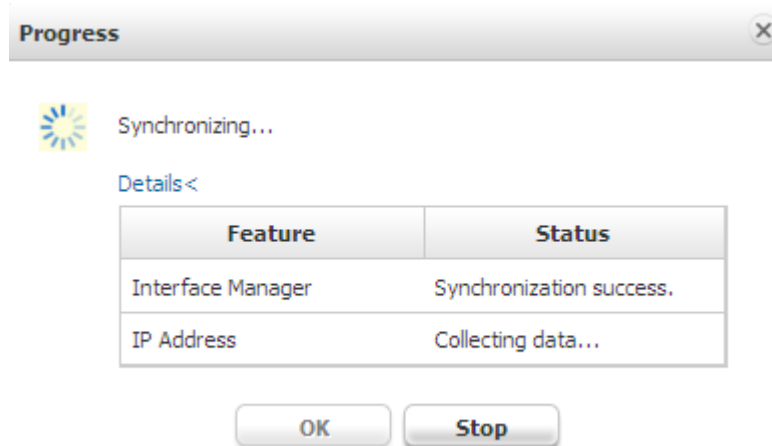


**Step 2** In the navigation tree on the left, choose **Device Config** > **IP Address**.

**Figure 13-46** IP Address



**Step 3** Click **Synchronize**. After the synchronization, in the displayed **Progress** window, view the detailed information, and click **OK** to synchronize the IP address of the NE to eSight.

**Figure 13-47** Progress

**Step 4** Set filter parameters at the top of the pane and click **Search**. On the lower part of the right pane of the window, view the IP address parameters of the interface.

----End

## 13.8 Invoking the Web NMS of User-Defined Devices

eSight supports invocation of the Web NMS function of user-defined devices. eSight can configure services of user-defined devices on the Web NMS page.

### Prerequisites

The type of devices is customized.

The user-defined device supports the Web NMS and the Web NMS has been configured when you customize the NE type on eSight.

### Context



#### NOTE

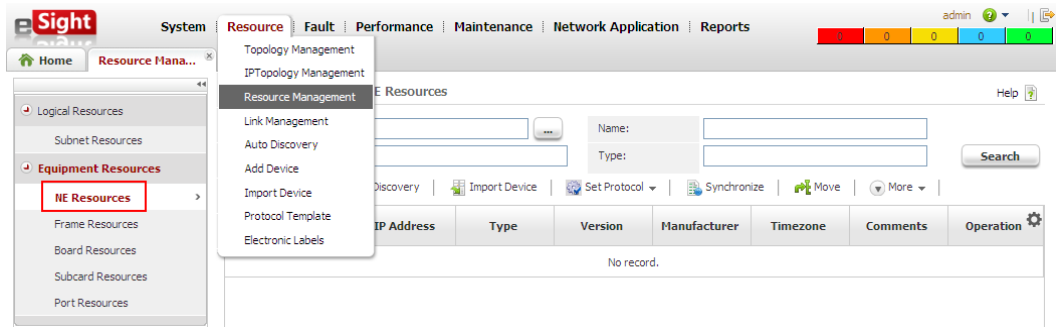
Huawei frame-type switches and routers do not support the Web NMS function and services of the devices must be configured by using the smart configuration tool.

### Procedure

**Step 1** Access the NE manager page.

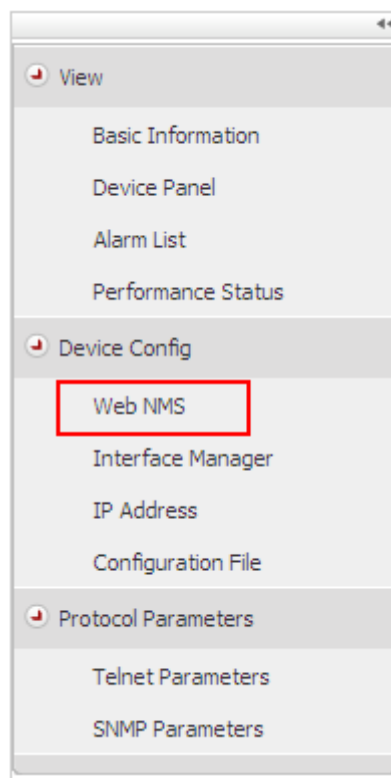
1. Choose **Resource** > **Resource Management** from the main menu.
2. Choose **Equipment Resources** > **NE Resources** from the navigation tree on the left.
3. Click the NE name.

**Figure 13-48 Resource Management**



**Step 2** In the navigation tree on the left, choose **Config > Web NMS**.

**Figure 13-49 Web NMS**



----End

---

# 14 System Management

---

## About This Chapter

### [14.1 Overview of System Management Operations](#)

This topic describes the system management operations.

### [14.2 Setting eSight Data Overflow Dump](#)

The eSight supports data overflow dump to avoid tablespace insufficiency of the database. Data overflow dump is classified into log overflow dump, alarm overflow dump, performance overflow dump, and SLA overflow dump. You need to perform settings based on the actual condition after installing the eSight.

### [14.3 Querying logs](#)

A log records the operations and major events of the eSight. By querying logs, you can learn about the eSight running status and operation details.

### [14.4 Lower-Layer NMS](#)

eSight allows you to manage NEs on a network by layer in a hierarchical manner and construct an area- and layer-based management system. This helps share management responsibilities between multiple NMSs and reduce the pressure of managing a large-scale network.

### [14.5 Managing Licenses](#)

You have permission for the eSight only after obtaining a license. The license file controls the resources and functions of the eSight.

## 14.1 Overview of System Management Operations

This topic describes the system management operations.

[Figure 14-1](#) shows the overview of system management operations. For more details, click the operation in the overview.

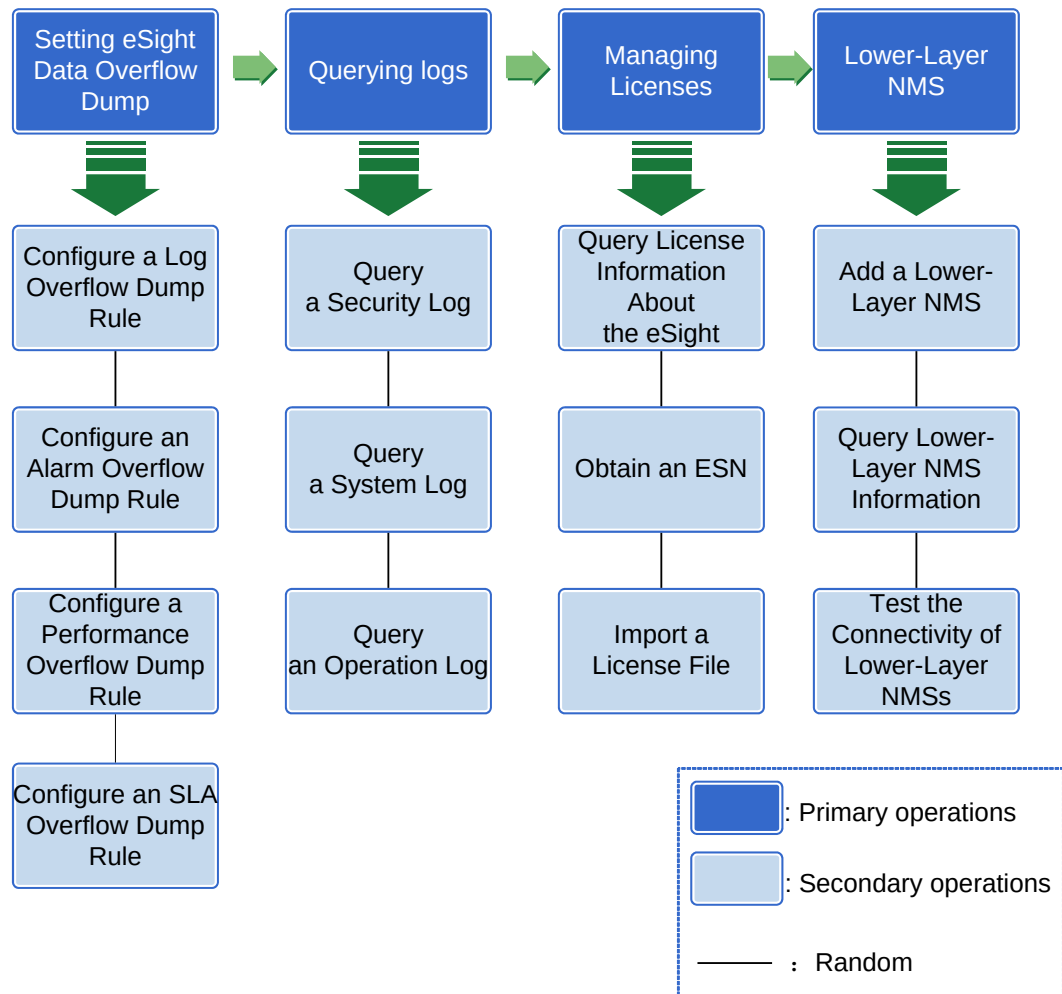
**Figure 14-1** Overview of system management operations

Table 14-1 describes the system management operations.

**Table 14-1** Operation description

| Operation                                                           | Description                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">14.2.1 Configuring a Log Overflow Dump Rule</a>         | The eSight provides log overflow dump to avoid insufficient log database tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the oldest data to a specified path.       |
| <a href="#">14.2.2 Configuring an Alarm Overflow Dump Rule</a>      | The eSight provides alarm overflow dump to avoid insufficient alarm management tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the oldest data to a specified path. |
| <a href="#">14.2.3 Configuring a Performance Overflow Dump Rule</a> | The eSight provides performance overflow dump to avoid insufficient performance management tablespace of the database. If the eSight detects that the tablespace usage                                                                                                         |

| Operation                                                             | Description                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                       | exceeds the specified database space threshold, the eSight automatically dumps the oldest data to a specified path.                                                                                                                                                                   |
| <a href="#">14.2.4 Configuring an SLA Overflow Dump Rule</a>          | The eSight provides SLA database overflow dump to avoid insufficient SLA database tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the original data to a specified folder. |
| <a href="#">14.3.2 Querying a Security Log</a>                        | You can query security logs to understand the information about eSight related security operations.                                                                                                                                                                                   |
| <a href="#">14.3.3 Querying a System Log</a>                          | You can query system logs to understand the information about eSight operations.                                                                                                                                                                                                      |
| <a href="#">14.3.4 Querying an Operation Log</a>                      | You can query operation logs to understand the information about eSight user operations.                                                                                                                                                                                              |
| <a href="#">14.5.1 Querying License Information About the eSight</a>  | You can query the information about the current license.                                                                                                                                                                                                                              |
| <a href="#">14.5.2 Obtaining an ESN</a>                               | This topic describes how to obtain an equipment serial number (ESN). When your license is going to expire, you need to obtain the ESN of your computer for applying for a new license.                                                                                                |
| <a href="#">14.5.3 Importing a License File</a>                       | When the current eSight license is invalid, expires, or cannot meet network management requirements, you must import a new license to the eSight to ensure normal services of the eSight.                                                                                             |
| <a href="#">14.4.2.1 Adding a Lower-Layer NMS</a>                     | You can add a lower-layer NMS to enable eSight to manage it.                                                                                                                                                                                                                          |
| <a href="#">14.4.2.2 Querying Lower-Layer NMS Information</a>         | You can periodically query the lower-layer NMS status.                                                                                                                                                                                                                                |
| <a href="#">14.4.2.3 Testing the Connectivity of Lower-Layer NMSs</a> | You can periodically test the connectivity of lower-layer NMSs.                                                                                                                                                                                                                       |

## 14.2 Setting eSight Data Overflow Dump

The eSight supports data overflow dump to avoid tablespace insufficiency of the database. Data overflow dump is classified into log overflow dump, alarm overflow dump, performance overflow dump, and SLA overflow dump. You need to perform settings based on the actual condition after installing the eSight.

## 14.2.1 Configuring a Log Overflow Dump Rule

The eSight provides log overflow dump to avoid insufficient log database tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the oldest data to a specified path.

### Prerequisites

You have the operation rights for **System Configuration**.

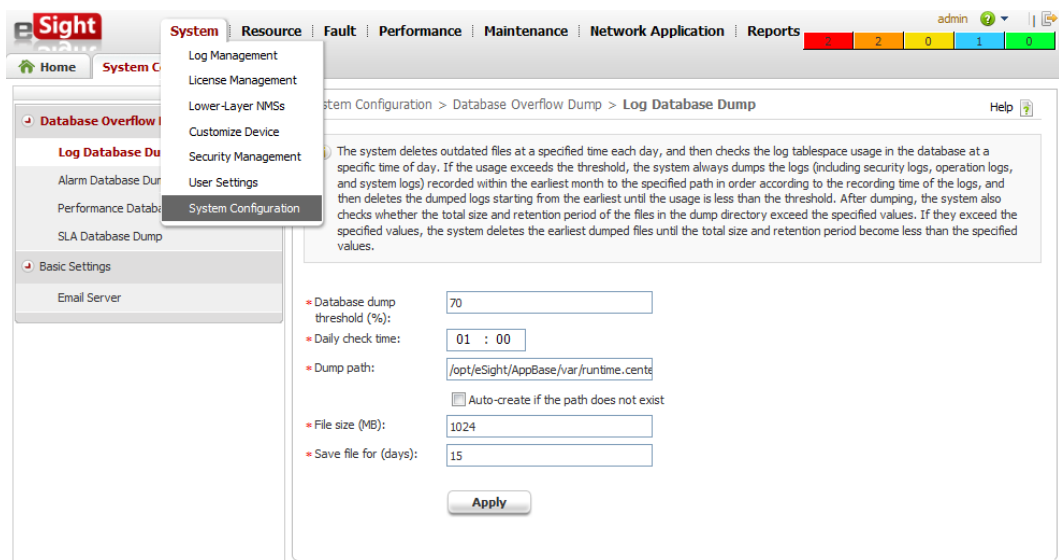
### Context

If the log tablespace usage exceeds the specified database space threshold, a data overflow occurs.

### Procedure

**Step 1** Choose **System > System Configuration** from the main menu.

**Figure 14-2** System configuration



**Step 2** In the **System Configuration** window, select **Database Overflow Dump > Log Database Dump**.

**Step 3** On the **Log Database Dump** page, set log overflow dump parameters.

The maximum log management tablespace size varies according to eSight edition and database type. For details, see [Table 14-2](#).



**Figure 14-3** Setting the log database dump

\* Database dump threshold (%):

\* Daily check time:

\* Dump path:   
☒ Auto-create if the path does not exist

\* File size (MB):

\* Save file for (days):

**Table 14-2** Maximum log management tablespace size

| Edition                   | MySQL Database | SQL Server Database | Oracle Database |
|---------------------------|----------------|---------------------|-----------------|
| Express                   | 2G             | -                   | -               |
| Compact                   | 2G             | -                   | -               |
| Standard (Windows)        | 2G             | 2G                  | -               |
| Professional (Windows)    | 2G             | 2G                  | -               |
| Standard (SUSE Linux)     | -              | -                   | 2G              |
| Professional (SUSE Linux) | -              | -                   | 2G              |

**NOTE**

The **Database dump threshold (%)** parameter indicates the percentage of the maximum log management tablespace size.

**Dump path** can be an absolute path or a relative path. The relative path is relative to the eSight installation path `%eSight_ROOT/AppBase/var/runtime.center/data/dump` (on Linux). If you specify **Dump path** to **AAA**, the file is saved to `%eSight_ROOT/AppBase/var/runtime.center/data/dump/AAA`.

**Step 4** Click **Apply**.

----End

## 14.2.2 Configuring an Alarm Overflow Dump Rule

The eSight provides alarm overflow dump to avoid insufficient alarm management tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the oldest data to a specified path.

## Prerequisites

You have the operation rights for **System Configuration**.

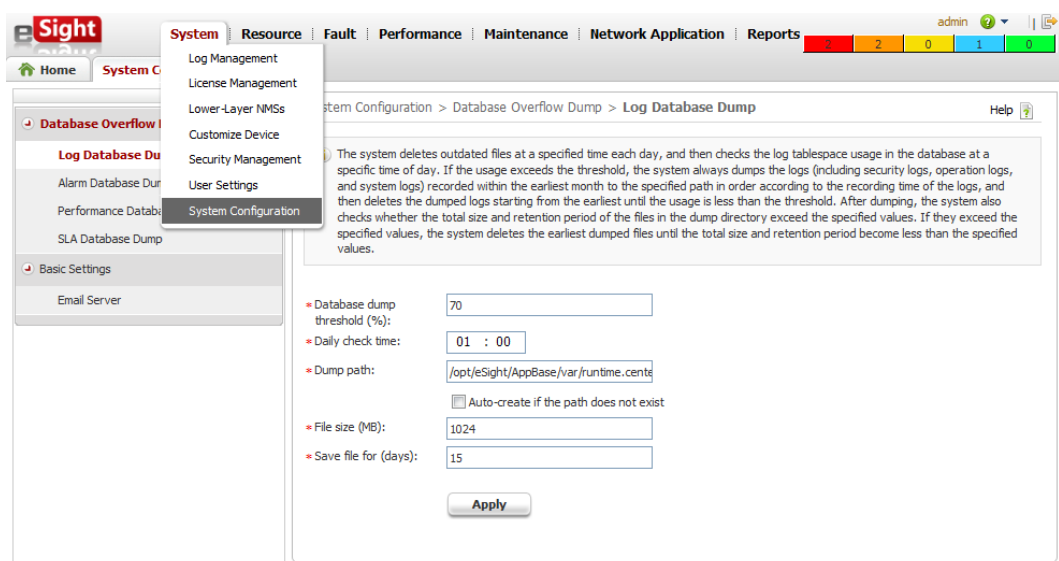
## Context

If the alarm management tablespace usage exceeds the specified database space threshold, a data overflow occurs.

## Procedure

**Step 1** Choose **System > System Configuration** from the main menu.

**Figure 14-4** System configuration



**Step 2** In the **System Configuration** window, select **Database Overflow Dump > Alarm Database Dump**.

**Step 3** On the **Alarm Database Dump** page, set alarm overflow dump parameters.

The maximum alarm management tablespace size varies according to eSight edition and database type. For details, see [Table 14-3](#).

**Figure 14-5** Setting the alarm database dump

\* Database dump threshold (%):

\* Daily check time:

\* Dump path:   
☒ Auto-create if the path does not exist

\* File size (MB):

\* Save file for (days):

**Table 14-3** Maximum alarm management tablespace size

| Edition                   | MySQL Database | SQL Server Database | Oracle Database |
|---------------------------|----------------|---------------------|-----------------|
| Express                   | 8G             | -                   | -               |
| Compact                   | 8G             | -                   | -               |
| Standard (Windows)        | 8G             | 2G                  | -               |
| Professional (Windows)    | 8G             | 2G                  | -               |
| Standard (SUSE Linux)     | -              | -                   | 4G              |
| Professional (SUSE Linux) | -              | -                   | 4G              |

**NOTE**

The **Database dump threshold (%)** parameter indicates the percentage of the maximum log management tablespace size.

**Dump path** can be an absolute path or a relative path. The relative path is relative to the eSight installation path **%eSight\_ROOT/AppBase/var/runtime.center/data/dump** (on Linux). If you specify **Dump path** to AAA, the file is saved to **%eSight\_ROOT/AppBase/var/runtime.center/data/dump/AAA**.

**Step 4** Click **Apply**.

----End

## 14.2.3 Configuring a Performance Overflow Dump Rule

The eSight provides performance overflow dump to avoid insufficient performance management tablespace of the database. If the eSight detects that the tablespace usage

exceeds the specified database space threshold, the eSight automatically dumps the oldest data to a specified path.

## Prerequisites

You have the operation rights for **System Configuration**.

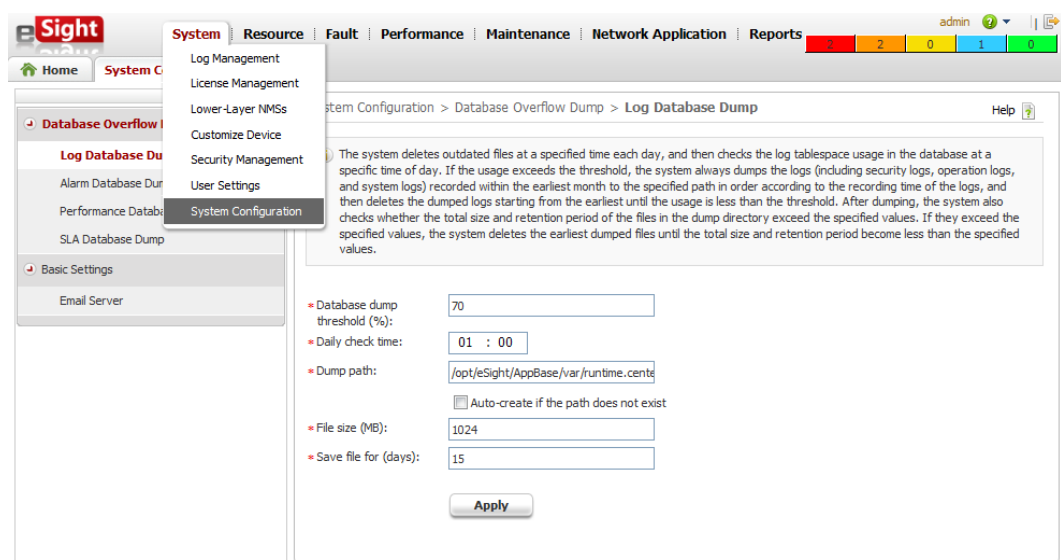
## Context

If the performance management tablespace usage exceeds the specified database space threshold, a data overflow occurs.

## Procedure

**Step 1** Choose **System > System Configuration** from the main menu.

**Figure 14-6** System configuration



**Step 2** In the **System Configuration** window, select **Database Overflow Dump > Performance Database Dump**.

**Step 3** On the **Performance Database Dump** page, set performance overflow dump parameters.

The maximum performance management tablespace size varies according to eSight edition and database type. For details, see [Table 14-4](#).

**Figure 14-7** Setting the performance database dump

\* Database dump threshold (%):

\* Daily check time:

\* Dump path:   
☒ Auto-create if the path does not exist

\* File size (MB):

\* Save file for (days):

**Table 14-4** Maximum performance management tablespace size

| Edition                   | MySQL Database | SQL Server Database | Oracle Database |
|---------------------------|----------------|---------------------|-----------------|
| Express                   | 8G             | -                   | -               |
| Compact                   | 8G             | -                   | -               |
| Standard (Windows)        | 8G             | 4G                  | -               |
| Professional (Windows)    | 8G             | 30G                 | -               |
| Standard (SUSE Linux)     | -              | -                   | 30G             |
| Professional (SUSE Linux) | -              | -                   | 30G             |

**NOTE**

The **Database dump threshold (%)** parameter indicates the percentage of the maximum log management tablespace size.

**Dump path** can be an absolute path or a relative path. The relative path is relative to the eSight installation path **%eSight\_ROOT/AppBase/var/runtime.center/data/dump** (on Linux). If you specify **Dump path** to AAA, the file is saved to **%eSight\_ROOT/AppBase/var/runtime.center/data/dump/AAA**.

**Step 4** Click **Apply**.

----End

## 14.2.4 Configuring an SLA Overflow Dump Rule

The eSight provides SLA database overflow dump to avoid insufficient SLA database tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified

database space threshold, the eSight automatically dumps the original data to a specified folder.

## Prerequisites

You have the operation rights for **System Configuration**.

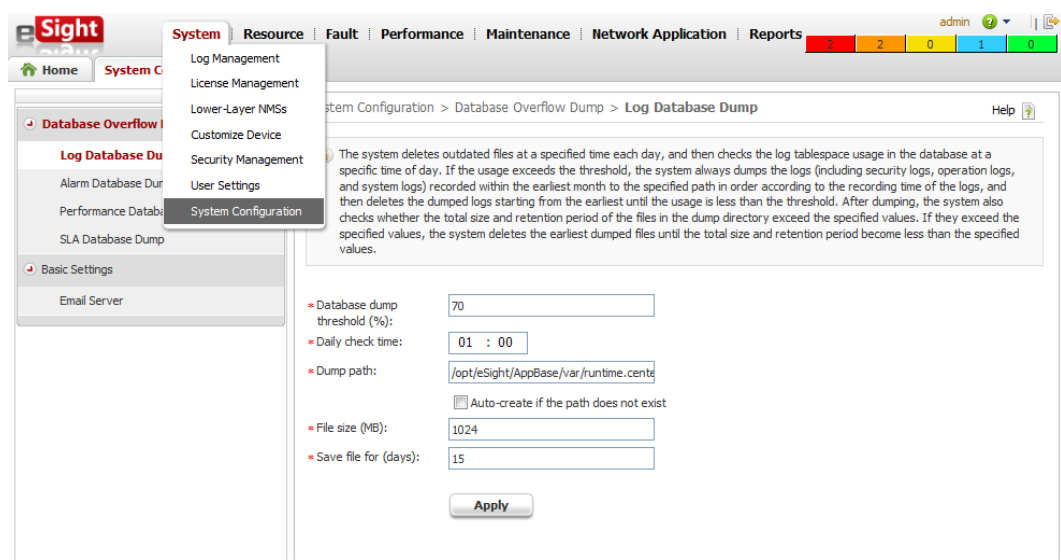
## Context

If the SLA tablespace usage exceeds the specified database space threshold, a data overflow occurs.

## Procedure

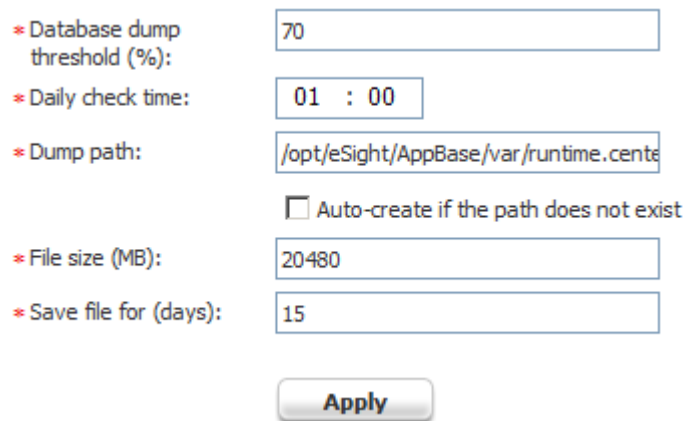
**Step 1** Choose **System > System Configuration** from the main menu.

**Figure 14-8** System Configuration



**Step 2** In the **System Configuration** window, select **Database Overflow Dump > SLA Database Dump**.

**Step 3** On the **SLA Database Dump** page, set SLA database overflow dump parameters.

**Figure 14-9** SLA overflow dump parameters settings

\* Database dump threshold (%): 70

\* Daily check time: 01 : 00

\* Dump path: /opt/eSight/AppBase/var/runtime.center

☐ Auto-create if the path does not exist

\* File size (MB): 20480

\* Save file for (days): 15

Apply

The maximum SLA management tablespace size varies according to eSight edition and database type. For details, see [Table 14-5](#).

**Table 14-5** Maximum SLA management tablespace size

| Edition    | MySQL Database | SQL Server Database | Oracle Database |
|------------|----------------|---------------------|-----------------|
| Windows    | 20G            | 20G                 | -               |
| SUSE Linux | -              | -                   | 20G             |

**NOTE**

The **Database dump threshold (%)** parameter indicates the percentage of the maximum SLA management tablespace size.

**Dump path** can be an absolute path or a relative path. The relative path is relative to the eSight installation path `%eSight_ROOT/var/runtime.center/data/dump` (on Linux). If you specify **Dump path** to **AAA**, the file is saved to `%eSight_ROOT/var/runtime.center/data/dump/AAA`.

**Step 4** Click **Apply**.

----End

## 14.3 Querying logs

A log records the operations and major events of the eSight. By querying logs, you can learn about the eSight running status and operation details.

### 14.3.1 Log Types

eSight logs are classified into security logs, system logs, and operation logs.

## Security Logs

Security logs record security operations that are performed on the eSight, such as logging in to the server, changing passwords, creating users, and logging out of the server.

## System Logs

System logs record the events occurred on the eSight, such as abnormal running of the eSight, network failures, and attacks to the eSight. These logs help you analyze the eSight status and rectify faults.

## Operation Logs

Operation logs record the user operations that are performed on the eSight, such as creating monitoring views and modifying NE managers.

### 14.3.2 Querying a Security Log

You can query security logs to understand the information about eSight related security operations.

#### Prerequisites

You have the operation rights for **Log Management**.

#### Context

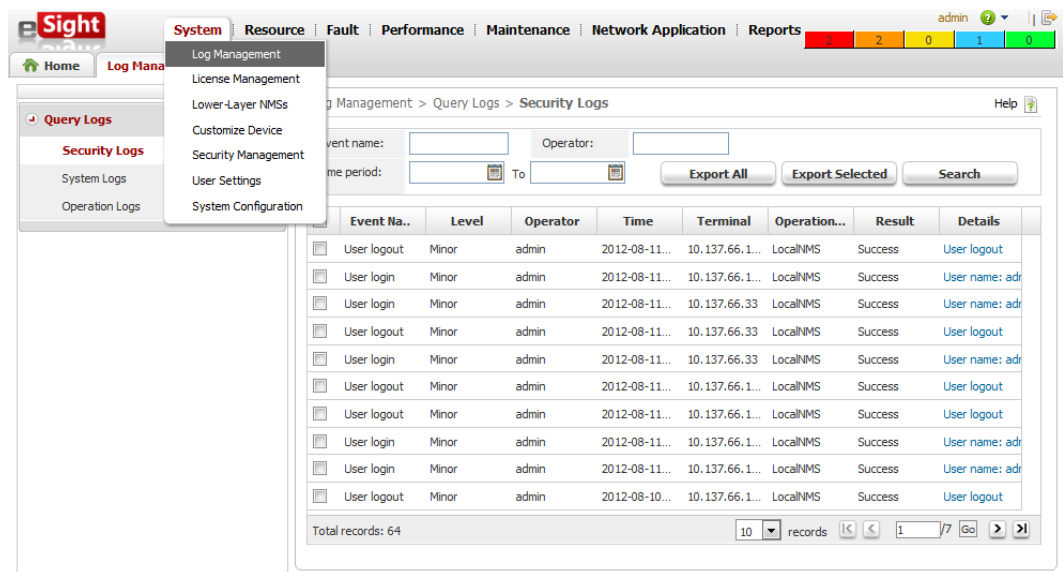
- All security logs are queried if you do not set any search criteria.
- The query result is generated based on the existing data in the database. No information is displayed if no data is generated.

#### Procedure

**Step 1** Choose **System > Log Management** from the main menu.

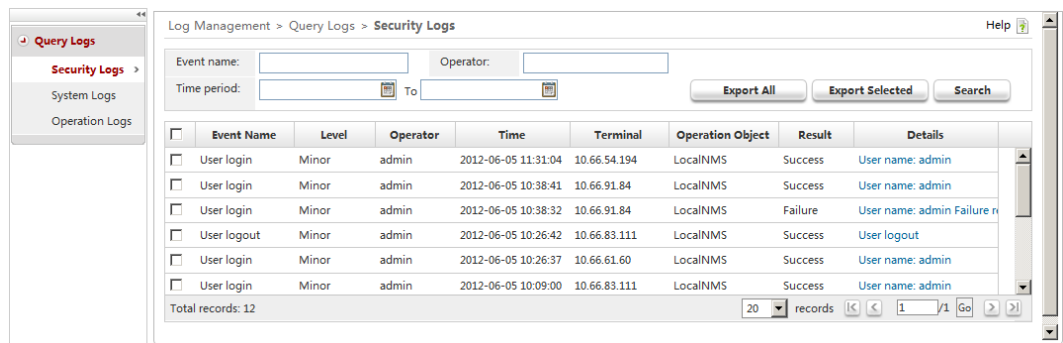


Figure 14-10 Log management



**Step 2** In the **Log Management** window, select **Query Logs > Security Logs**.

Figure 14-11 Querying the security logs



**Step 3** Directly view the logs or set search criteria to search for the specified logs.

After clicking the value in the **Details** column of the target log, you can view logs details in **Security Log Details**.

**NOTE**

A maximum of 800 characters can be displayed in **Security Log Details**. Contents other than the first 800 characters are displayed as ....

----End

## Follow-up Procedure

The following table describes the operations that can be performed on the **Security Logs** page.

| Export Security Logs              | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Export all security logs          | <ol style="list-style-type: none"><li>1. Click <b>Export All</b> to export all security logs.</li><li>2. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>3. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p>                                                                                                              |
| Export the selected security logs | <ol style="list-style-type: none"><li>1. In the log list, select the check box before <b>Event Name</b> of the required log.</li><li>2. Click <b>Export Selected</b> to export the selected security logs.</li><li>3. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>4. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p> |

### 14.3.3 Querying a System Log

You can query system logs to understand the information about eSight operations.

#### Prerequisites

You have the operation rights for **Log Management**.

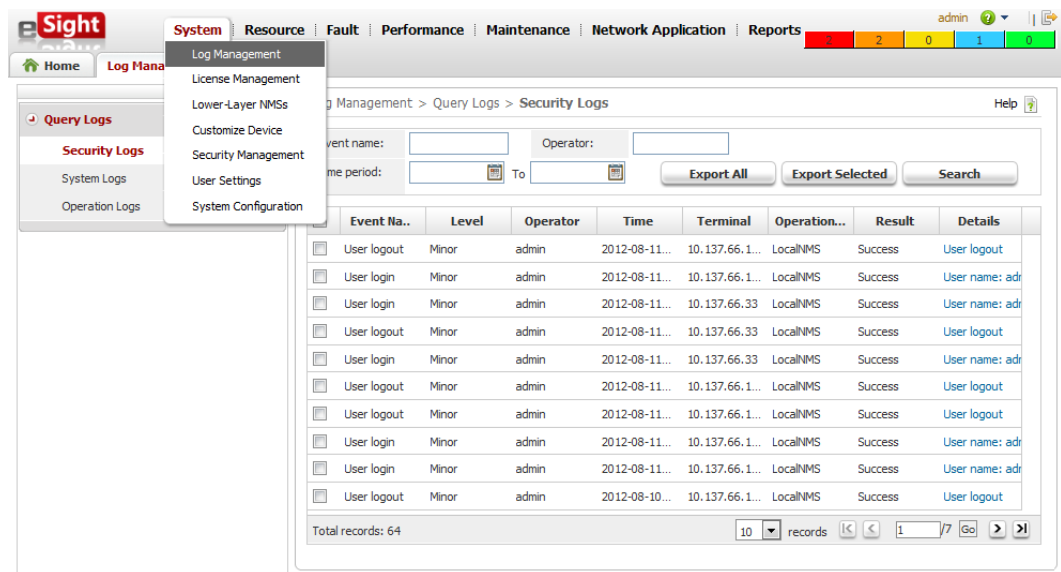
#### Context

- All system logs are queried if you do not set any search criteria.
- The query result is generated based on the existing data in the database. No information is displayed if no data is generated.

#### Procedure

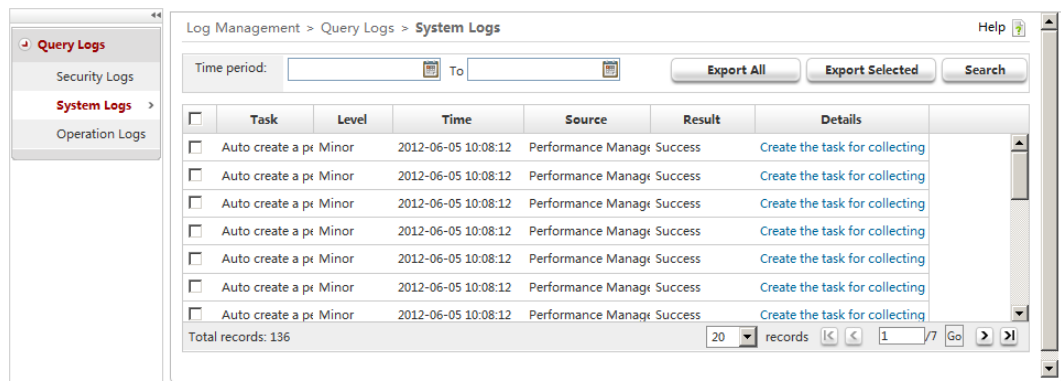
**Step 1** Choose **System > Log Management** from the main menu.

Figure 14-12 Log management



**Step 2** In the **Log Management** window, select **Query Logs > System Logs**.

Figure 14-13 Querying the system logs



**Step 3** Directly view the logs or set search criteria to search for the specified logs.

After clicking the value in the **Details** column of the target log, you can view logs details in **System Log Details**.

**NOTE**

A maximum of 800 characters can be displayed in **Security Log Details**. Contents other than the first 800 characters are displayed as ....

----End

## Follow-up Procedure

The following table describes the operations that can be performed on the **System Logs** page.

| Export System Logs              | Operation Method                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Export all system logs          | <ol style="list-style-type: none"><li>1. Click <b>Export All</b> to export all system logs.</li><li>2. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>3. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p>                                                                                                        |
| Export the selected system logs | <ol style="list-style-type: none"><li>1. In the log list, select the check box before <b>Task</b> of the required log.</li><li>2. Click <b>Export Selected</b> to export the selected system logs.</li><li>3. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>4. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p> |

## 14.3.4 Querying an Operation Log

You can query operation logs to understand the information about eSight user operations.

### Prerequisites

You have the operation rights for **Log Management**.

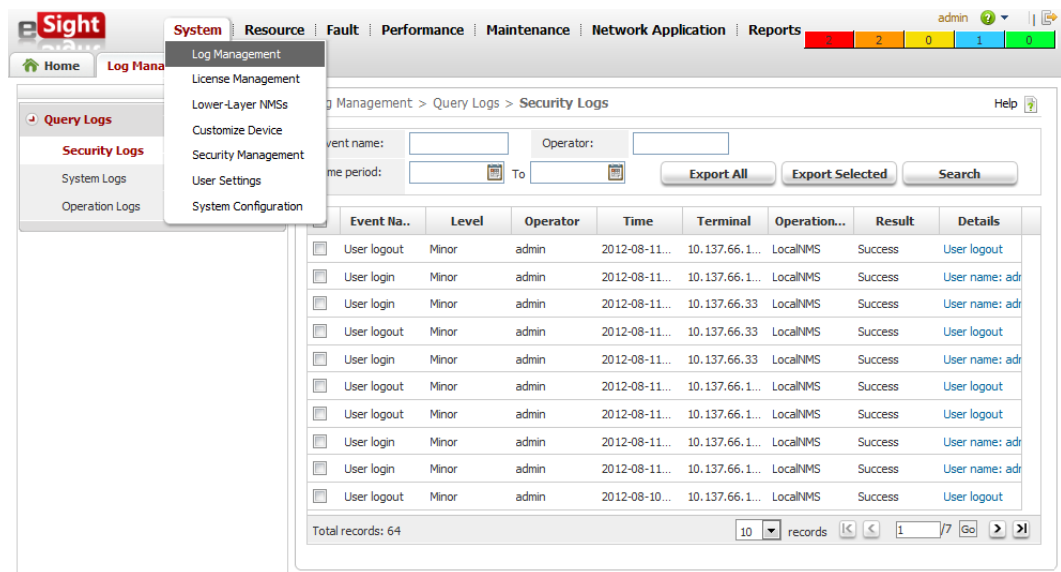
### Context

- All operation logs are queried if you do not set any search criteria.
- The query result is generated based on the existing data in the database. No information is displayed if no data is generated.

### Procedure

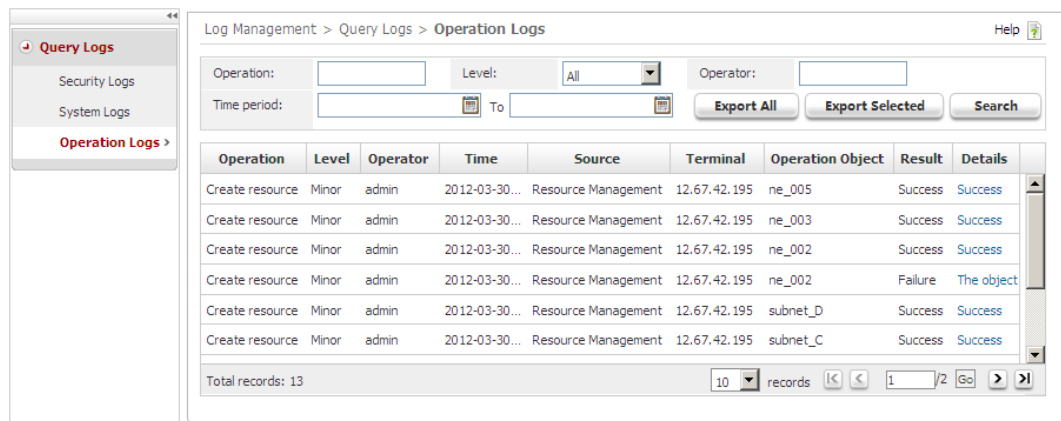
**Step 1** Choose **System > Log Management** from the main menu.

Figure 14-14 Log management



**Step 2** In the **Log Management** window, select **Query Logs > Operation Logs**.

Figure 14-15 Querying the operation logs



**Step 3** Directly view the logs or set search criteria to search for the specified logs.

- View details about an operation log.  
After clicking the value in the **Details** column of the target log, you can view logs details in **Operation Log Details**.
- View details about a batch operation log.
  1. Click the value in the **Details** column of the target log.
  2. In the **Operation Log Details** dialog box, click **Operation Log Details** to view the result of each operation.

**NOTE**

A maximum of 800 characters can be displayed in **Security Log Details**. Contents other than the first 800 characters are displayed as ....

----End

## Follow-up Procedure

The following table describes the operations that can be performed on the **Operation Logs** page.

| Export Operation Logs              | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Export all operation logs          | <ol style="list-style-type: none"><li>1. Click <b>Export All</b> to export all operation logs.</li><li>2. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>3. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p>                                                                                                             |
| Export the selected operation logs | <ol style="list-style-type: none"><li>1. In the log list, select the check box before <b>Operation</b> of the required log.</li><li>2. Click <b>Export Selected</b> to export the selected operation logs.</li><li>3. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>4. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p> |

## 14.4 Lower-Layer NMS

eSight allows you to manage NEs on a network by layer in a hierarchical manner and construct an area- and layer-based management system. This helps share management responsibilities between multiple NMSs and reduce the pressure of managing a large-scale network.

### 14.4.1 Lower-Layer NMS Management

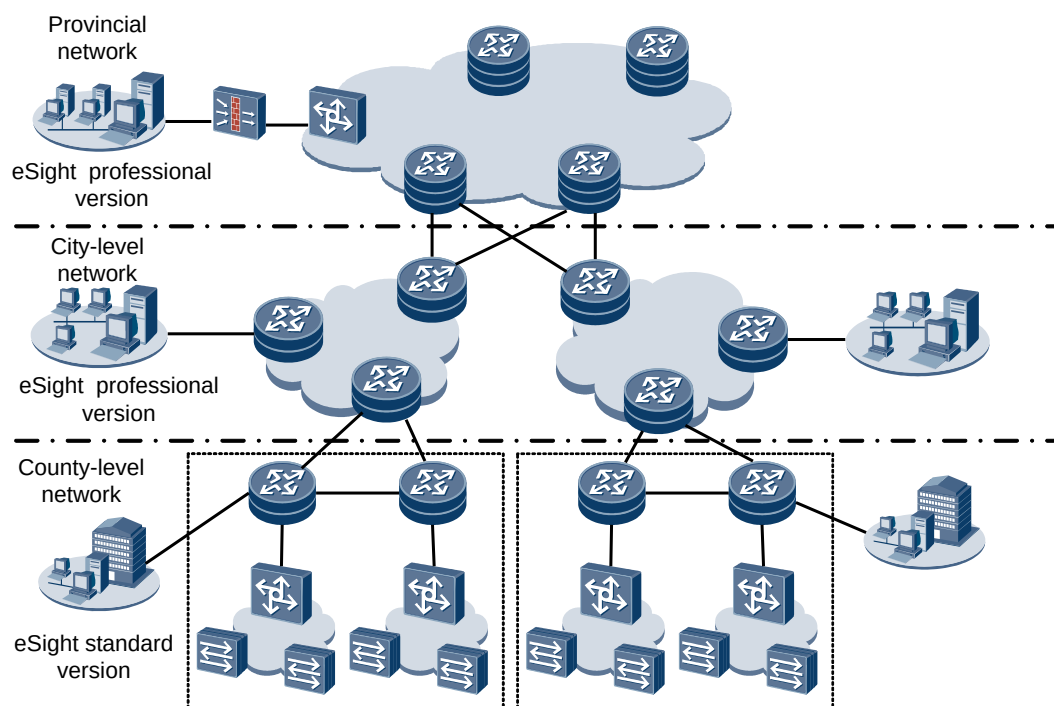
The hierarchical network management mechanism of eSight enables users to divide management areas and construct a layer-based management system based on the geographical area and organization structure. Upper-layer NMSs have higher rights than lower-layer NMSs. Upper-layer NMSs have rights to manage lower-layer NMSs; however, lower-layer NMSs have no right to manage upper-layer NMSs.

#### 14.4.1.1 Lower-Layer NMS Application

The hierarchical network management mechanism enables multiple NMSs to share the management responsibilities and reduces the management pressure.

See [Figure 14-16](#). Lower-layer NMSs manage different management areas. Upper-layer NMSs can log in to lower-layer NMSs to manage devices in the corresponding management areas.

**Figure 14-16** Lower-Layer NMS application



### 14.4.1.2 Lower-Layer NMS Function

This topic describes the basic functions of the hierarchical network management.

You can display a lower-layer NMS page on the upper-layer NMS page to view the alarms, topology, performance, and reports of the lower-layer NMS. You can implement all functions of a lower-layer NMS on the lower-layer NMS page. Upper-layer NMSs monitor only the connection status of lower-layer NMSs and can log in to lower-layer NMSs in SSO mode.

eSight provides the following functions for upper-layer NMSs to monitor lower-layer NMSs:

- **Adding a lower-layer NMS**  
You can add a lower-layer NMS so that the upper-layer NMS can monitor the lower-layer NMS.
- **Displaying a lower-layer NMS page**  
You can display a lower-layer NMS page on the upper-layer NMS page to view the alarms, topology, performance, and reports of the lower-layer NMS.
- **Viewing the lower-layer NMS list**  
You can view the list of lower-layer NMSs that are managed by an upper-layer NMS.
- **Deleting a lower-layer NMS**  
You can delete a lower-layer NMS as required.

### 14.4.2 Managing a Lower-Layer NMS

This topic describes how to manage a lower-layer NMS.

### 14.4.2.1 Adding a Lower-Layer NMS

You can add a lower-layer NMS to enable eSight to manage it.

#### Prerequisites

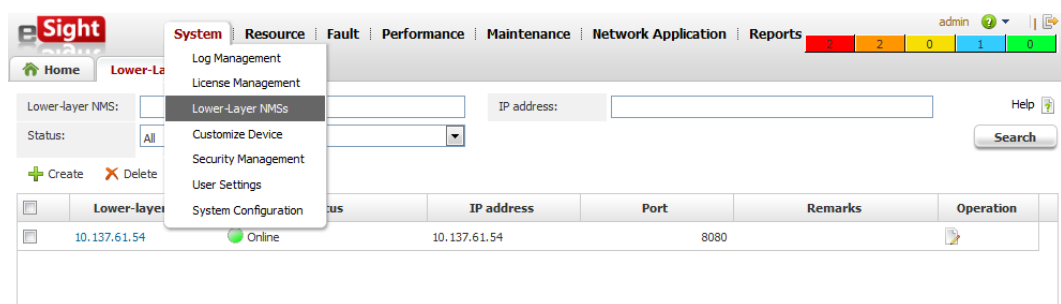
The lower-layer NMS runs properly.

A user has the permission to add a lower-layer NMS.

#### Procedure

**Step 1** Choose **System > Lower-Layer NMSs** from the main menu.

Figure 14-17 Lower-Layer NMSs



**Step 2** Click **Create**, and set **Lower-layer NMS**, **IP address**, **Port**, and **Remarks** in the window that is displayed.

Figure 14-18 New record

The screenshot shows a 'New record' form. It has four input fields: 'Lower-layer NMS:', 'IP address:', 'Port:', and 'Remarks:'. Each field is preceded by a red asterisk, indicating it is a required field. Below the input fields are two buttons: 'OK' and 'Cancel'.

**Step 3** Click **OK**.

----End

### 14.4.2.2 Querying Lower-Layer NMS Information

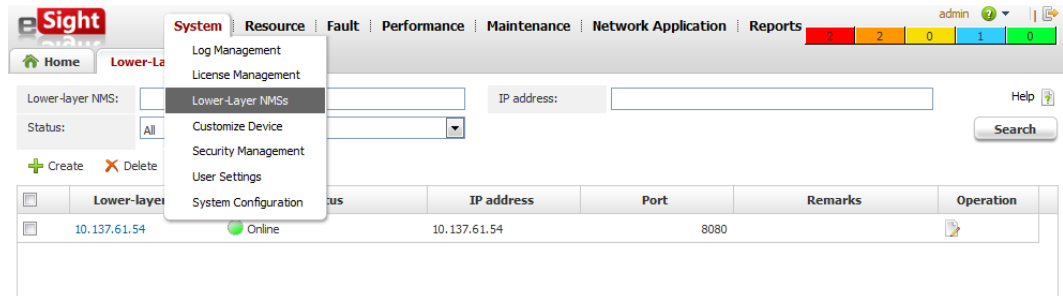
You can periodically query the lower-layer NMS status.



## Procedure

**Step 1** Choose **System > Lower-Layer NMSs** from the main menu.

**Figure 14-19** Lower-Layer NMSs



**Step 2 Optional:** Set filter parameters at the top of the pane and click **Search**.

**Step 3** Query the lower-layer NMS status.

**Figure 14-20** Lower-layer NMS status



**Step 4 Optional:** Click  to modify the lower-layer NMS remarks. Click **OK**.

**Step 5 Optional:** Click a lower-layer NMS name. On the lower-layer NMS login page that is displayed, enter the user name and password to log in to the lower-layer NMS and manage it.

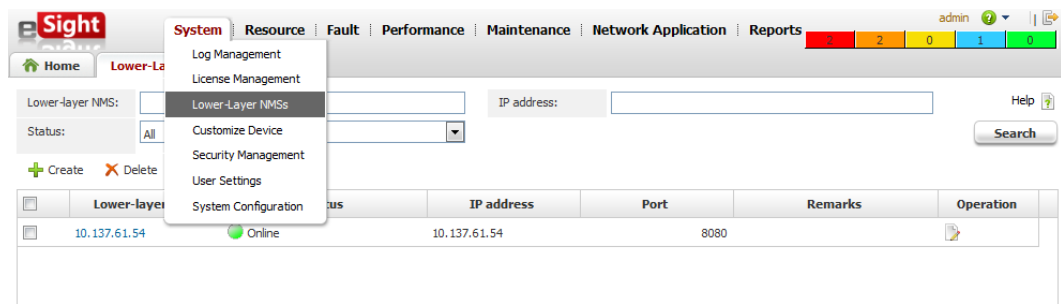
----End

### 14.4.2.3 Testing the Connectivity of Lower-Layer NMSs

You can periodically test the connectivity of lower-layer NMSs.

## Procedure

**Step 1** Choose **System > Lower-Layer NMSs** from the main menu.

**Figure 14-21** Lower-Layer NMSs

**Step 2** Click **Check Status**. eSight tests the connectivity of lower-layer NMSs.

**Figure 14-22** Check status**NOTE**

If you do not specify a lower-layer NMS, by default, eSight tests the connectivity of all lower-layer NMSs.

----End

## 14.5 Managing Licenses

You have permission for the eSight only after obtaining a license. The license file controls the resources and functions of the eSight.

### 14.5.1 Querying License Information About the eSight

You can query the information about the current license.

#### Prerequisites

You have imported a license file into the eSight.

#### Context

Table 14-6 describes the license information.

**Table 14-6** License information

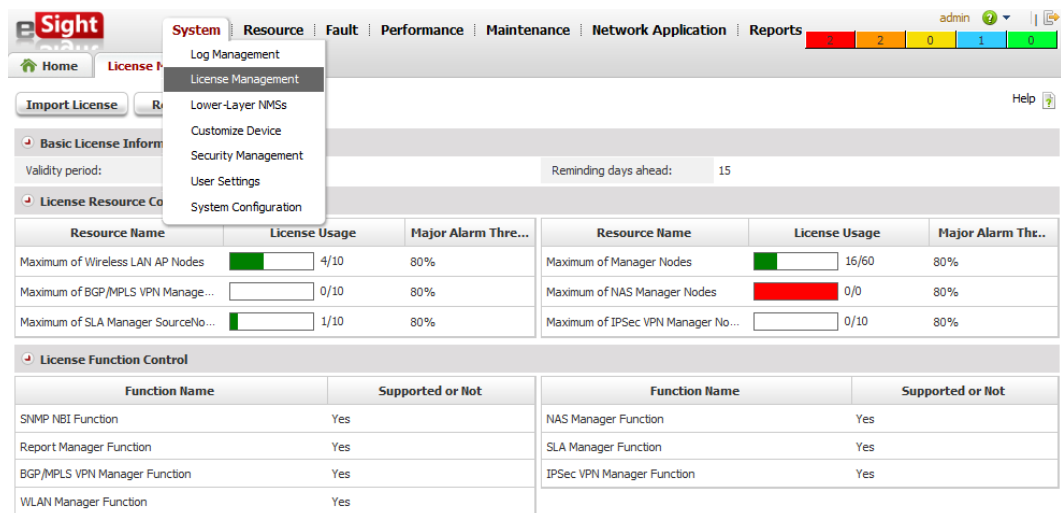
| Item                      | Attribute       | Description                         | Example    |
|---------------------------|-----------------|-------------------------------------|------------|
| Basic License Information | Validity period | Date when the license file expires. | 2011-04-14 |

| Item                     | Attribute             | Description                                                                                                                            | Example                                                                                                      |
|--------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
|                          | Reminding days ahead  | An alarm reporting that the license file will expire after the specified days is generated, and you need to import a new license file. | 15                                                                                                           |
| License Resource Control | Resource Name         | Name of the resource for license file management.                                                                                      | Client Count                                                                                                 |
|                          | License Usage         | Resource usage for license management.                                                                                                 | 30/2000<br>indicates that the number of resources managed by the license is 2000, and 30 resources are used. |
|                          | Major Alarm Threshold | An alarm is generated if the resource usage exceeds the specified alarm threshold.                                                     | 80%                                                                                                          |
| License Function Control | Function Name         | Functions provided by the eSight.                                                                                                      | SLA Manager Function                                                                                         |
|                          | Supported or Not      | Whether the function is supported by the license file.                                                                                 | Supported                                                                                                    |

## Procedure

**Step 1** Choose **System > License Management** from the main menu.

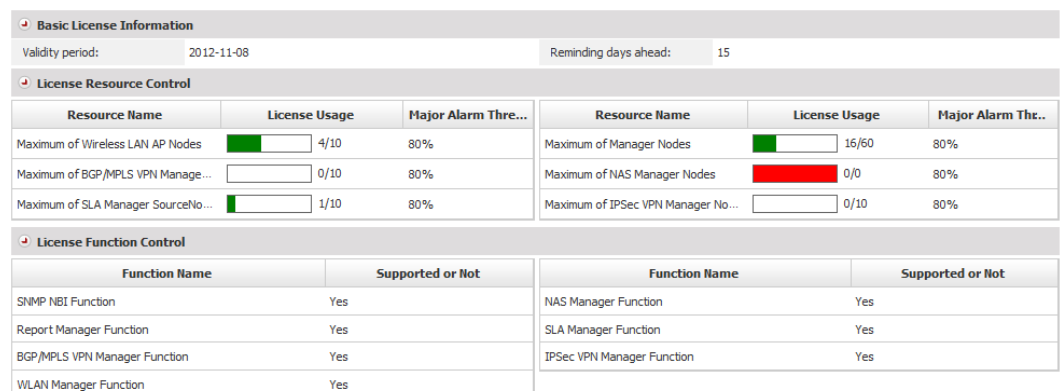
Figure 14-23 License management



In the **License Management** window, view the basic license information, license resource control and license function control.

If the current license will be expired, you need to import a new valid license in time. For details about how to import a license, see [14.5.3 Importing a License File](#).

Figure 14-24 Viewing the license of the current system



----End

## 14.5.2 Obtaining an ESN

This topic describes how to obtain an equipment serial number (ESN). When your license is going to expire, you need to obtain the ESN of your computer for applying for a new license.

### Prerequisites

The current user knows the network adapter number or MAC address of the eSight server.

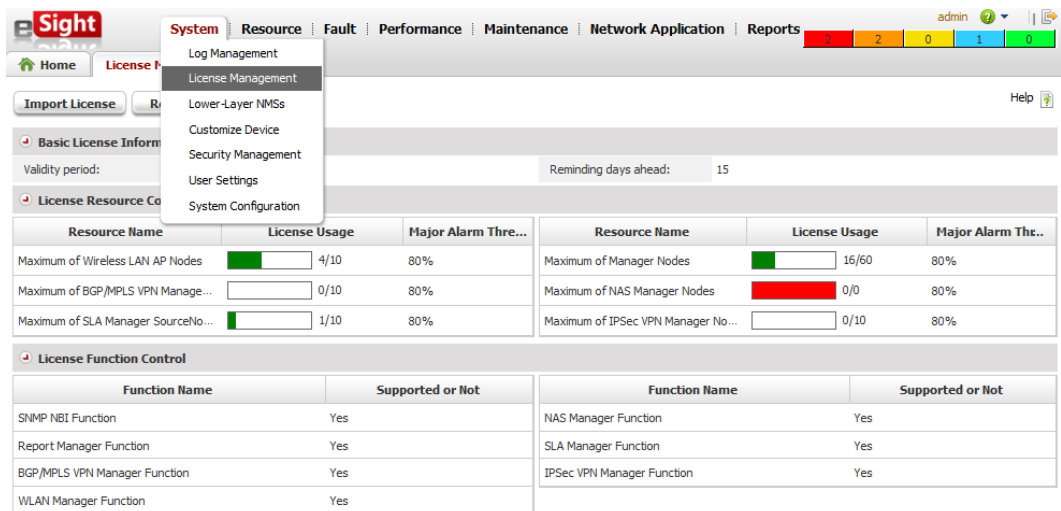
## Context

You can obtain an ESN by selecting the network adapter number or entering the MAC address.

## Procedure

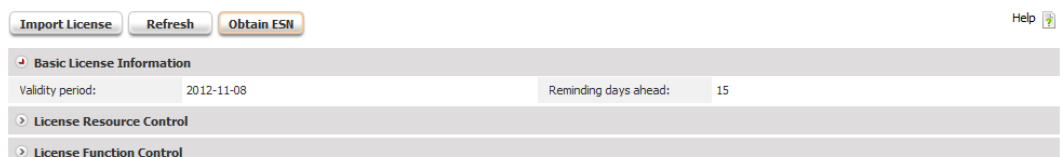
**Step 1** Choose **System > License Management** from the main menu.

**Figure 14-25** License management



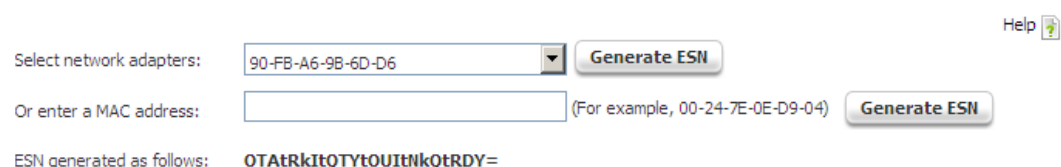
**Step 2** In the **License Management** window, click **Obtain ESN**.

**Figure 14-26** Obtaining the ESN



**Step 3** On the **Obtain ESN** page, create an ESN.

**Figure 14-27** Creating an ESN



- Obtain the ESN by selecting the network adapter.
  1. Set the network adapter.

2. Click **Generate ESN** next to the network adapter text box.
- Obtain the ESN by entering the MAC address.
1. Enter the MAC address of the computer.
2. Click **Generate ESN** next to the MAC address text box.

The generated ESN is displayed in **ESN generated as follows** in the lower part of the page.

----End

### 14.5.3 Importing a License File

When the current eSight license is invalid, expires, or cannot meet network management requirements, you must import a new license to the eSight to ensure normal services of the eSight.

#### Prerequisites

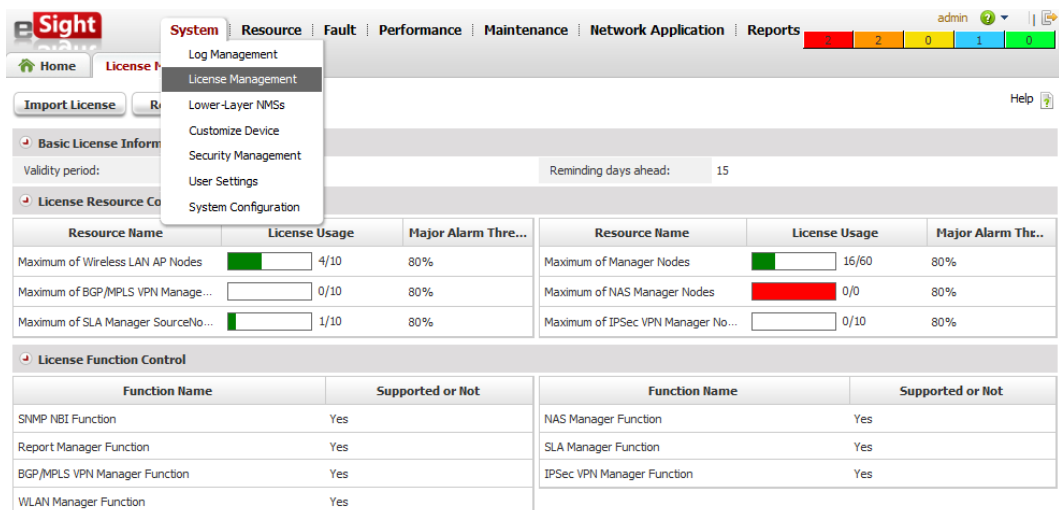
- You have the operation rights for **Update License**.
- A new license is obtained.

#### Procedure

**Step 1** Choose **System > License Management** from the main menu.

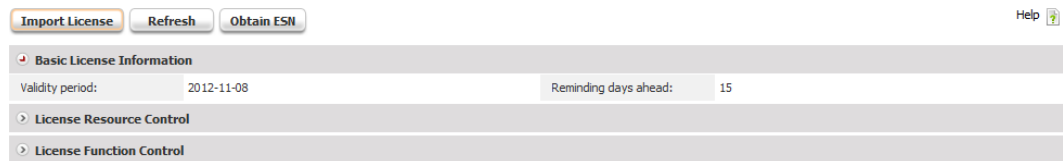
The information about the current license file is displayed.

**Figure 14-28** License management



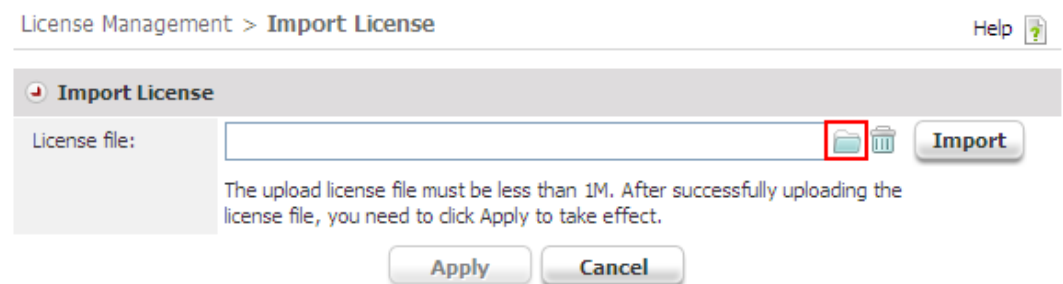
**Step 2** In the **License Management** window, click **Import License**.

**Figure 14-29** Importing the license



**Step 3** On the displayed **Import License** page, click  next to the **License file** text box and select a license file.

**Figure 14-30** Uploading the License



**Step 4** Click **Import**.

The information about the imported license file is displayed.

**Step 5** Click **Apply**.

----End

---

# 15 Routine Maintenance

---

## About This Chapter

This document describes the method of obtaining the technical support for the eSight, and how to perform routine maintenance on a daily, weekly, monthly, or quarterly basis. Through routine maintenance, you can detect and rectify the potential faults to ensure the secure, stable, and reliable running of the eSight.

### 15.1 Maintenance Item List

This topic describes the table listing the maintenance items on the basis of the maintenance period. According to the maintenance period, routine maintenance can be classified into daily maintenance, weekly maintenance, monthly maintenance, and quarterly maintenance.

### 15.2 Obtaining Technical Support

This topic describes how to obtain technical support in the case of any problems encountered during routine maintenance.

### 15.3 Daily Maintenance

This topic describes how to perform daily maintenance. Daily maintenance allows you to collect the information about the running status and trend of the eSight in real time, which improves the efficiency of handling emergencies.

### 15.4 Weekly Maintenance

This topic describes how to perform weekly maintenance. Weekly maintenance allows you to find defects such as function failure or performance degradation during the running of the eSight in a timely manner. This helps you to take proper measures to handle the problem as soon as possible and eliminate potential risks and avoid accidents.

### 15.5 Monthly Maintenance

This topic describes how to perform monthly maintenance. Monthly maintenance keeps the eSight health in a good state for a long time, which ensures secure, stable and reliable running of the system.

### 15.6 Quarterly Maintenance

This topic describes how to perform quarterly maintenance. Quarterly maintenance keeps the equipment room environment of the eSight in good condition, which ensures the reliability of power supply and related hardware.



## 15.1 Maintenance Item List

This topic describes the table listing the maintenance items on the basis of the maintenance period. According to the maintenance period, routine maintenance can be classified into daily maintenance, weekly maintenance, monthly maintenance, and quarterly maintenance.

See [Table 15-1](#) during the maintenance of the eSight.

**Table 15-1** List of maintenance items

| Maintenance Period | Routine Maintenance Task                                                      |
|--------------------|-------------------------------------------------------------------------------|
| Daily              | <a href="#">15.3.1 Browsing Current Alarms</a>                                |
|                    | <a href="#">15.3.2 Querying Security Logs</a>                                 |
| Weekly             | <a href="#">15.4.1 Checking the Disk Status of the eSight Server</a>          |
|                    | <a href="#">15.4.2 Checking the Disk Space of the eSight Server</a>           |
|                    | <a href="#">15.4.3 Checking Oracle Database Logs</a>                          |
|                    | <a href="#">15.4.4 Checking the Running Status of Anti-Virus Software</a>     |
|                    | <a href="#">15.4.5 Checking the Logs of the OS</a>                            |
|                    | <a href="#">15.4.6 Checking MySQL Database Logs</a>                           |
| Monthly            | <a href="#">15.5.1 Changing the Password of an eSight User</a>                |
|                    | <a href="#">15.5.2 Checking the Server Time of the eSight</a>                 |
|                    | <a href="#">15.5.3 Releasing the Disk Space of the eSight Server</a>          |
| Quarterly          | <a href="#">15.6.1 Checking the Equipment Room Environment</a>                |
|                    | <a href="#">15.6.2 Checking the Power Supply of the eSight Server</a>         |
|                    | <a href="#">15.6.3 Checking Hardware and Peripherals of the eSight Server</a> |

## 15.2 Obtaining Technical Support

This topic describes how to obtain technical support in the case of any problems encountered during routine maintenance.

During routine maintenance of the eSight, if there is any problem that is uncertain or hard to solve, or if you cannot find the solution to a problem from this manual, contact the customer service center of Huawei or send an email to [ChinaEnterprise\\_TAC@huawei.com](mailto:ChinaEnterprise_TAC@huawei.com). Go to <http://enterprise.huawei.com> to obtain the latest technical materials of Huawei.

Before seeking technical support, collect the relevant information.

## 15.3 Daily Maintenance

This topic describes how to perform daily maintenance. Daily maintenance allows you to collect the information about the running status and trend of the eSight in real time, which improves the efficiency of handling emergencies.

### 15.3.1 Browsing Current Alarms

You can set the filter criteria in the current alarm list to view the alarms to be concerned and handled.

#### Prerequisites

You have the operation rights for **Current Alarms Management**.

#### Context

- The current alarm list represents the merged alarms. For example, if a new alarm is reported and meets the merging rule, the information about the alarm will overwrite the previous alarm information, and the number of alarms is increased by one. If a new alarm is reported and does not meet the merging rule, it is displayed as a new record in the current alarm list.

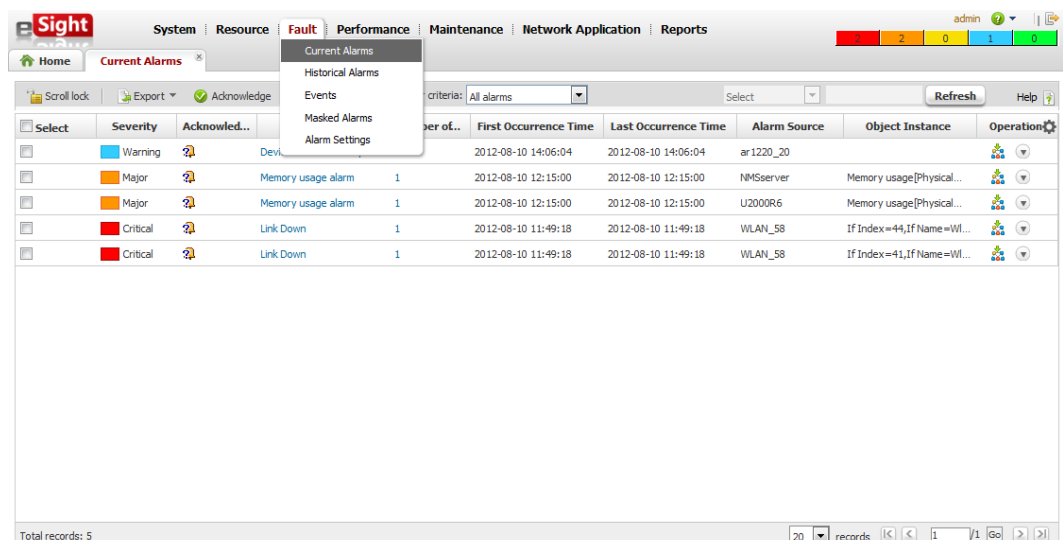
Alarm merging rule: If alarms have the same alarm source, location information, and alarm ID, the alarms are reported as only one record.

- The system always searches for alarms based on the filter criteria rule you select.

#### Procedure

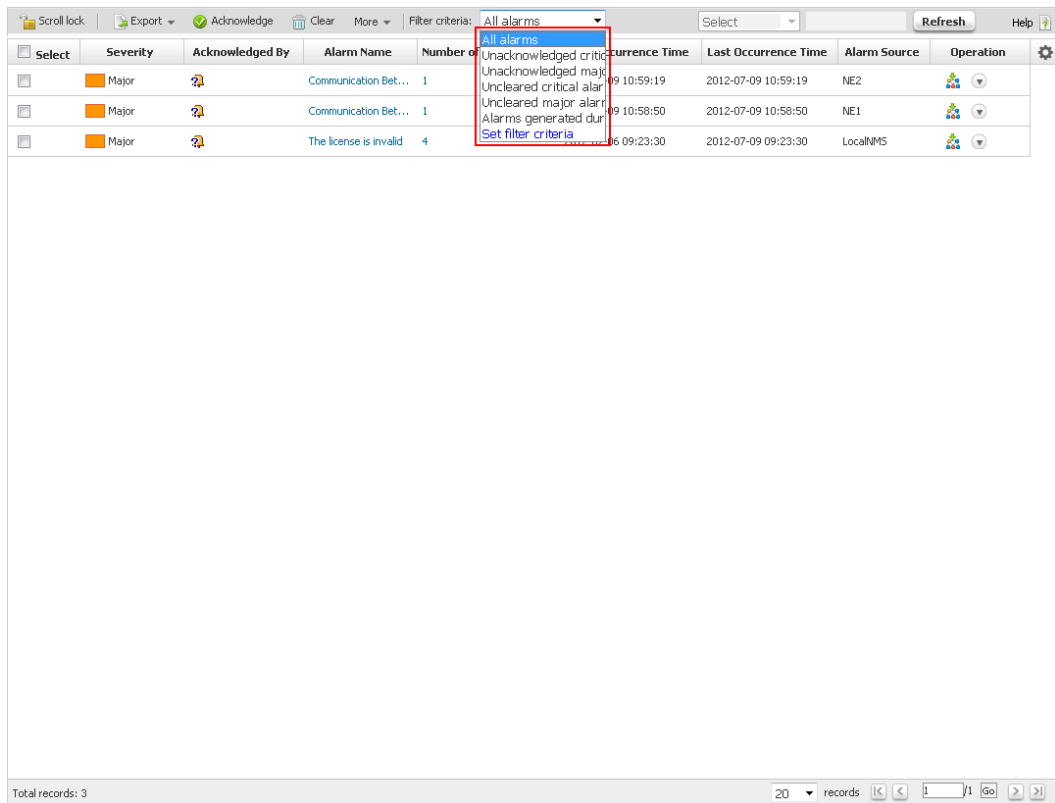
**Step 1** Choose **Fault > Current Alarms** from the main menu.

**Figure 15-1** Current alarms



**Step 2** In the **Current Alarms** window, select filter criteria rule from the **Filter criteria** drop-down list and perform a search. You can customize filter criteria rule if required. For details, see [5.3.3 Creating an Alarm Filter Rule](#).

Figure 15-2 Customizing the filter rule



**Step 3** In the **Current Alarms** window, you can perform the following steps:

| Management Alarms | Operation Method                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lock alarms       | Click <b>Scroll lock</b> . The alarms in the current list are locked.<br><br>In addition, <b>Scroll lock</b> is automatically changed to <b>Scroll unlock</b> . | If the alarms in the current list are locked, note that: <ul style="list-style-type: none"><li>Newly reported alarms can be displayed in the current alarm list only after you click <b>Scroll unlock</b>.</li><li>When an alarm is available, you can perform operations such as acknowledging or clearing the alarm, or viewing details about the alarm. When an alarm is unavailable, you cannot perform any operations on the alarm.</li></ul> <b>NOTE</b><br>If you can select the check box next to an alarm, the alarm is available. If the check box is dimmed, the alarm is unavailable. <ul style="list-style-type: none"><li>If you acknowledge or clear an</li></ul> |

| Management Alarms | Operation Method                                                                                                                                                                                                                                                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                                                                                                                                                                                                                                                                                                                                                                                                 | alarm when you click <b>Scroll lock</b> , the alarm can be updated to the historical alarm list only when you click <b>Scroll unlock</b> .                                                                                                                                                                        |
| Unlock alarms     | Click <b>Scroll unlock</b> . The eSight reports alarms to the alarm list automatically.<br>In addition, <b>Scroll unlock</b> is automatically changed to <b>Scroll lock</b> .                                                                                                                                                                                                                   | When the current alarm list is in the unlocked status, you cannot select filter rule for search. You can perform a search only after the current alarm list becomes locked.                                                                                                                                       |
| Search alarm      | You can perform a search by using either of the following methods: <ul style="list-style-type: none"><li>Click <b>Search</b> without setting any search criteria. All alarms are displayed in the current list.</li><li>When the current alarm list is in the locked state, select a search scope from the drop-down list and enter a value in the text box, and click <b>Search</b>.</li></ul> | -                                                                                                                                                                                                                                                                                                                 |
| Acknowledge       | Select one or more alarms and click <b>Acknowledge</b> .                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"><li>If the alarm is acknowledged, <b>Acknowledged By</b> displays the user who acknowledges the alarm.</li><li>If the alarm is unacknowledged, <b>Acknowledged By</b> displays .</li></ul> |
| Unacknowledge     | Select one or more alarms and choose <b>More &gt; Unacknowledge</b> .                                                                                                                                                                                                                                                                                                                           | After an alarm is unacknowledged, its status is changed from <b>Acknowledged</b> to <b>Unacknowledged</b> .                                                                                                                                                                                                       |
| Clear             | Select one or more uncleared alarms and click <b>Clear</b> .                                                                                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"><li>The background color of clear alarms is green.</li><li>The background color of uncleared alarms is white.</li></ul>                                                                                                                                                         |
| Mask Alarm        | <ol style="list-style-type: none"><li>Click  in the <b>Operation</b> column where the required alarm is located, and select <b>Mask Rules</b>.</li><li>In the <b>Mask Rules</b> dialog box, set the rule name and shielding date. Click <b>OK</b>.</li></ol>                                                 | <ul style="list-style-type: none"><li>The newly created alarm mask rule is in enabled status by default.</li><li>A mask rule is valid only to the alarms reported when the masking rule is enabled and valid. The masking rule does not take effect for the alarms reported before the masking</li></ul>          |

| Management Alarms                                       | Operation Method                                                                                                                                                                          | Description                                                                                                                            |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
|                                                         |                                                                                                                                                                                           | rule is configured. <ul style="list-style-type: none"><li>You cannot set a mask rule for a performance alarm or clear alarm.</li></ul> |
| Customize the columns to be displayed in the alarm list | Click  . On the displayed page, set the columns to be displayed in the alarm list, and click <b>OK</b> . | -                                                                                                                                      |
| Locate to Topo                                          | Click  in the <b>Operation</b> column where the required alarm record is located.                        | eSight locates the NE in the managed object that generates the alarm in the physical view.                                             |
| Redefine the severity of an alarm                       | For details, see <a href="#">5.3.4 Redefining the Severity of an Alarm</a> .                                                                                                              | After you redefine the severity of an alarm, the new alarm severity is valid only for newly reported alarms.                           |
| Alarm Details                                           | Click <b>Alarm Name</b> of which you want to view details.                                                                                                                                | The <b>Alarm Details</b> dialog box displays the name, probable cause, and proposed repair actions for the selected alarm.             |
| Alarm Logs                                              | Click <b>Number of Occurrences</b> about which you want to view the log information.                                                                                                      | The <b>Alarm Logs</b> dialog box displays the alarm log related to this alarm record.                                                  |
| Export                                                  | Select one or more alarms and choose <b>Export &gt; Selected Records</b> to export the alarm information.<br><br>If you want to export all alarms, choose <b>Export &gt; All</b> .        | -                                                                                                                                      |

----End

## 15.3.2 Querying Security Logs

You can query security logs to understand the information about eSight related security operations.

### Prerequisites

You have the operation rights for **Log Management**.

### Context

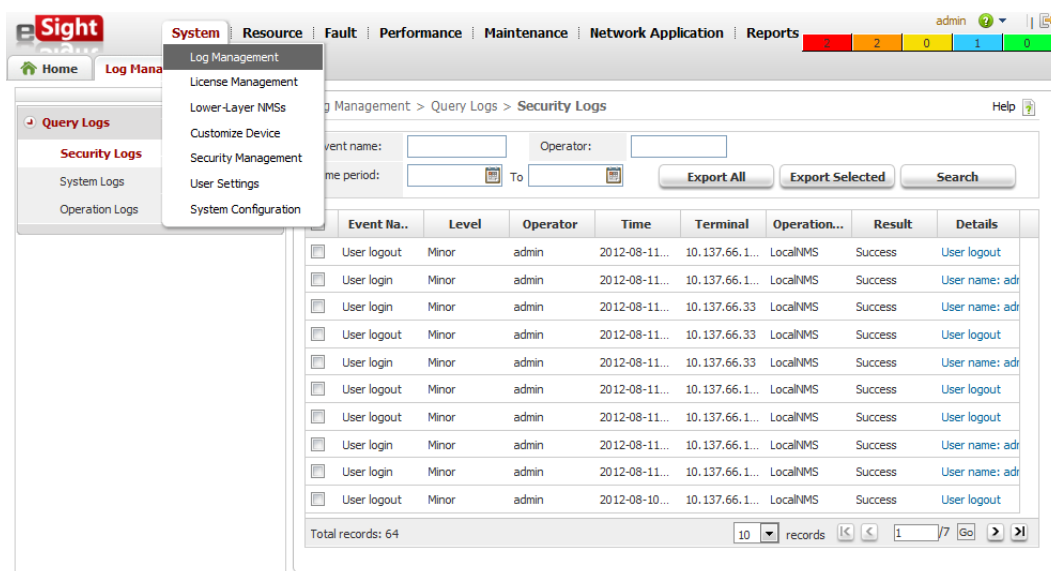
- All security logs are queried if you do not set any search criteria.

- The query result is generated based on the existing data in the database. No information is displayed if no data is generated.

## Procedure

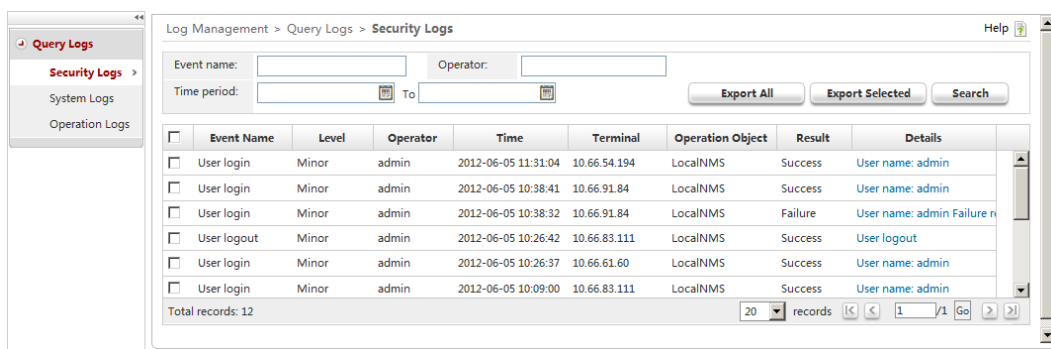
**Step 1** Choose **System > Log Management** from the main menu.

**Figure 15-3** Log management



**Step 2** In the **Log Management** window, select **Query Logs > Security Logs**.

**Figure 15-4** Querying the security logs



**Step 3** Directly view the logs or set search criteria to search for the specified logs.

After clicking the value in the **Details** column of the target log, you can view logs details in **Security Log Details**.



### NOTE

A maximum of 800 characters can be displayed in **Security Log Details**. Contents other than the first 800 characters are displayed as ....

----End

## Follow-up Procedure

The following table describes the operations that can be performed on the **Security Logs** page.

| Export Security Logs              | Operation Method                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Export all security logs          | <ol style="list-style-type: none"><li>1. Click <b>Export All</b> to export all security logs.</li><li>2. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>3. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p>                                                                                                              |
| Export the selected security logs | <ol style="list-style-type: none"><li>1. In the log list, select the check box before <b>Event Name</b> of the required log.</li><li>2. Click <b>Export Selected</b> to export the selected security logs.</li><li>3. In the <b>File Download</b> dialog box, click <b>Save</b>.</li><li>4. Select a save path and click <b>Save</b>.</li></ol> <p><b>NOTE</b><br/>Log files must be saved in <b>.csv</b> format.</p> |

## 15.4 Weekly Maintenance

This topic describes how to perform weekly maintenance. Weekly maintenance allows you to find defects such as function failure or performance degradation during the running of the eSight in a timely manner. This helps you to take proper measures to handle the problem as soon as possible and eliminate potential risks and avoid accidents.

### 15.4.1 Checking the Disk Status of the eSight Server

This topic describes how to check the disk status of the eSight server. If the disk status is abnormal, the data may be lost and the eSight cannot be properly used. Therefore, you must check the disk status periodically. If any disk fault occurs, clear the fault or replace the disk in time.

#### Procedure

- Perform the following steps in a Single-Server System (Windows):
  1. In the **My Computer** window, select a disk, right-click, and then choose **Attribute** from the shortcut menu.
  2. In the dialog box that is displayed, click the **Tools** tab.
  3. In the **Check Error** area, click **Start Check**.
  4. In the dialog box that is displayed, select related check items and click **Start**. Then, check the disk status as prompted.
- Perform the following steps in a Single-Server System (SUSE Linux-distributed):
  1. Open a CLI. Then, run the following commands to switch to the **root** user:  

```
$ su
```

Password: *password\_of\_user\_root*

2. Run the following commands to view the physical status of the disk on the current server:

```
smartctl -H /dev/sda
```

----End

## Reference Standard

If the following standards are met, the disk status is normal:

1. On a Windows single-server system, after the disk error check is performed, a messages is displayed indicating that the device or disk has no error.
2. After you run the **smartctl -H /dev/sda** command, if the **SMART overall-health self-assessment test result** of the disk is **PASSED**, the physical status of the disk is normal.

## Troubleshooting

If a disk does not function properly, contact the equipment supplier to repair or replace the disk in a timely manner.

### 15.4.2 Checking the Disk Space of the eSight Server

This topic describes how to check the disk space of the eSight server. If the disk space usage exceeds 80%, the running efficiency of the eSight may be affected, or the server may not be started. Therefore, you must periodically check the disk space and clear the space in a timely manner.

## Procedure

- Perform the following steps on Windows:

In **Server Manager**, choose **Storage > Disk Management**, and view the disk space of the eSight server. The information to be viewed includes the disk space usage of the OS and eSight.

- Perform the following steps on SUSE Linux:

You can view the disk space of the server by using command lines. The following describes how to view the disk space by running commands:

1. Log in to the OS as the root user.
2. Run the following command to view the disk space usage on the server:

```
df -k
```

----End

## Reference Standard

Generally, the space usage of each disk should be less than 80%.



## 15.4.3 Checking Oracle Database Logs

This topic describes how to check Oracle database logs.

### Background

eSight uses the Oracle database.

### Procedure

Check the Oracle database log file

`$ORACLE_BASE/diag/rdbms/esight/$ORACLE_SID/trace/alert_$ORACLE_SID.log`.



#### NOTE

The values of **ORACLE\_BASE** and **ORACLE\_SID** vary according to site scenario.

### Expected Results

The log file contains no information indicating Oracle database running errors.

### Troubleshooting

See error information in the log file to rectify faults. If a fault persists, contact Oracle technical support.

## 15.4.4 Checking the Running Status of Anti-Virus Software

This topic describes how to check the running status of anti-virus software. You must install OS patches in time, upgrade the anti-virus software, and search for viruses to prevent the server and computer from affecting network viruses and to ensure the normal running of the eSight.

### Procedure

Install OS patches in time, upgrade anti-virus software, and periodically search for viruses.

### Reference Standard

No virus is found.

### Troubleshooting

If any virus is found, clear it at once. If the troubleshooting fails, reinstall the OS.

## 15.4.5 Checking the Logs of the OS

This topic describes how to check the running status of the OS by the related log information.

### Procedure

- Windows:
  1. Choose **Start > Control Panel > Administrative Tools > Event Viewer**.

2. In the window that is displayed, view the log and event information and check whether the information about the abnormal events that affect system running exists.



#### NOTE

For the method of using the Event Browser, refer to the OS Help or the user manuals.

- Perform the following steps in a SUSE Linux:
  1. Log in to the operating system as the **root** user.
  2. Run the following command to navigate to the path where the log file is saved:
    - SUSE Linux: # **cd /var/log**
  3. Run the following command to quickly search for error information:  
# **grep error messages\***

If there is no error information, no information is displayed in the command output.

If there is error information, all error information contained in the file is displayed in the command output.

----End

## Reference Standard

- On Windows:  
The **Error** information is not displayed in **Event Viewer**.
- In a SUSE Linux:  
The **error** information is not contained in the log file of the OS.



#### TIP

Run the following command to view all OS log files, namely, files whose names start with **messages** (including error logs and non-error logs):

# **more messages\***

## Troubleshooting

If a fault occurs, rectify it according to the error information contained in the log file. If the problem still persists, contact technical support engineers of Huawei.

## 15.4.6 Checking MySQL Database Logs

This topic describes how to check MySQL database logs.

### Background

eSight uses the MySQL database.

### Procedure

Check the .err log file in \$eSight\_ROOT\MySQL\data.

### Expected Results

The log file contains no information indicating MySQL database running errors.

## Troubleshooting

See error information in the log file to rectify faults. If a fault persists, contact Huawei technical support.

## 15.5 Monthly Maintenance

This topic describes how to perform monthly maintenance. Monthly maintenance keeps the eSight health in a good state for a long time, which ensures secure, stable and reliable running of the system.

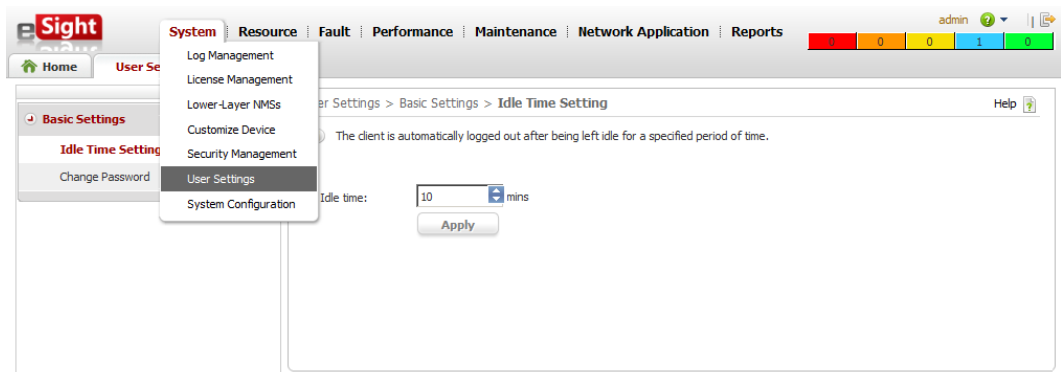
### 15.5.1 Changing the Password of an eSight User

This topic describes how to change the password of the current user.

#### Procedure

**Step 1** Choose **System > User Settings** from the main menu.

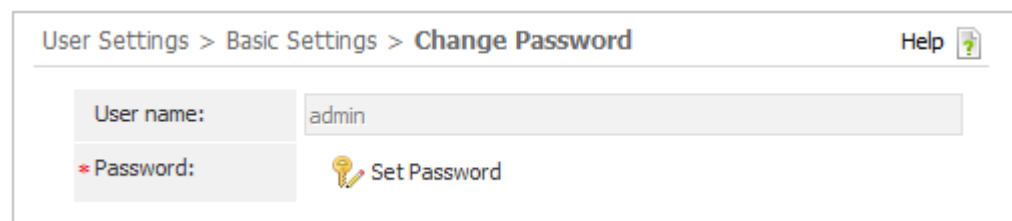
**Figure 15-5** Setting a user



**Step 2** In the **User Settings** window, choose **Basic Settings > Change Password**.

**Step 3** On the **Change Password** page, click **Set Password**.

**Figure 15-6** Setting the password



**Step 4** In the displayed window, set **Old password**, **New password**, and **Confirm password**.

**Figure 15-7** Changing the password

**The password must meet the following rules:**

- 1, The password is different from the user name.
- 2, The length ranges from 6 to 32 characters.
- 3, The number of occurrences of a character in a password cannot exceed 3.
- 4, The password contains uppercase and lowercase letters and digits.
- 5, The password cannot be the same as the latest 3 passwords.
- 6, The interval between two password changes must be greater than 5 minutes.

**Step 5** Click **OK**.

----End

## 15.5.2 Checking the Server Time of the eSight

This topic describes how to check whether the server time of the eSight is correct.

### Procedure

- Perform the following steps on Windows:
  1. Open the **Control Panel** window. Then, double-click the **Data/Time** icon.
  2. In the dialog box that is displayed, click the **Data&Time** tab, and then check the system time.
- Perform the following steps in a SUSE Linux:
  1. Log in to the OS as the **root** user.
  2. Run the following command to view the current server time:
 

```
date
```

----End

### Reference Standard

The server time is correct.



### CAUTION

- Incorrect time in the alarm information causes incorrect alarm occurrence sequence, alarm lasting period, and alarm association.
  - Incorrect time in performance data recording and statistics affects statistics precision.
- 

## 15.5.3 Releasing the Disk Space of the eSight Server

This topic describes how to clear the disk space of the eSight server to save resources.

### Prerequisites



### CAUTION

Make sure all files to be deleted are useless. Do not delete files generated in the recent three days.

---

### Procedure

- Perform the following steps on Windows:
  1. Log in to the Windows OS as a user with the administrator rights.
  2. Delete the useless and outdated abnormal event files that are automatically dumped. The default directory is **\$eSight\_ROOT/AppBase/var/runtime.center/data/dump/**.
  3. Delete the outdated and useless running log files. The default directory is **\$eSight\_ROOT/AppBase/var/runtime.center/log/**.
  4. Delete other outdated and unnecessary files, such as the program installation files and patch installation files of earlier versions.
- Do as follows in the Single-Server System (SUSE Linux):
  1. Log in to the OS as the **root** user.
  2. Delete the useless and outdated abnormal event files that are automatically dumped. The default directory is **\$eSight\_ROOT/AppBase/var/runtime.center/data/dump/**.
  3. Delete the outdated and useless running log files. The default directory is **\$eSight\_ROOT/AppBase/var/runtime.center/log/**.
  4. Delete other outdated and unnecessary files, such as the program installation files and patch installation files of earlier versions.

----End

## 15.6 Quarterly Maintenance

This topic describes how to perform quarterly maintenance. Quarterly maintenance keeps the equipment room environment of the eSight in good condition, which ensures the reliability of power supply and related hardware.

## 15.6.1 Checking the Equipment Room Environment

This topic describes how to check the environment of the equipment room.

### Procedure

- Step 1** Check the temperature, humidity, and dust-proof conditions of the equipment room.
- Step 2** Check the power supply system, air filter, fire alarm system, and lightning proof system.
- End

### Reference Standard

**Table 15-2** Reference Standard

| Item                   | Index                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------|
| Temperature            | Range: 15°C-35°C                                                                                     |
| Humidity               | Range: 40%-65%                                                                                       |
| Dust condition         | Clear and spotless                                                                                   |
| Power supply           | The power supply is normal, which ensures the normal running of the equipment in the equipment room. |
| Air filter             | The air filter is clean and the cabinet is in good ventilation condition.                            |
| Fire alarm system      | The fire alarm system works properly and can effectively sense fire accidents.                       |
| Lightning proof system | The lightning proof system works properly and can effectively prevent the lightning stroke.          |

### Troubleshooting

1. Adjust the temperature and humidity properly. Make sure that the doors and windows are airtight.
2. Remove the air filter from the cabinet, remove the dusts on the air filter with the vacuum cleaner, and then place the air filter in the cabinet.
3. Repair the power supply system, fire alarm system, and lightning proof system to ensure that the equipment in the equipment room works properly and securely.

## 15.6.2 Checking the Power Supply of the eSight Server

This topic describes how to check whether the power supply of the eSight server is normal.

### Prerequisites

The eSight server must be powered on.

## Procedure

- Step 1** Check whether the power indicators of the server and monitor are normal.
- Step 2** Perform the following steps on SUSE Linux, run the following commands to view information about the power supply faults in the logs recorded in recent days:

```
more /var/log/messages|grep PSU
```

```
more /var/log/warn|grep PSU
```

Information similar to the following is displayed:

```
Jun 23 16:53:40 Server rmclomv: [ID 632913 kern.error] Input power unavailable for PSU
@ PS1.
```

If **error** or **WARN** is contained in the command output, the power supply is in the abnormal state.

- Step 3** Check the faults of the external power of the system.
- Step 4** Confirm that the power supply of the server is normal.

----End

## Reference Standard

In normal cases, all the power indicators of the server peripherals turn green and all fault indicators are off.

## Troubleshooting

If a fault about the external power of the system occurs, the system does not record the related information. In this case, you must detect the external power supply and circuits in other methods. For details, refer to the delivery manual of the server. If you encounter complicated problems, contact the manufacturer to repair or replace the server.

## 15.6.3 Checking Hardware and Peripherals of the eSight Server

This topic describes how to check the status of hardware and peripherals of the eSight server.

## Prerequisites

The eSight server is powered on.

## Procedure

- Step 1** Refer to the delivery manual of the server according to the server model to check the hardware of the server.
- Step 2** If a disk array is used, refer to the related manual of the disk array according to the disk array model to check the hardware of the server.
- Step 3** Check whether the CD/DVD-ROM runs properly.

----End

## Reference Standard

In normal cases, the server and peripherals run properly and all indicators work properly.

## Troubleshooting

Refer to the delivery manual according to the models of the server and peripherals to locate faults. If you encounter complicated problems, contact the manufacturer to repair or replace the server.



# 16 FAQs

## About This Chapter

This topic describes the solutions to the frequently asked questions (FAQs) about the eSight.

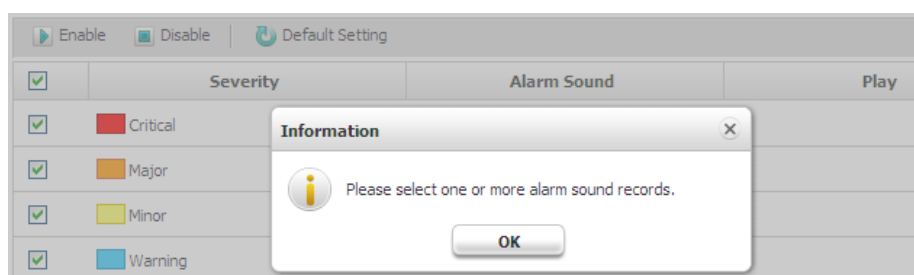
- 16.1 How Do I Solve the Problem When Internet Explorer 8 Displays a Message Indicating that No Alarm Sound Is Selected?
- 16.2 How to Solve the Problem That the Web Browser Displays a Message Indicating That the Security Certificate Is Incorrect During Login to the eSight?
- 16.3 How Do I Resolve the Problem That A Security Alarm Is Generated When Logging In to the eSight By Internet Explorer 8?
- 16.4 What Do I Do When a Few English Fields Cannot Be Displayed Completely During the Process of Accessing the eSight GUI in English by Mozilla Firefox in Chinese?
- 16.5 What Do I Do When Adobe Flash Player Provided by the eSight Cannot Be Installed in Internet Explorer?
- 16.6 How to Resolve the Problem that the Flash Plug-in Is Down When the eSight Flash Is Opened Using a Browser
- 16.7 What Do I Do When Arabic Characters Appear Garbled After Being Copied?
- 16.8 How Do I Resolve the Nesting Problems of the eSight Page after Clearing the Cache from Firefox?
- 16.9 How Do I Install an SSL Certificate for the Email Server?
- 16.10 How Do I Customize Connection Rules for Ports Required by eSight?
- 16.11 How Do I Solve the Problem When eSight Cannot Manage an NE Due to Junk Data Caused by Unexpected Database Stop?
- 16.12 How Do I Solve the Problem When the eSight GUI Fails to Display Properly and the GUI Displays Page-wide Code When I Log Out?
- 16.13 How Do I Set SNMP Parameters on a PC?
- 16.14 How Do I Prevent Problems Caused by eSight Server System Time Change?
- 16.15 When I Use IE8 to Import Sheets, the System Displays an Incorrect Path. How Do I Solve the Problem?
- 16.16 How Do I Solve the Service Session Failure That Occurs When I Log In to eSight?

## 16.1 How Do I Solve the Problem When Internet Explorer 8 Displays a Message Indicating that No Alarm Sound Is Selected?

### Symptom

Internet Explorer 8 displays a message indicating that no alarm sound is selected.

**Figure 16-1** Error message



### Possible Causes

This problem occurs because Compatibility View is enabled in Internet Explorer 8. To solve the problem, disable Compatibility View for Internet Explorer 8.

### Procedure

- Step 1** Open Internet Explorer 8.
  - Step 2** Choose **Tools > Developer Tools**.
  - Step 3** On the **Developer Tools** page that is displayed, set **Browser Mode** to **Internet Explorer 8** and **Document Mode** to **Internet Explorer 8 Standards**.
  - Step 4** Close the **Developer Tools** page, and log in to eSight again.
- End

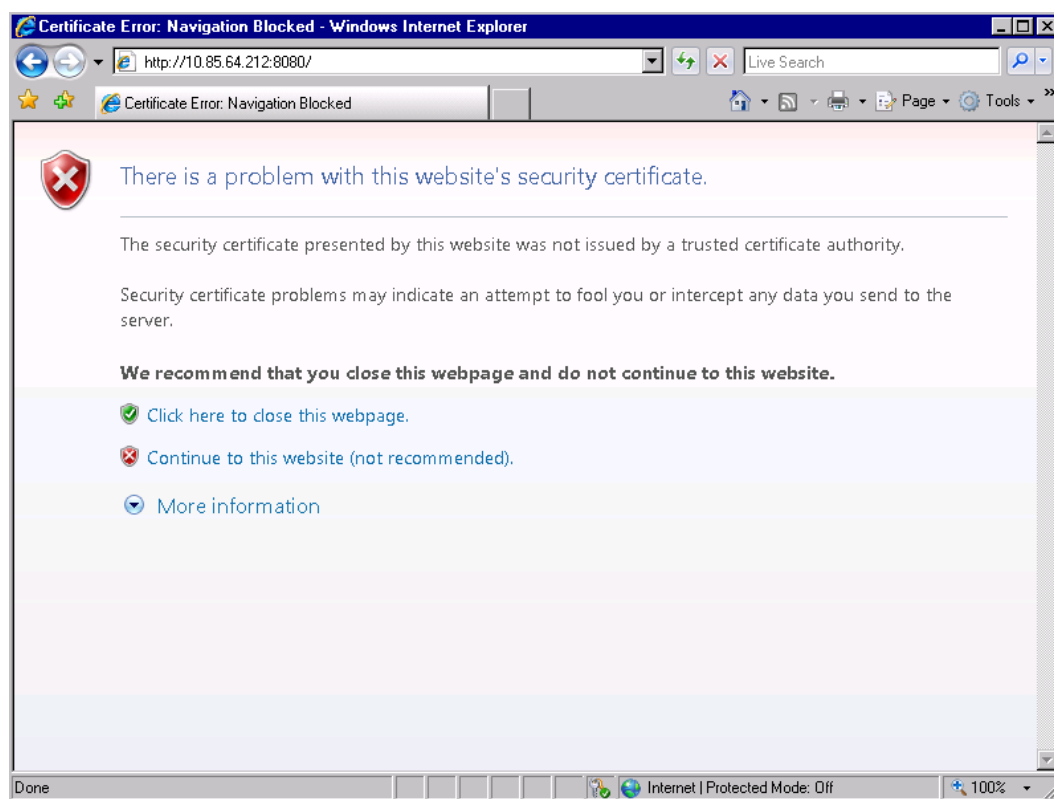
## 16.2 How to Solve the Problem That the Web Browser Displays a Message Indicating That the Security Certificate Is Incorrect During Login to the eSight?

### Symptom

Internet Explorer or Mozilla Firefox displays a message indicating that the security certificate is incorrect when you log in to the eSight.

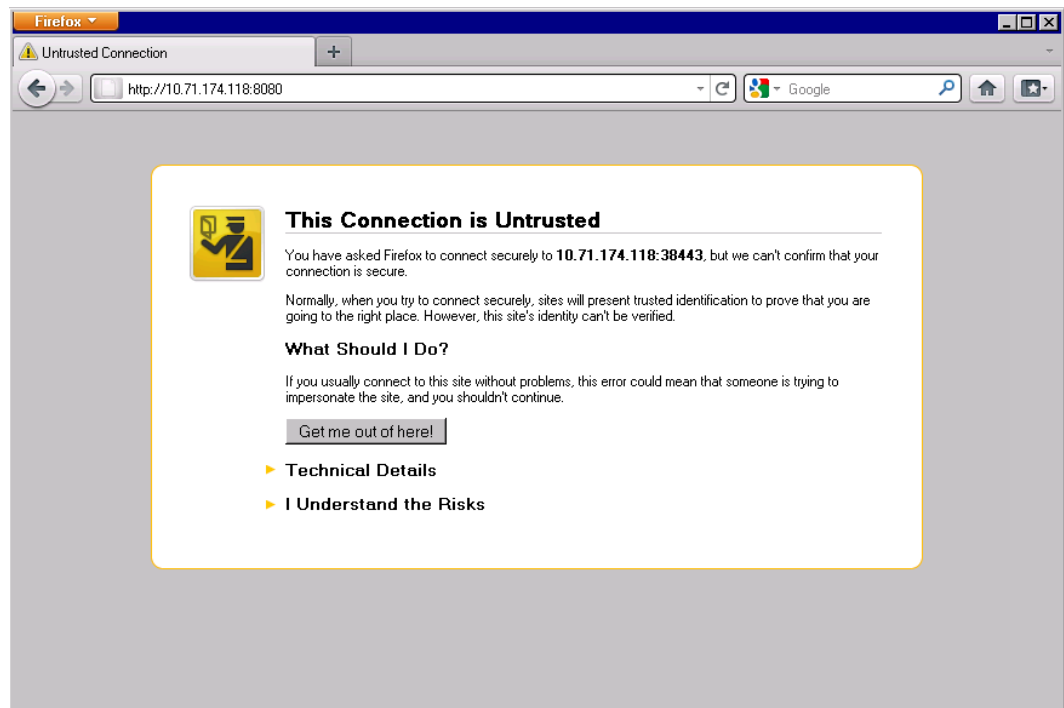
- The following figure shows the security certificate error prompted by Internet Explorer.

**Figure 16-2** Error message (IE)



- The following figure shows the security certificate error prompted by Firefox.

**Figure 16-3** Error message (Firefox)



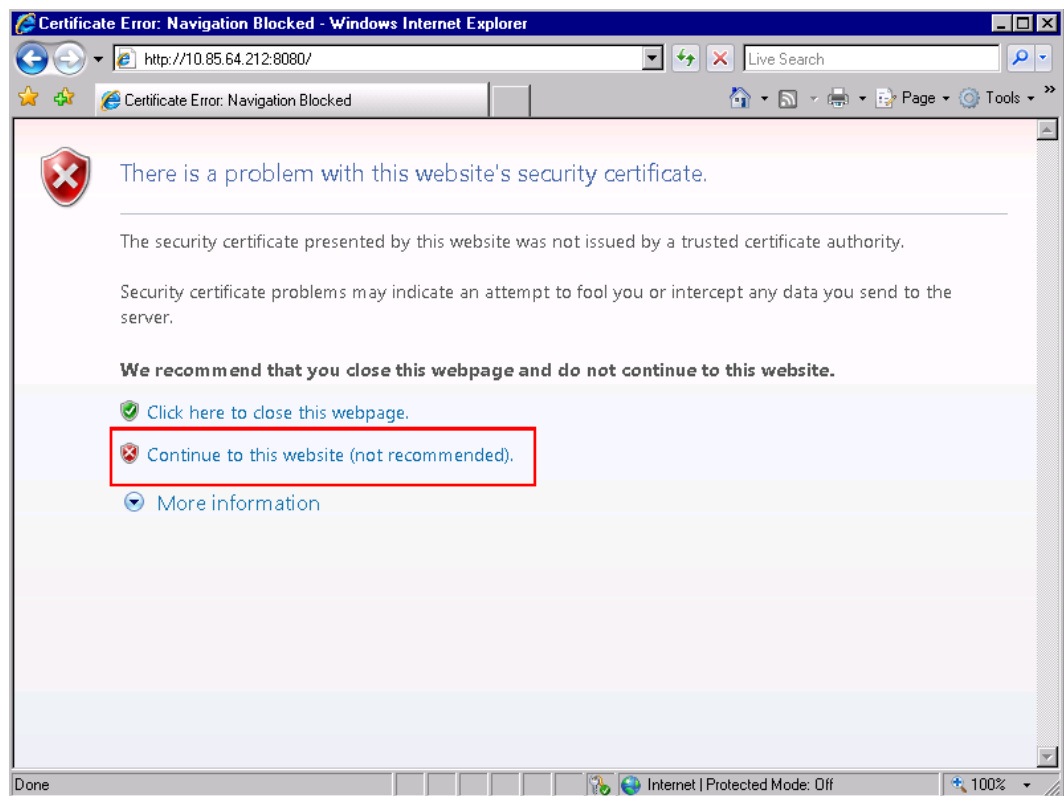
## Possible Causes

You need to install a security certificate.

## Procedure

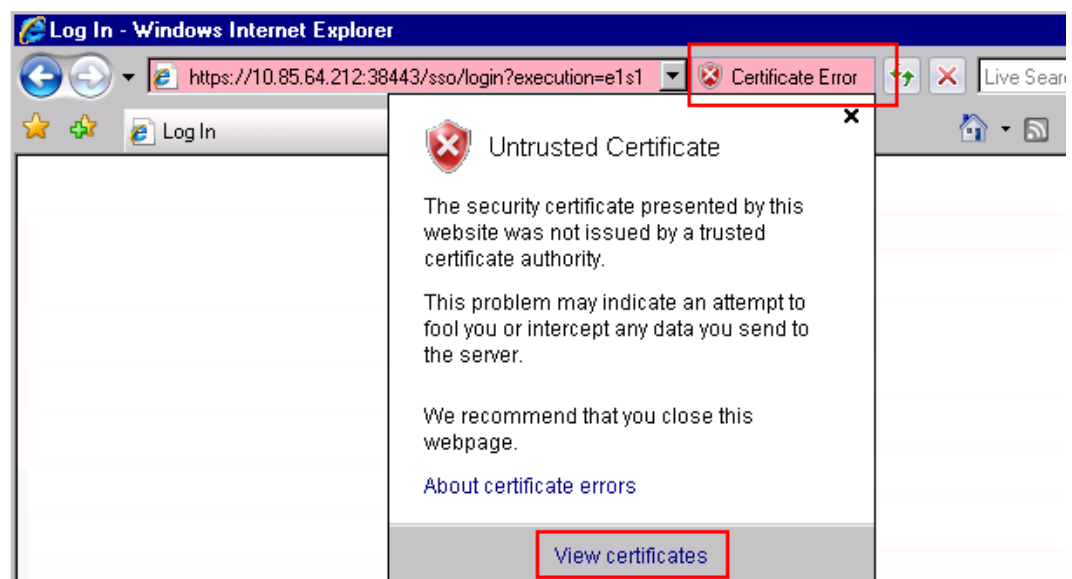
- Install the security certificate in Internet Explorer.
1. On the error message page, click **Continue to this website (not recommended)**.

**Figure 16-4** Error message (IE)



2. Click **Certificate Error**. In the **Untrusted Certificate** dialog box, click **View certificates**.

**Figure 16-5** Untrusted Certificate



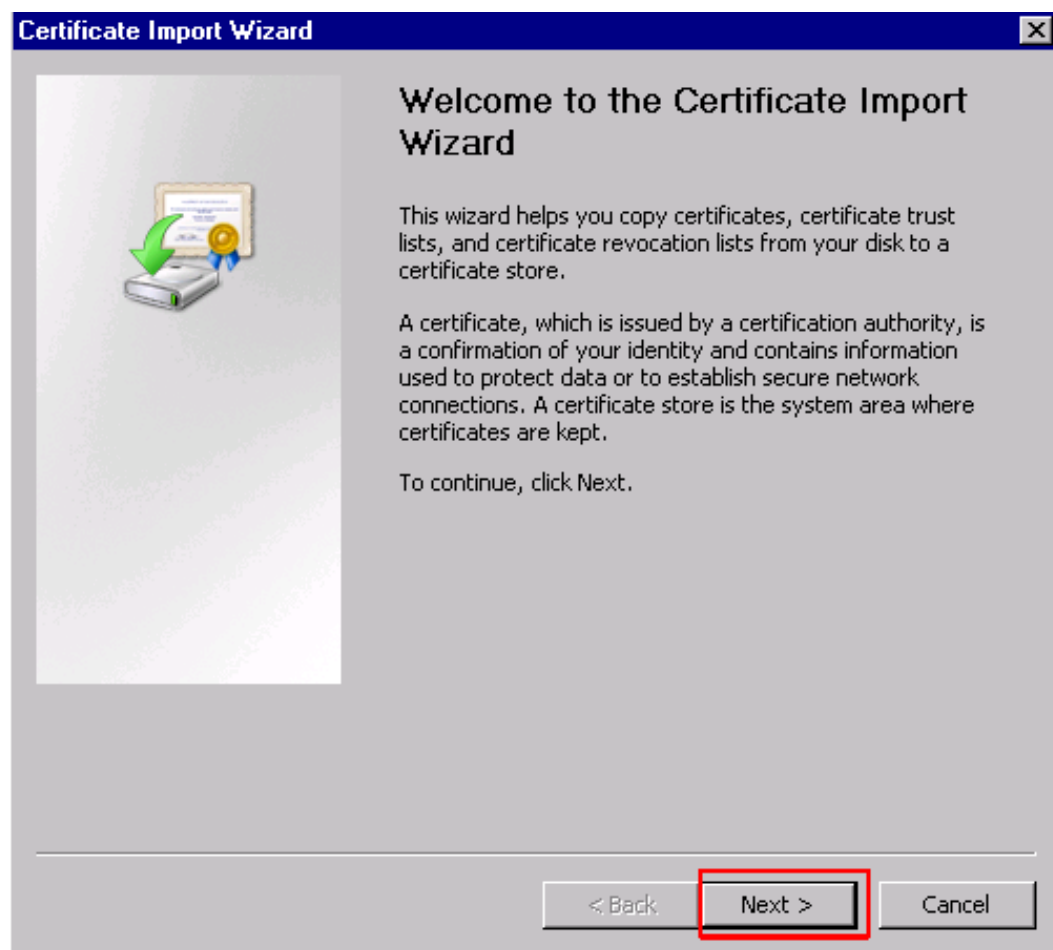
3. On the **General** tab page, click **Install Certificate**.

**Figure 16-6** Certificate Information



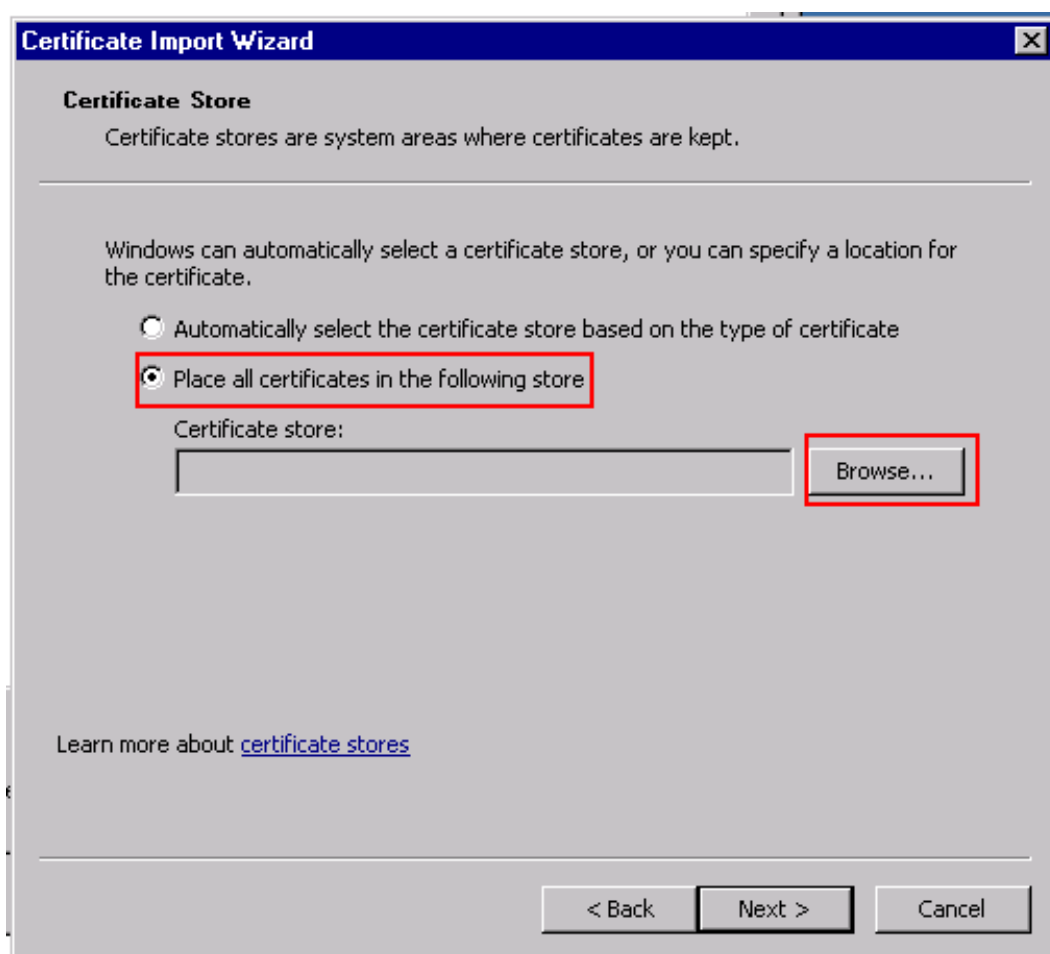
4. In the **Certificate Import Wizard** dialog box, click **Next**.

**Figure 16-7** Certificate Import Wizard



5. Select **Place all certificates in the following store** and click **Browse**.

**Figure 16-8** Import Certificate



6. In the **Select Certificate Store** dialog box, select **Trusted Root Certification Authorities** and click **OK**.

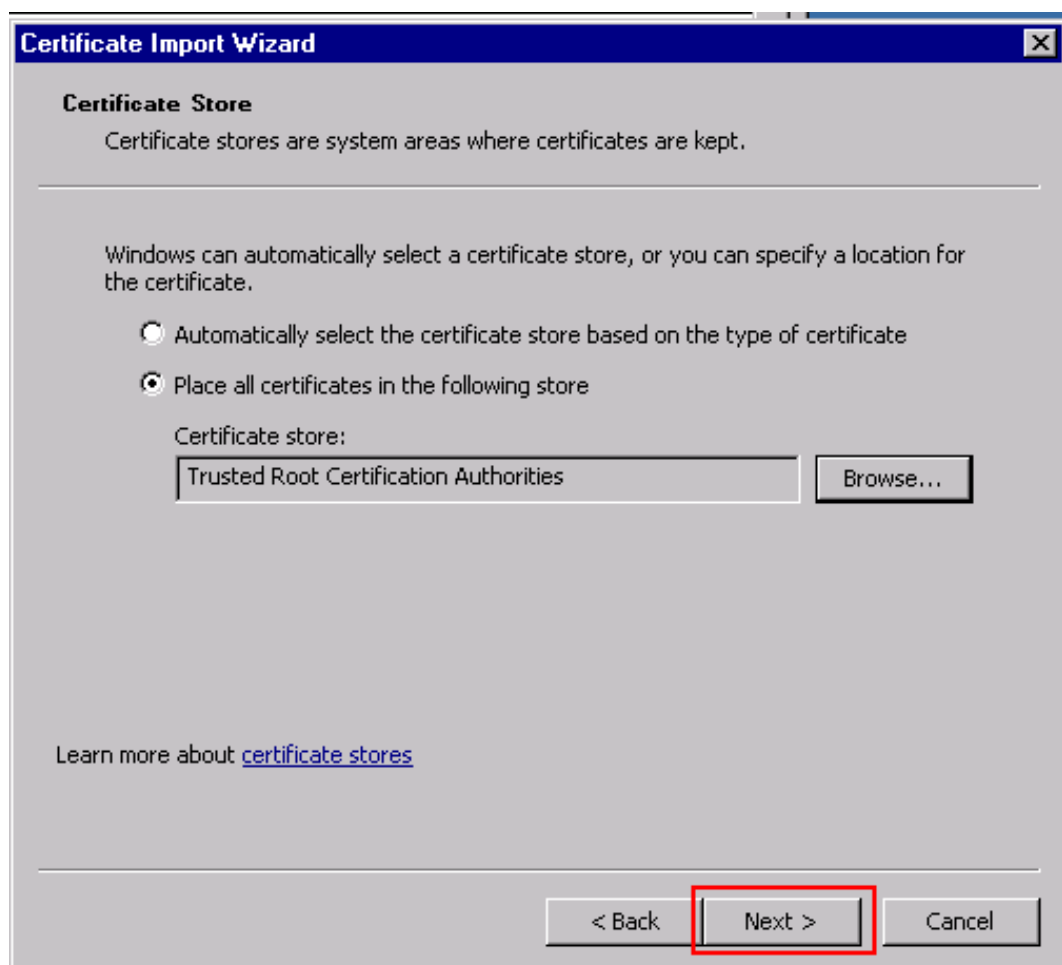


**Figure 16-9** Select Certificate Store



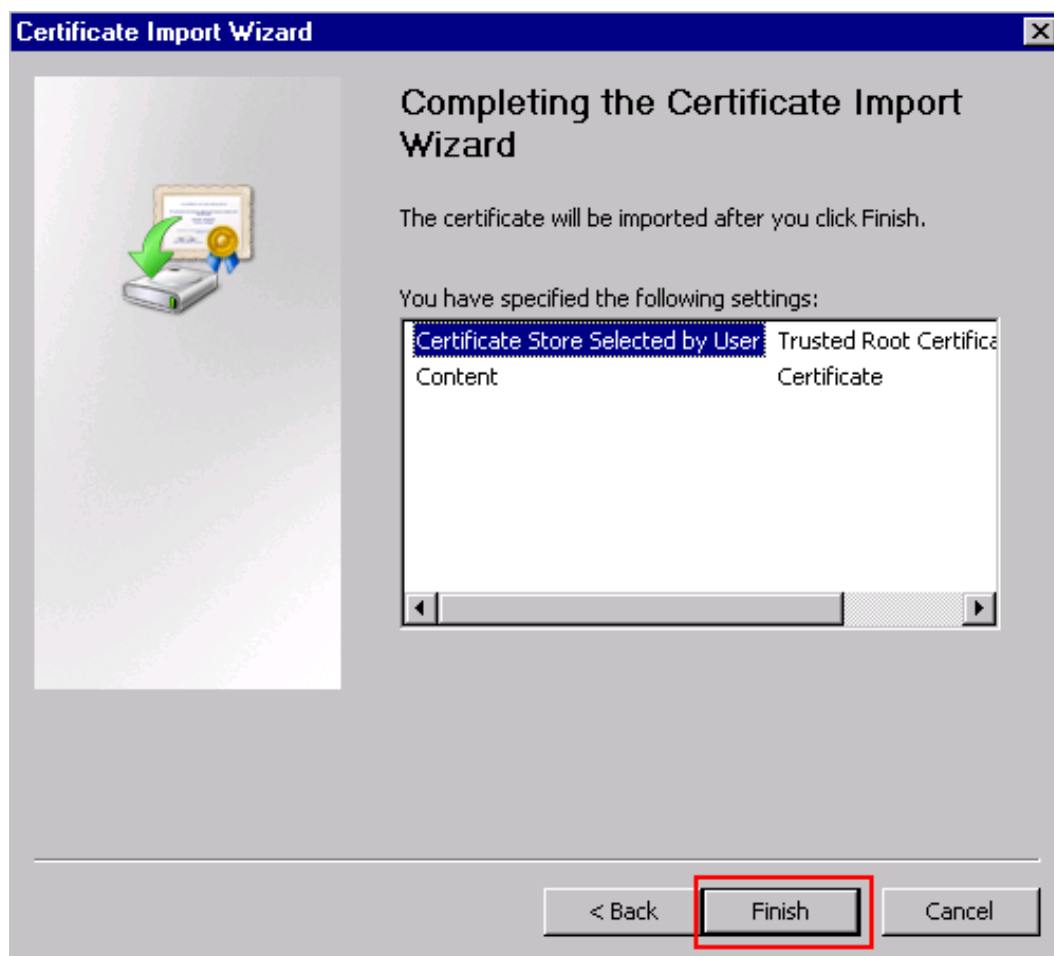
7. Click **Next**.

**Figure 16-10** Certificate Store



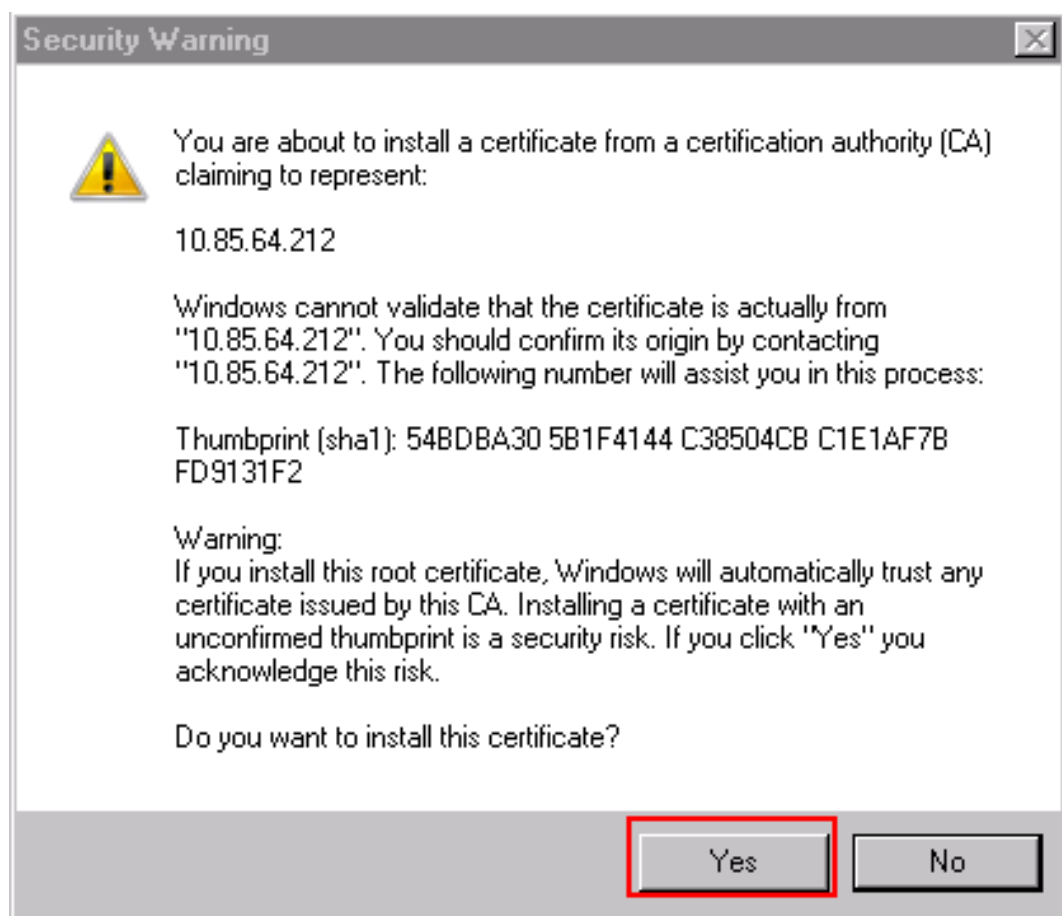
8. In the **Certificate Import Wizard** dialog box, click **Finish**.

**Figure 16-11** Complete the Certificate Import Wizard



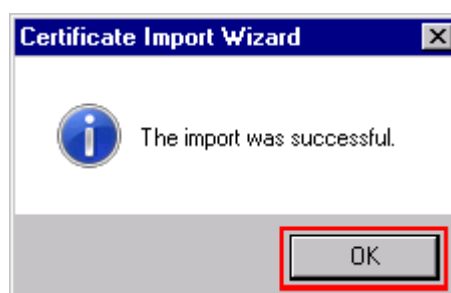
9. In the **Security Warning** dialog box, click **Yes**.

**Figure 16-12** Install Certificate



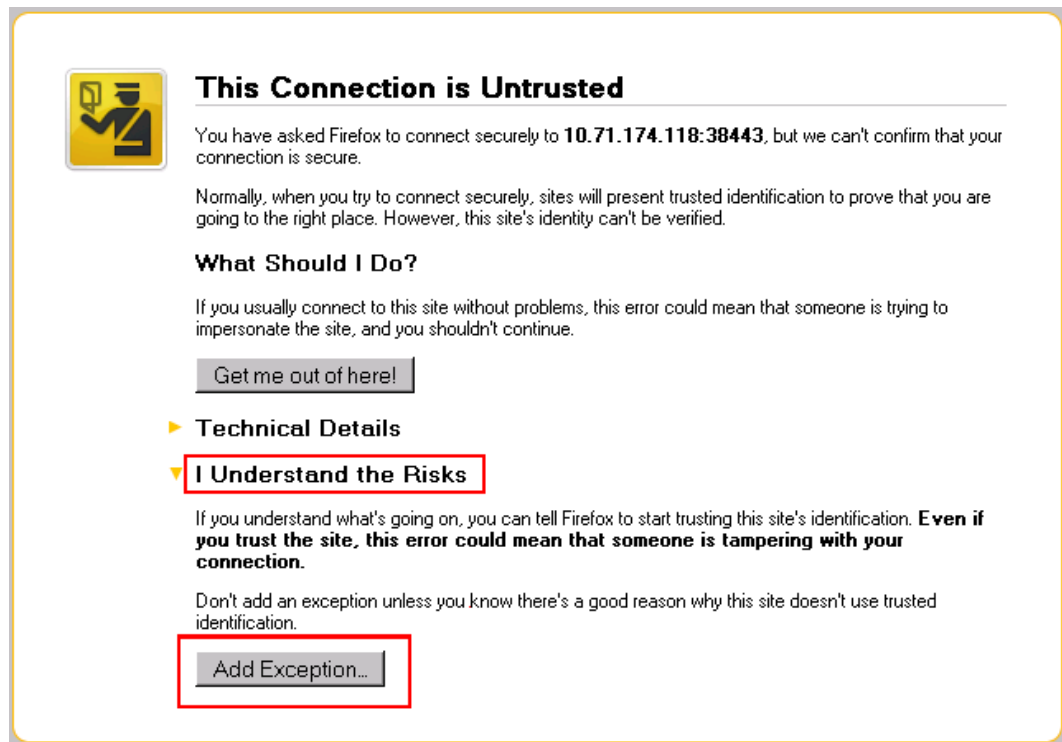
10. In the **Certificate Import Wizard** dialog box, click **OK**.

**Figure 16-13** Certificate importing succeeded



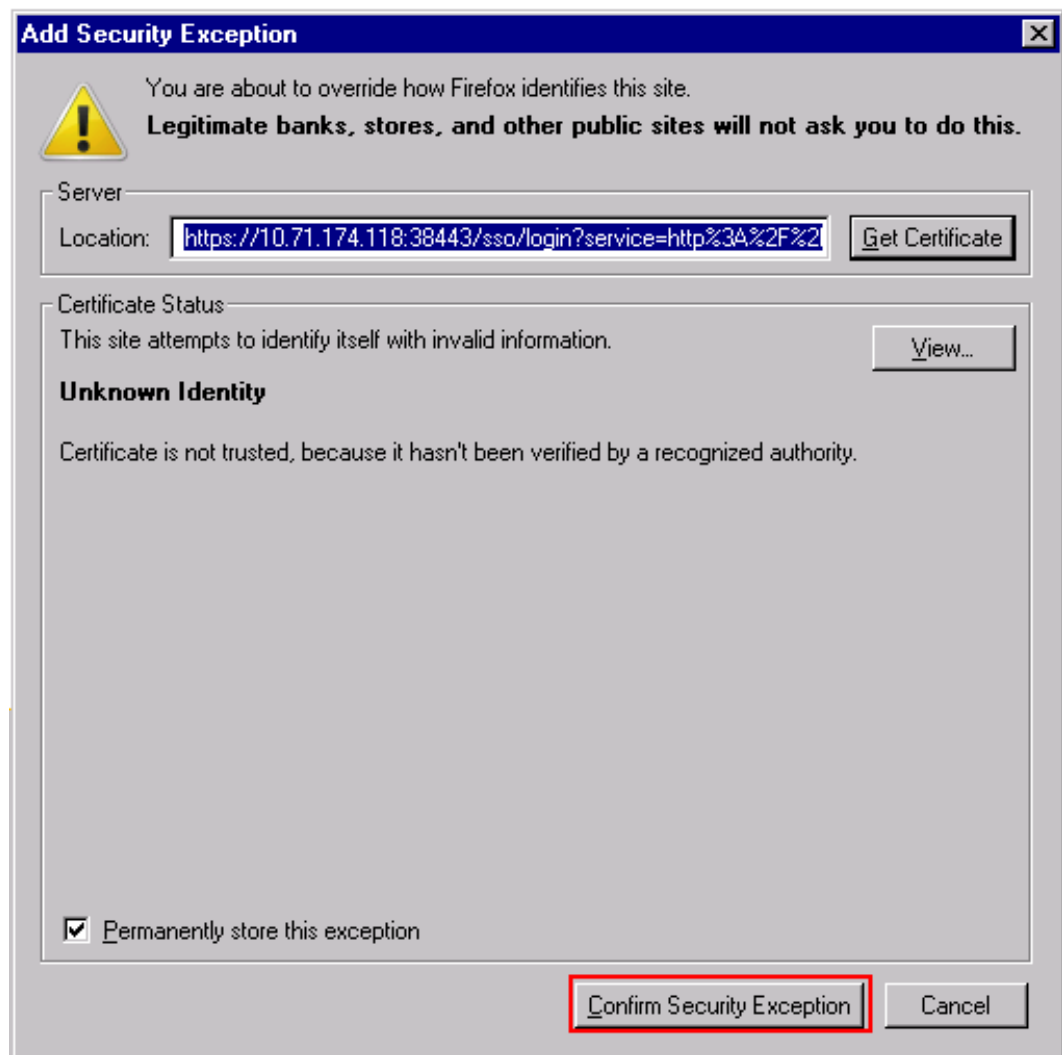
11. Close Internet Explorer and open it again to log in to the eSight.
  - Install the security certificate in Mozilla Firefox.
1. On the error message page, expand **I Understand the Risks** and click **Add Exception**.

Figure 16-14 Add Exception



2. In the **Add Security Exception** dialog box, click **Confirm Security Exception**.

Figure 16-15 Confirm Security Exception



3. Close Mozilla Firefox and open it again to log in to the eSight.

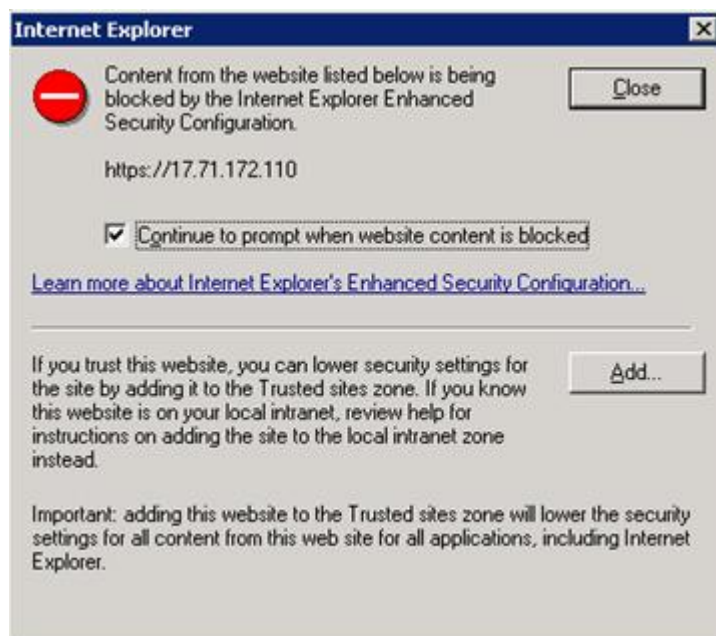
----End

## 16.3 How Do I Resolve the Problem That A Security Alarm Is Generated When Logging In to the eSight By Internet Explorer 8?

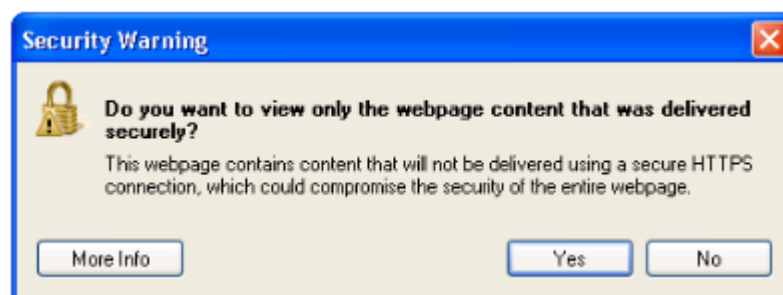
### Symptom

The Web browser displays a security alarm when you log in to the eSight by Internet Explorer 8.

- **Scenario 1:** On Windows Server 2008, a security warning message shown in [Figure 16-16](#) is displayed.

**Figure 16-16** Security warning 1

- **Scenario 2:** On Windows 7, a security warning message shown in Figure 16-17 is displayed.

**Figure 16-17** Security warning 2

## Possible Causes

- **Scenario 1**  
The security level of the browser is too high. To solve this problem, you can add the website of the I2000 as a trusted website or set the security level of the browser to a low level.
- **Scenario 2**  
Windows Internet Explorer 8 displays mixed contents in **Prompt** mode.

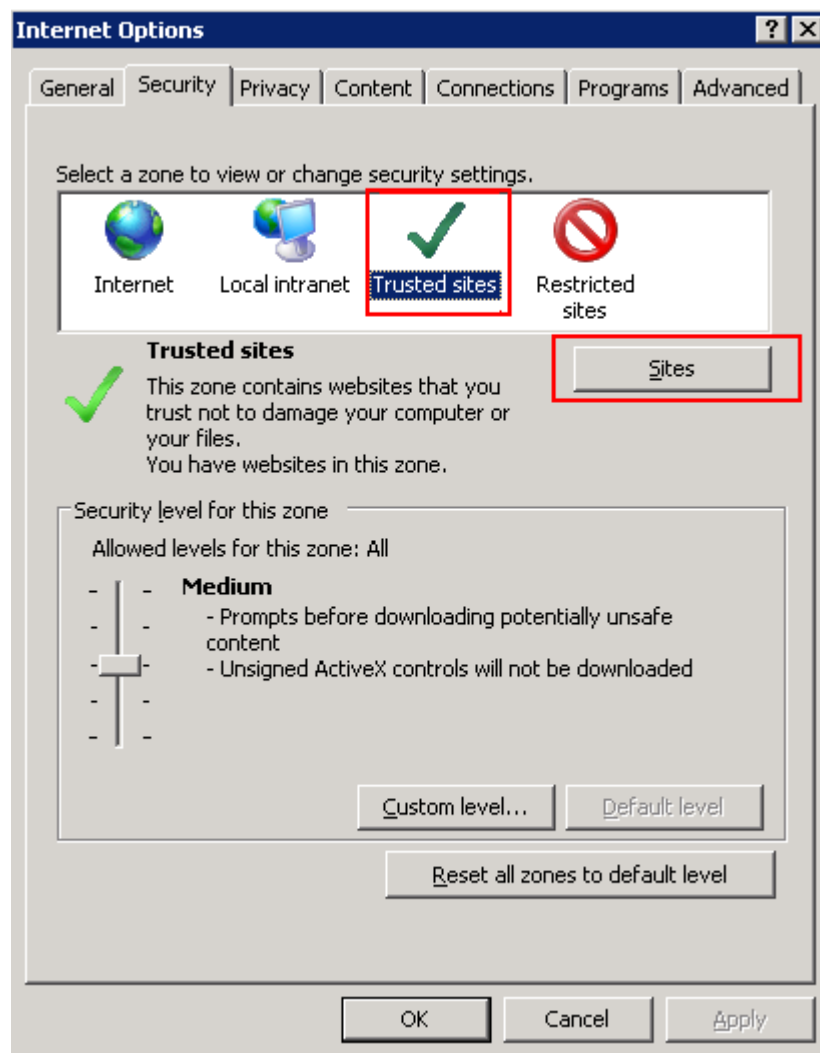
## Procedure

### Scenario 1: The security level of the browser is too high.

- Solution 1: Add Trusted Websites

1. In the dialog box shown in Figure 16-16, click **Add**.
2. In the **Internet Options** dialog box, click the **Security** tab.
3. On the **Security** tab page, select **Trusted sites** and then click **Sites**.

**Figure 16-18** Internet Options



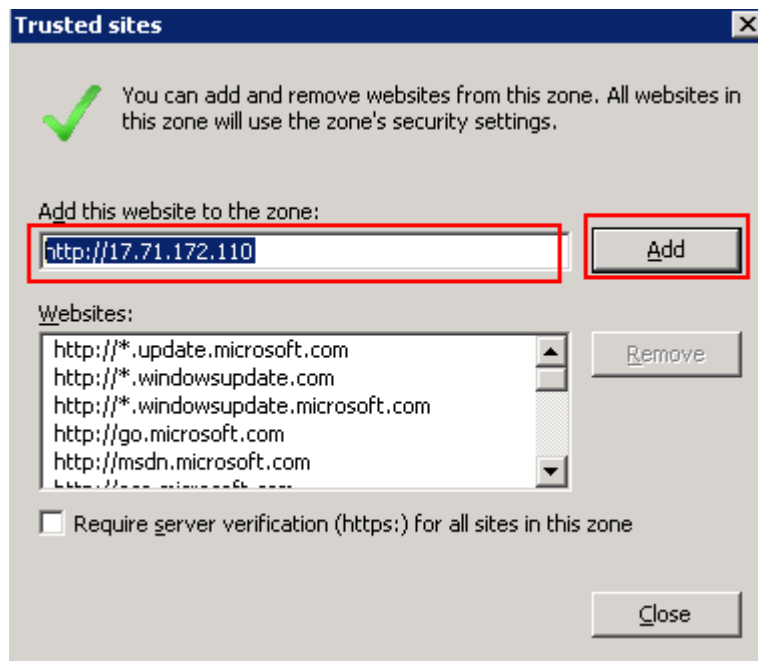
4. In the **Add this website to the zone** text box in the **Trusted sites** dialog box, enter the website for accessing the eSight, and click **Add** to add the website to the list of trusted websites.



**NOTE**

The websites for accessing the eSight over HTTP or HTTPS must be added to the list of trusted websites.

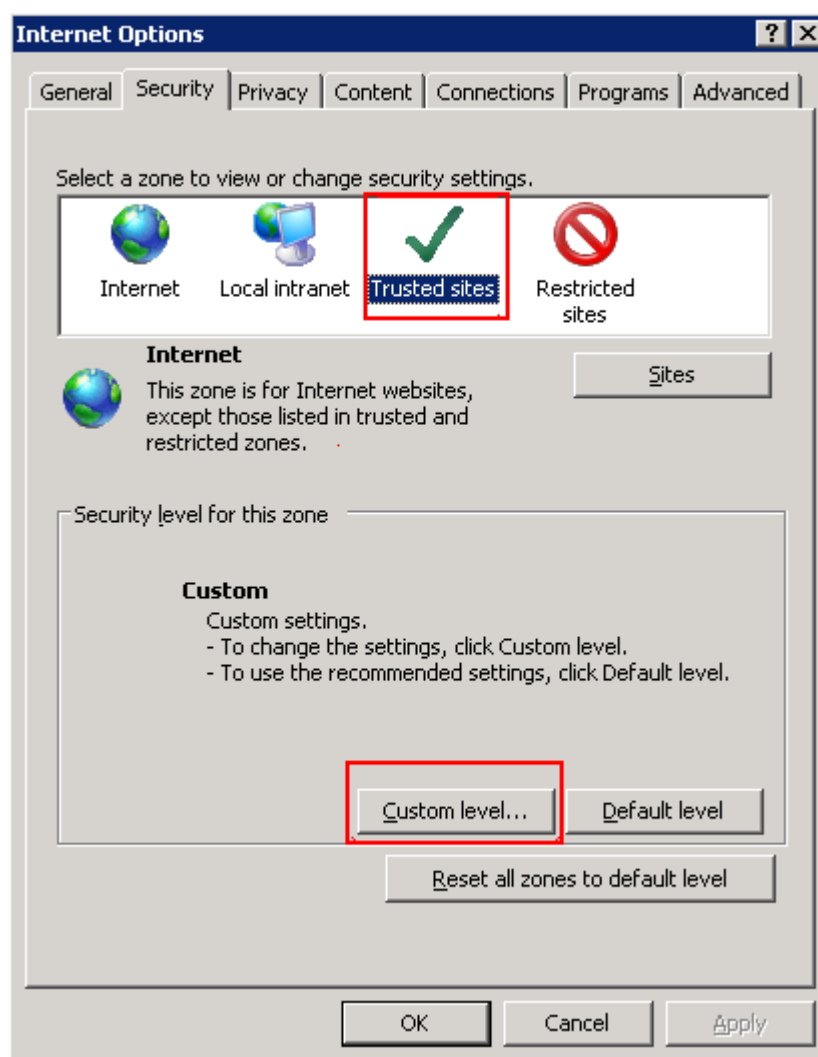
**Figure 16-19** Trusted sites



5. Click **Close**.
- Solution 2: Set the Security Level of the Browser
  1. Open Microsoft Internet Explorer, and choose **Tools > Internet Options**.
  2. In the **Internet Options** dialog box, click the **Security** tab.
  3. On the **Security** tab page, select **Trusted sites** and then click **Custom level**.

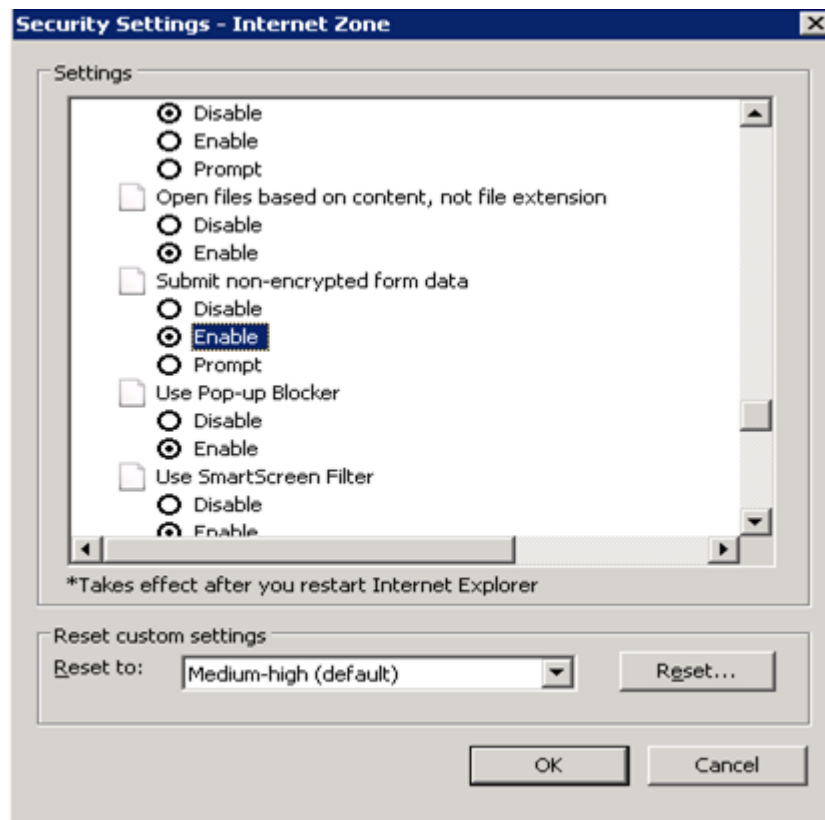


**Figure 16-20** Internet Options



4. In the **Security Settings-Internet Zone** dialog box, select **Enable** under **Submit non-encrypted from data** and **Enable** under **Active scripting**, and click **OK**.

**Figure 16-21** Security Settings-Internet Zone

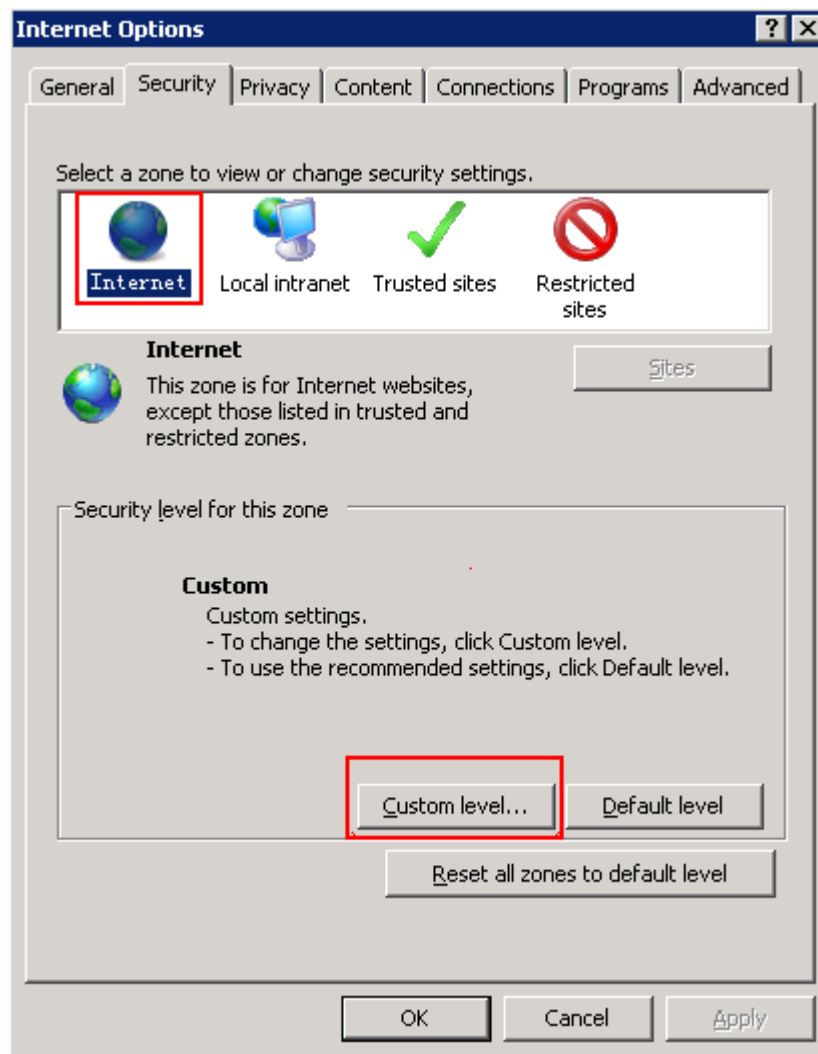


5. In the **Internet Options** dialog box, click **OK**.

**Scenario 2: Windows Internet Explorer 8 displays mixed contents in Prompt mode.**

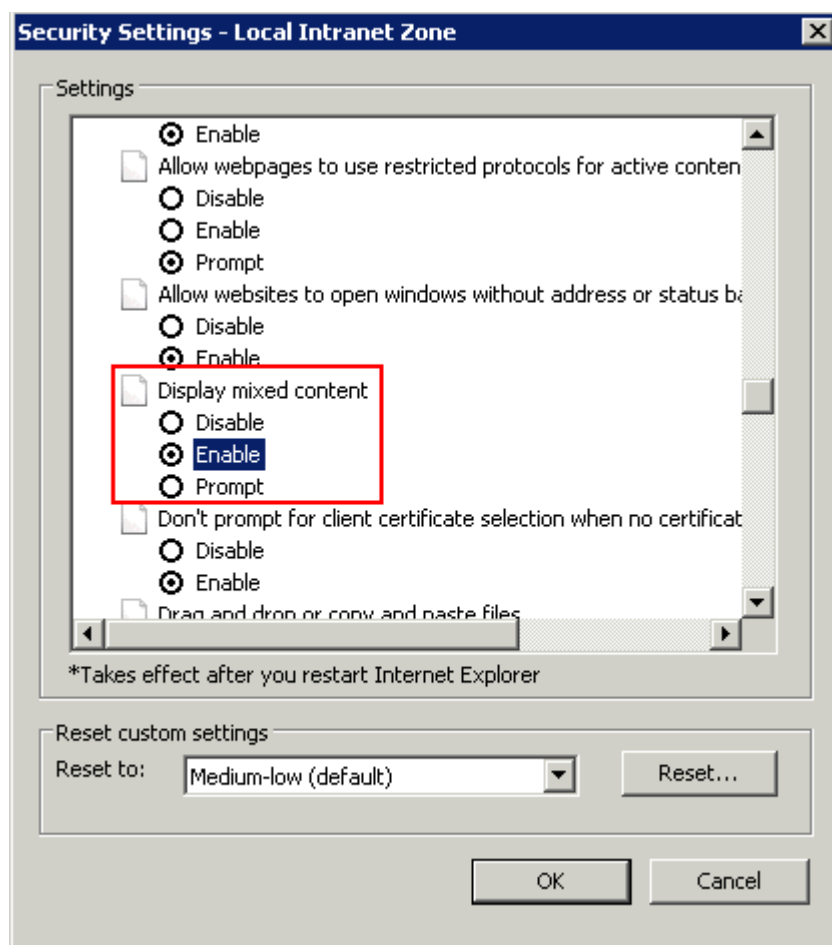
2. Open Microsoft Internet Explorer, and choose **Tools > Internet Options**.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. On the **Security** tab page, select **Internet** and then click **Custom level**.

**Figure 16-22** Internet Options



5. In the **Security Settings-Internet Zone** dialog box, select **Enable** under **Display mixed content**, and click **OK**.

**Figure 16-23** Security Settings-Internet Zone



6. In the **Internet Options** dialog box, click **OK**.
7. Restart Windows Internet Explorer 8.

----End

## 16.4 What Do I Do When a Few English Fields Cannot Be Displayed Completely During the Process of Accessing the eSight GUI in English by Mozilla Firefox in Chinese?

### Symptom

A few English fields cannot be displayed completely during the process of creating roles or users when Mozilla Firefox of the eSight GUI in English. However, this problem does not occur if Internet Explorer is used.

The problem may occur in the following scenarios:

- Scenario 1: On the English UI for creating users, the fields shown in [Figure 16-24](#) cannot be displayed completely.

**Figure 16-24** Fields that cannot be displayed completely

Security Management > Rights Assignment > User > **Create User** Help ?

Basic Info Roles Access Control Polici...

\* User name:

\* Password:

\* Confirm password:

Account status: ☒ Enabled ☐ Disabled

Description:

**The password must meet the following rules:**

- 1, The password is different from the user name.
- 2, The length ranges from 6 to 32 characters.
- 3, The number of occurrences of a character in a password cannot exceed 3.
- 4, The password contains uppercase and lowercase letters and digits.

- Scenario 1: On the English UI for creating roles, the fields shown in [Figure 16-25](#) cannot be displayed completely.

**Figure 16-25** Fields that cannot be displayed completely

Security Management > Rights Assignment > Role > **Create Role** Help ?

Basic Info   Select Managed Objects   Select Operations   Summary

\* Role name:

Description:

Select users:

User name:

|                                     | User Name  | Description   |
|-------------------------------------|------------|---------------|
| <input checked="" type="checkbox"/> | admin      | Administrator |
| <input type="checkbox"/>            | SampleUser |               |

Total records: 2   10 records   1 / 1  

| User Name  | Operation |
|------------|-----------|
| No record. |           |

## Possible Causes

The default font of the Mozilla Firefox of the Chinese version is not configured correctly.

## Fault Diagnosis

You can change the default font.

## Procedure

**Step 1** On the menu bar of the Mozilla Firefox of the Chinese version, choose **Tools > Options**.

**Step 2** In the **Options** dialog box, click the **Content** tab.

**Step 3** In the **Fonts & Colors** area, select **Arial** from the **Default fonts** drop-down list.

**Step 4** Click **OK**.

You can verify whether the problem occurs.

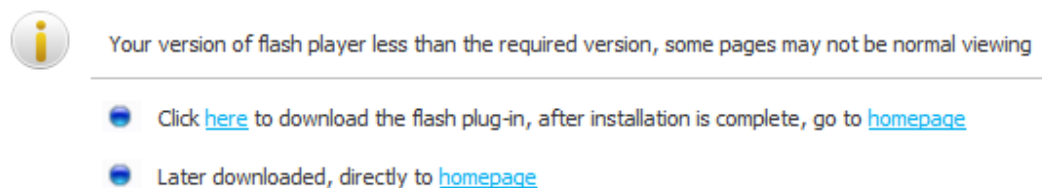
----End

## 16.5 What Do I Do When Adobe Flash Player Provided by the eSight Cannot Be Installed in Internet Explorer?

### Symptom

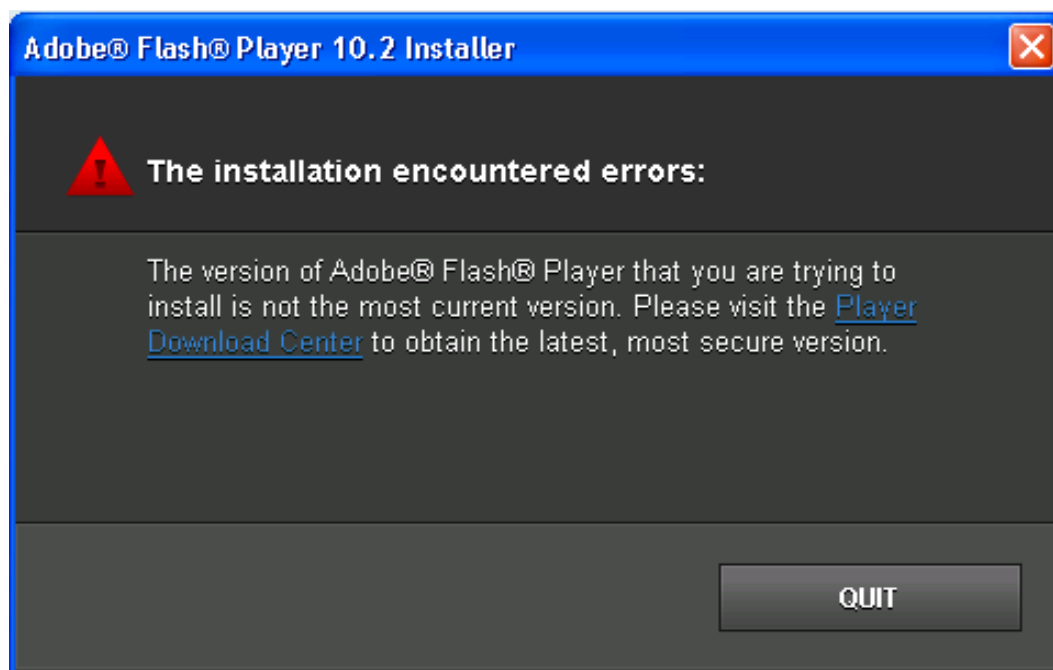
If Internet Explorer is used to access the eSight, the message shown in [Figure 16-26](#) is displayed after you log in.

**Figure 16-26** Message indicating that flash player is not the latest version



When you install Adobe Flash Player provided by the eSight under Internet Explorer as prompted, an error message shown in [Figure 16-27](#) is displayed, indicating installation failure.

**Figure 16-27** Error message



### Possible Causes

The version of Adobe Flash Player provided by the eSight is earlier than that of Adobe Flash Player recorded in the registration table of the client.

## Fault Diagnosis

Uninstall Adobe Flash Player and install the earlier and later versions of Adobe Flash Player respectively.

- No error message is displayed when you install Adobe Flash Player whose version is later than the Adobe Flash Player provided by the eSight. The installation is successful.
- An error message is displayed when you install Adobe Flash Player whose version is earlier than the Adobe Flash Player provided by the eSight. The installation failed.

## Procedure

**Step 1** In the error dialog box, click **Player Download Center**.

Go to the Adobe Flash Player download center to obtain the latest version.

**Step 2** Install the latest version of Adobe Flash Player.

----End

## 16.6 How to Resolve the Problem that the Flash Plug-in Is Down When the eSight Flash Is Opened Using a Browser

### Symptom

When a user attempts to use the Firefox or Windows Internet Explorer 8 to open an eSight Flash, such as is the alarm histogram page, topology page, or performance monitoring page on the home page, a message shown in [Figure 16-28](#) or [Figure 16-29](#) is displayed.

**Figure 16-28** Flash plug-in down message on Firefox

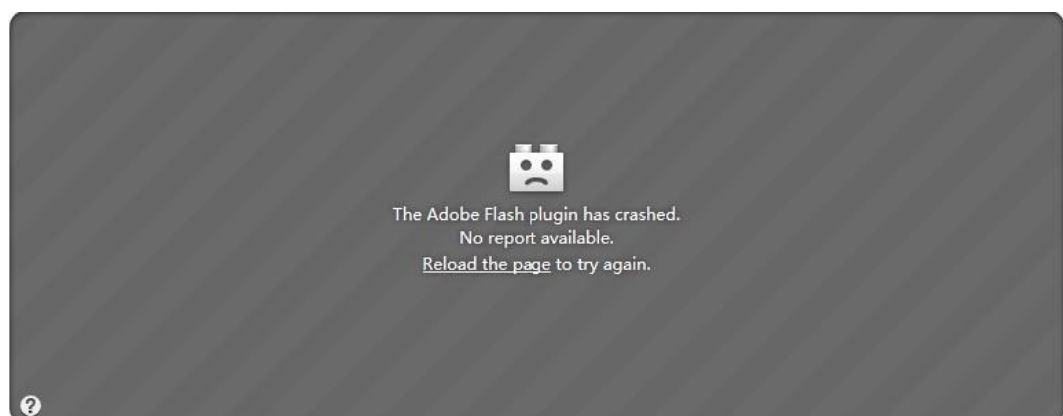
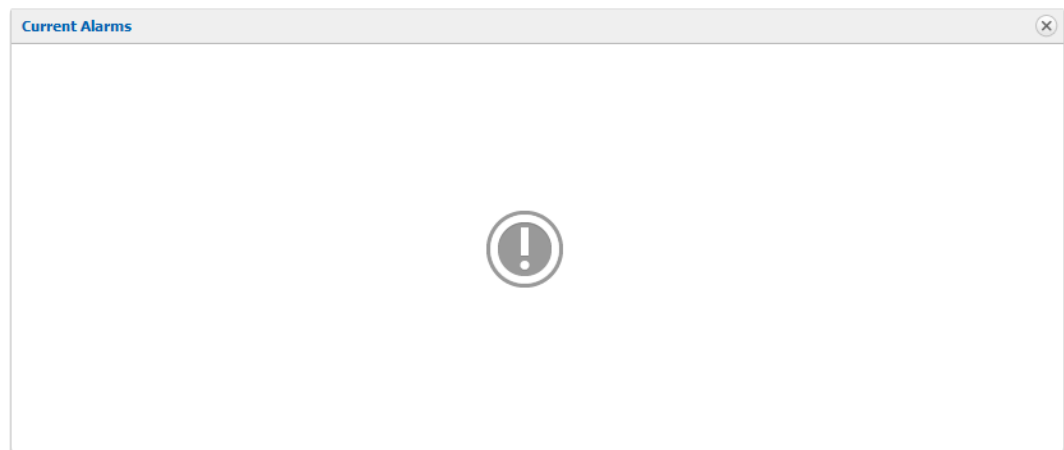




**Figure 16-29** Flash plug-in down message on Windows Internet Explorer 8



## Possible Causes

- During the running of the Flash plug-in, a conflict occurs when reading and writing the memory. The browser terminates the plug-in management process to ensure the normal running of the browser.
- During the running of the browser, the memory or CPU usage is high. The browser terminates the plug-in management process to release the memory or CPU.

## Procedure

- Firefox

Click the **Reload the page** link.

The first page of the eSight is displayed, and the Flash pages are displayed properly.

- Windows Internet Explorer 8

1. Click  to log out of the eSight.
2. Log in to the eSight again.

The Flash pages are displayed properly.

----End

## 16.7 What Do I Do When Arabic Characters Appear Garbled After Being Copied?

### Symptom

- Scenario 1: After some Arabic characters are copied to a text box (for example, the **Search** text box in the **Topology Management** window) on the Flex page, the Arabic characters are displayed as garbled.
- Scenario 2: After you copy some strings containing Arabic characters to the **Name** text box when creating an NE on the **Resource Management** page, the strings are displayed

normally, but the name of the NE is displayed as garbled on the Flex page (**Topology Management** and **Performance Management**).

## Possible Causes

Flex does not allow you to copy some Arabic characters.



### NOTE

The code point range for Arabic characters is as follows:

- 0x0600 to 0x06ff: for input processing. Flex supports the copy and paste operations.
- 0xfe70 to 0xfeff: for display. Flex does not support the copy and paste operations.

## Procedure

**Step 1** Enter the Arabic characters to be copied.

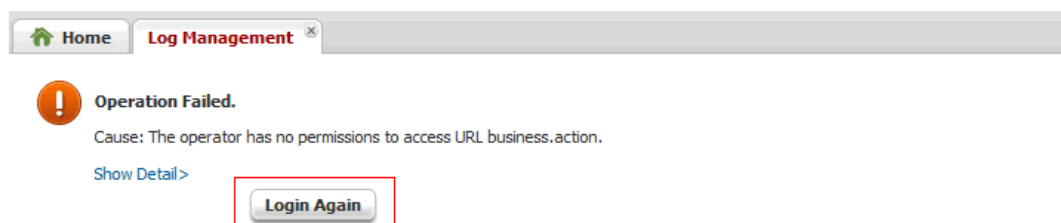
----End

# 16.8 How Do I Resolve the Nesting Problems of the eSight Page after Clearing the Cache from Firefox?

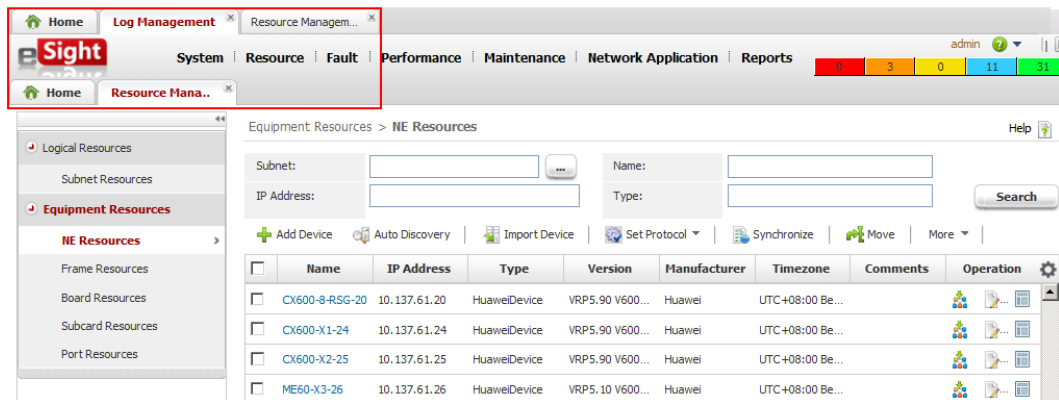
## Symptom

1. On Firefox, log in to eSight. Choose **Tools** > **Clear Recent History** from the toolbar.
2. When opening a window in the eSight client, the user is prompted to log in again. For example, choose **System** > **Log Management** to open the **Log Management** window. The login page is displayed, as shown in [Figure 16-30](#):

**Figure 16-30** Log in again



3. Click **Login Again**. The login page is displayed. Enter the user name, password, and verification code. Click **Login**. The error page shown in [Figure 16-31](#) is displayed.

**Figure 16-31** Nesting a page

## Possible Causes

The user login information is cleared as cache in the browser is cleared. Therefore, eSight cannot read user login information.

## Procedure

**Step 1** Click **Refresh** in the browser toolbar, or restart the browser.

**Step 2** Log in to eSight again.

----End

## 16.9 How Do I Install an SSL Certificate for the Email Server?

### Question

An SSL certificate is required when SSL is used to connect the eSight system to the email server. How do I install the SSL certificate?

### Answer

**Step 1** Obtain the SSL certificate for the email server.

Export the SSL certificate from the email server.



#### NOTE

The eSight does not support SSL V3 certificates.

**Step 2** Copy the SSL certificate to a temporary directory of the eSight server.

**Step 3** Install the SSL certificate.

Before performing the operation, ensure that you have the read and write permissions of the **eSight\_ROOT/AppBase/etc/oms.core/ent.keystore** directory.

- Windows

1. In the command line window, run the following commands:

```
keytool -import -file SSL certificate directory/SSL certificate name -keystore
eSight_ROOT/AppBase/etc/oms.core/ent.keystore -storepass changeit
```

**NOTE**

eSight\_ROOT is the installation directory of the eSight system.

For example: **keytool -import -file *D:/server4.crt* -keystore  
eSight\_ROOT/AppBase/etc/oms.core/ent.keystore -storepass changeit**

2. Check whether a prompt message is displayed, asking you whether to display the trust certificate.

- If the prompt is displayed, enter **Y** at the prompt.
- If the prompt is not displayed, the JDK is not installed. Run the following command to install it:

```
cd /d eSight_ROOT/AppBase/jre/bin
```

```
keytool -import -file SSL certificate directory/SSL certificate name -keystore
eSight_ROOT/etc/certificate/trustKeystore -storepass changeit
```

When a prompt is displayed, asking you whether to display the trust certificate, enter **Y**.

- Linux

1. In the command line window, run the following commands:

```
keytool -import -file SSL certificate directory/SSL certificate name -keystore
eSight_ROOT/AppBase/etc/oms.core/ent.keystore -storepass changeit
```

For example: **keytool -import -file *./server4.crt* -keystore  
eSight\_ROOT/AppBase/etc/oms.core/ent.keystore -storepass changeit**

2. Check whether a prompt message is displayed, asking you whether to display the trust certificate.

- If the prompt is displayed, enter **Y** at the prompt.
- If the prompt is not displayed, the JDK is not installed. Run the following command to install it:

```
cd eSight_ROOT/AppBase/jre/bin
```

```
./keytool -import -file SSL certificate directory/SSL certificate name -keystore
eSight_ROOT/AppBase/etc/oms.core/ent.keystore -storepass changeit
```

When a prompt is displayed, asking you whether to display the trust certificate, enter **Y**.

**Step 4** Restart the eSight process.

----End

## 16.10 How Do I Customize Connection Rules for Ports Required by eSight?

### Question

How Do I customize connection rules for ports required by eSight?



#### NOTE

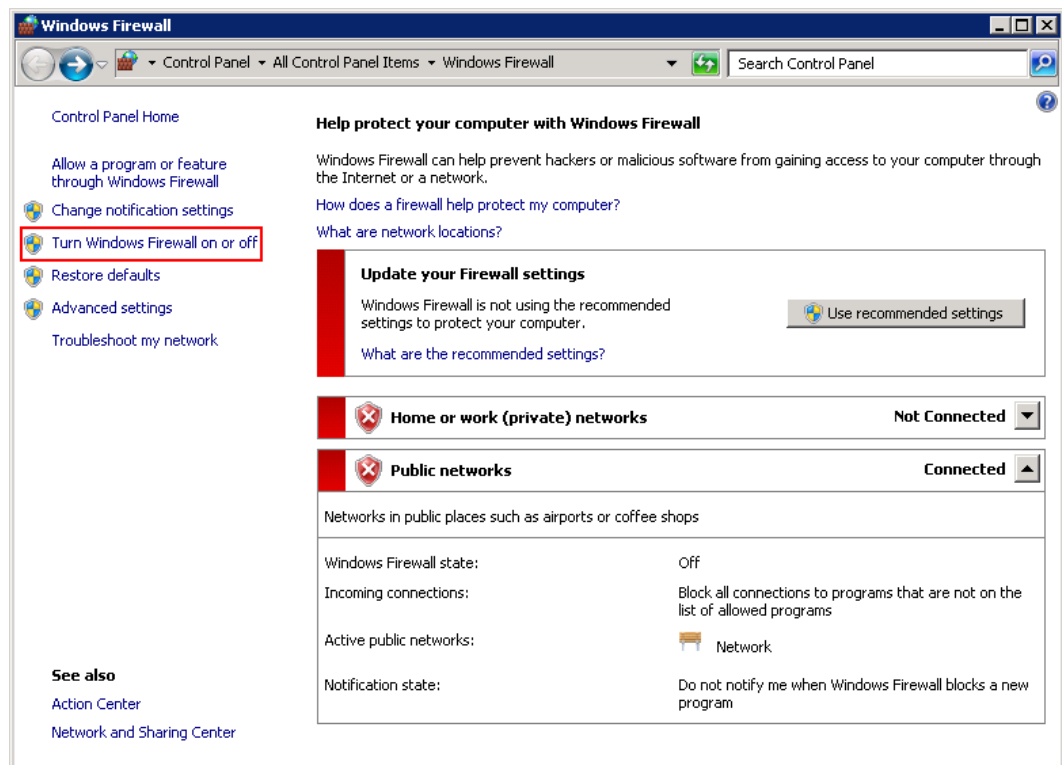
This topic applies to Windows 7 and Windows Server 2008.

## Answer

**Step 1** Click **Start**, and enter **firewall.cpl** in **Search Programs and files**.

The **Windows Firewall** window is displayed.

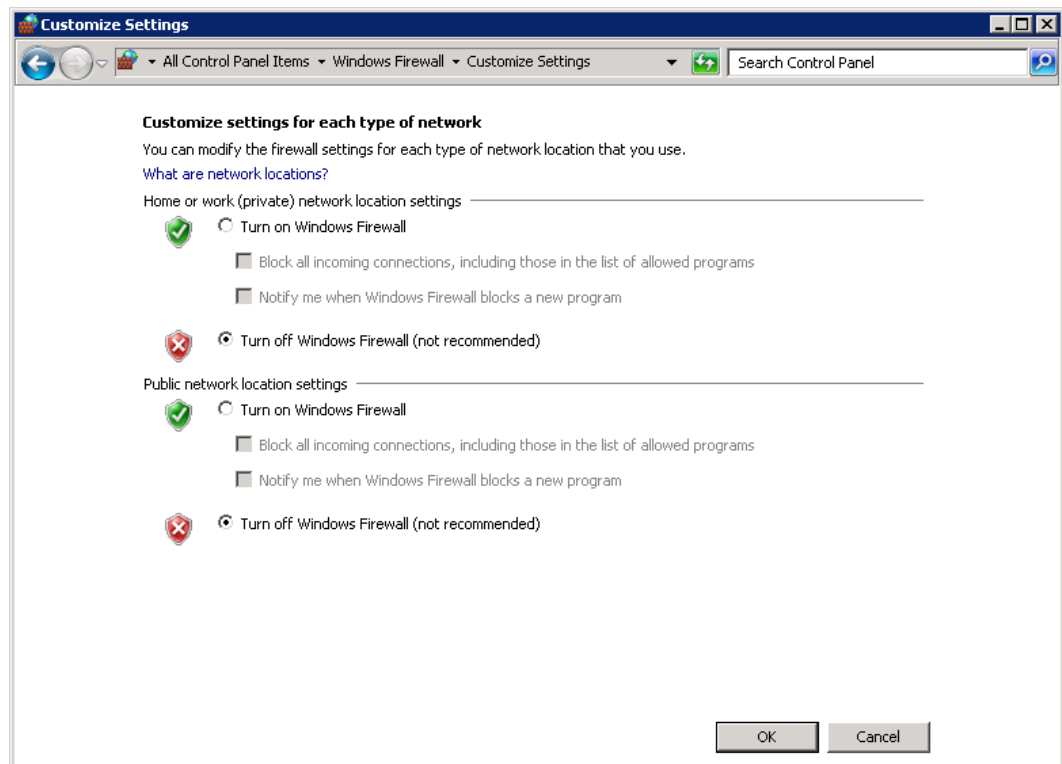
**Figure 16-32** Windows Firewall



**Step 2** Click **Turn Windows Firewall on and off** on the left. In the **Customize Settings** window that is displayed, click **Turn on Windows Firewall** in the area based on your actual network location, and click **OK**.

The **Windows Firewall** window is displayed.

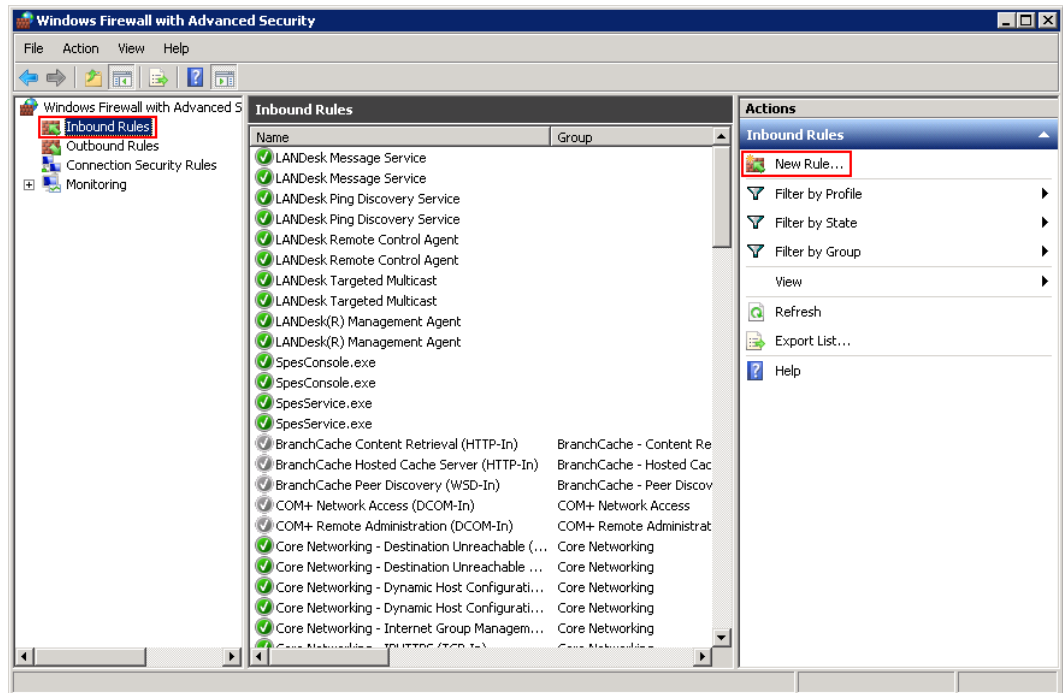
**Figure 16-33** Customize Settings



**Step 3** Click **Advanced Settings** on the left.

The **Windows Firewall with Advanced Security** window is displayed.

**Figure 16-34** Windows Firewall with Advanced Security



**Step 4** Click **Inbounds Rules** on the left.

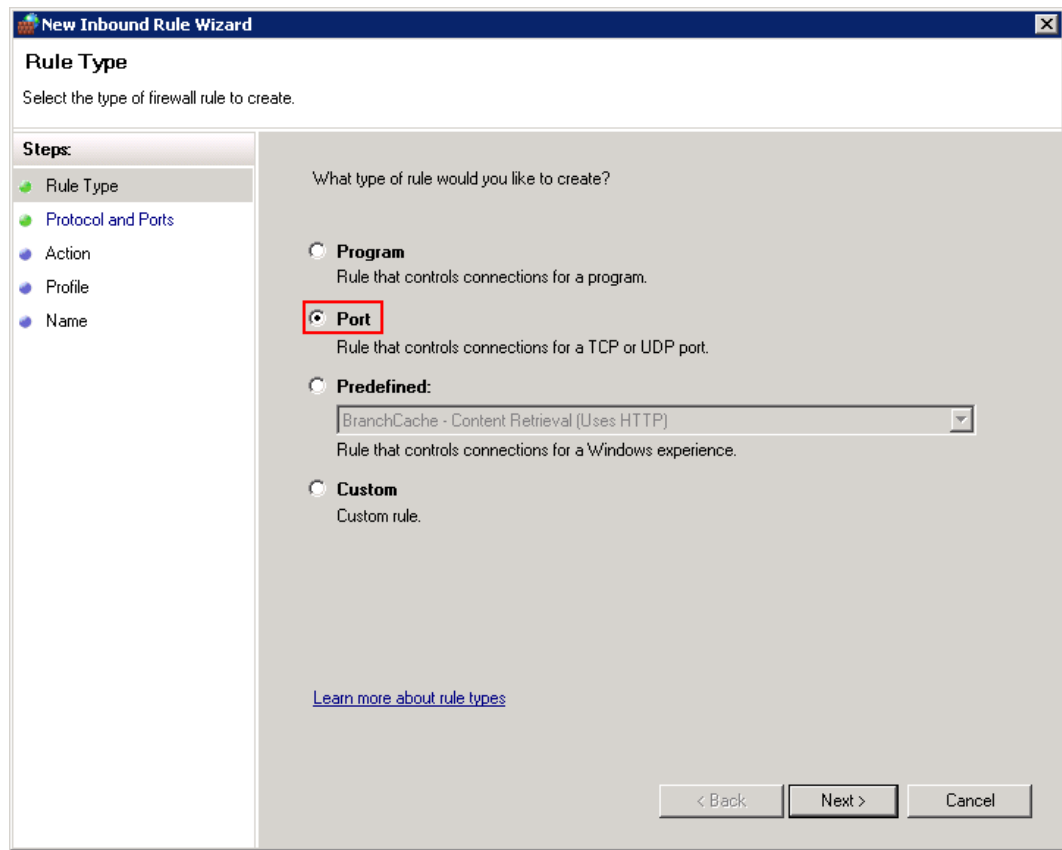
The **Actions** tab page is displayed on the left.

**Step 5** Click **New Rule**.

The **New Inbounds Rule Wizard** window is displayed.

**Step 6** Select **Rule Type** in the left pane, click **Port** in the right pane, and click **Next**.

**Figure 16-35 Rule Type**



**Step 7** Click **TCP** or **UDP** under **Does this rule apply to TCP or UDP?**. Then click **Specific local ports** under **Does this rule apply to all local or specific local ports?**, and set **Specific local ports** to port numbers required by eSight.

Click **Next**.

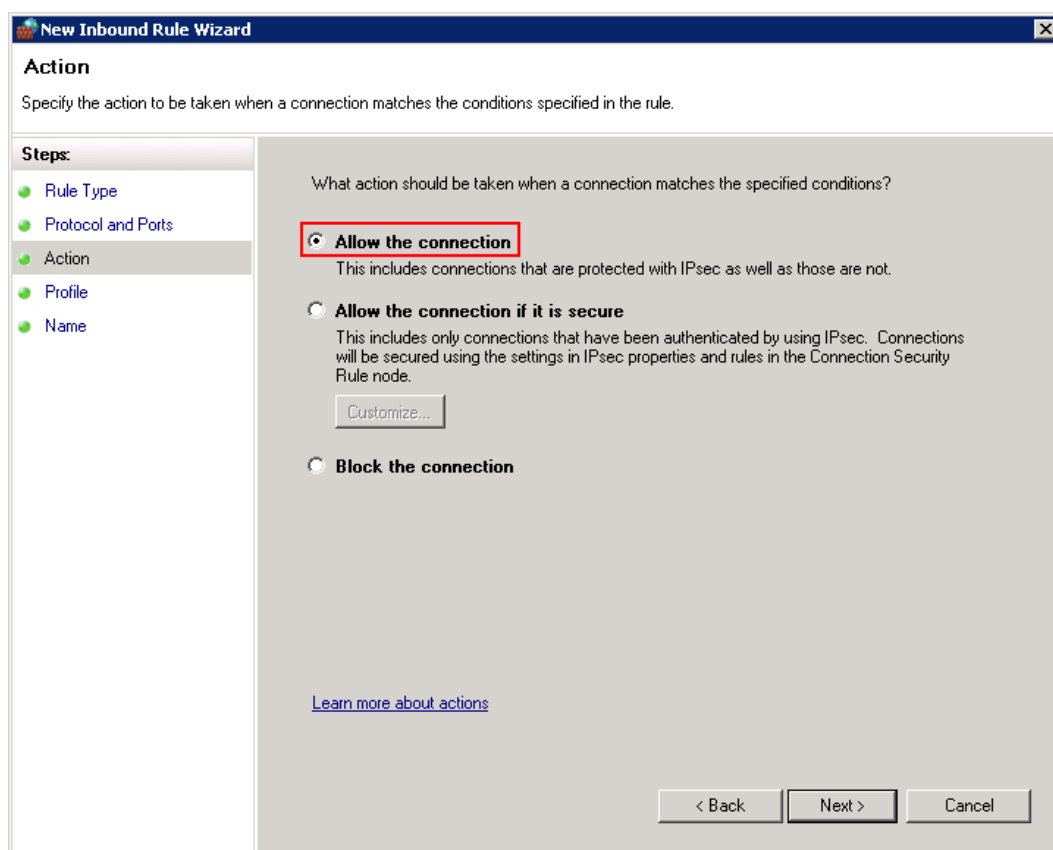


**Figure 16-36** Protocol and Ports

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' sidebar lists: 'Rule Type' (selected with a green dot), 'Protocol and Ports' (selected with a green dot), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main area contains two questions. The first is 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'. The second is 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:' (selected). The 'Specific local ports:' selection is followed by a text input field containing '8080'. Below the input field is the text 'Example: 80, 443, 5000-5010'. At the bottom left of the main area is a link: 'Learn more about protocol and ports'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

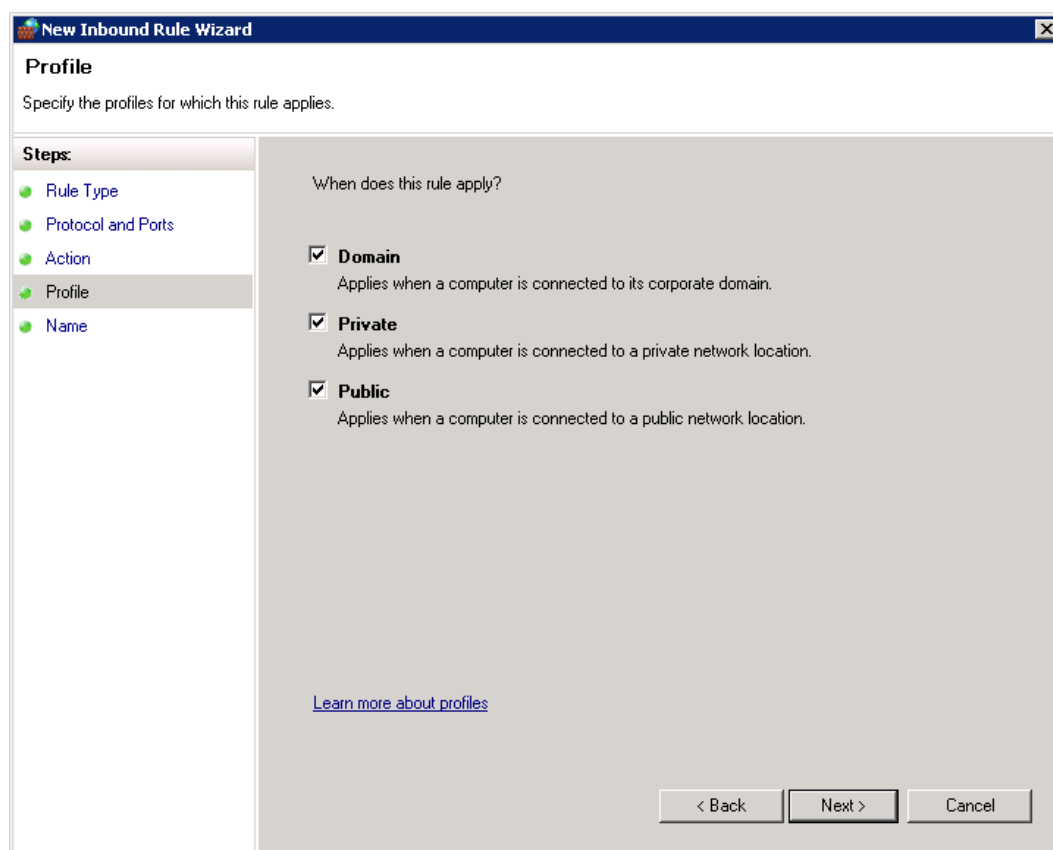
**Step 8** Select **Allow the connection**, and click **Next**.

**Figure 16-37 Action**



**Step 9** Click **Next**.

**Figure 16-38** Profile



**Step 10** Set **Name** and **Description**.

Click **Finish**.

**Figure 16-39 Rule Name**

**New Inbound Rule Wizard**

**Name**  
Specify the name and description of this rule.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile
- **Name**

Name:

Description (optional):

< Back   Finish   Cancel

----End

## 16.11 How Do I Solve the Problem When eSight Cannot Manage an NE Due to Junk Data Caused by Unexpected Database Stop?

### Symptom

When the NE resource management data, physical resource data, and physical topology are inconsistent, eSight cannot manage the NE.

### Possible Causes

If the database stops unexpectedly when an NE is added or deleted, the NE may generate junk data. This results in inconsistency between the NE resource management data, physical resource data, and physical topology. When this occurs, eSight cannot manage the NE.

### Procedure

**Step 1** Stop eSight services.

- Windows operating system:
  1. Choose **Start > All Programs > eSight > shutdown eSight**.
- SUSE Linux operating system:
  1. **cd eSight\_ROOT/mttools/bin**
  2. **./stop.sh**

**NOTE**

eSight\_ROOT is the installation directory of the eSight system.

**Step 2** Connect to the database, and run the following statements to delete junk data:

- **Oracle database:**

```
delete from nemgr.tbl_ne_extinfo where not exists (select * from
omsmodel.tbl_mobasicattr m where m.dn = nedn);
delete from nemgr.tbl_ne_info where not exists (select * from
omsmodel.tbl_mobasicattr m where m.dn = nedn);
delete from nemgr.tbl_ne_info where not exists (select * from
omsmodel.tbl_mobasicattr m where m.dn = nedn);
delete FROM omsmodel.tbl_moextendattr where dn in (select destNode from
omsmodel.tbl_morelation where srcnode in ((select m.dn from
omsmodel.tbl_mobasicattr m where not exists (select * from nemgr.tbl_ne_info n where
m.dn = n.nedn) and m.DN != '/NE=OMS' and m.DN like '%NE=%')) and type = 'Dependency');
delete from omsmodel.tbl_moextendattr where not exists (select * from
nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_mobasicattr where dn in (select destNode from
omsmodel.tbl_MORElation where not exists (select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%') and type = 'Dependency';
delete from omsmodel.tbl_mobasicattr where not exists (select * from
nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_tobasicattr where not exists (select * from
nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
commit;
```

- **MySQL database:**

```
delete from nemgr.tbl_ne_extinfo where not exists (select * from
omsmodel.tbl_mobasicattr m where m.dn = nedn);
delete from nemgr.tbl_ne_info where not exists (select * from
omsmodel.tbl_mobasicattr m where m.dn = nedn);
delete FROM omsmodel.tbl_moextendattr where dn in (select destNode from
omsmodel.tbl_morelation where srcnode in ((select m.dn from
omsmodel.tbl_mobasicattr m where not exists (select * from nemgr.tbl_ne_info n where
m.dn = n.nedn) and m.DN != '/NE=OMS' and m.DN like '%NE=%')) and type = 'Dependency');
delete from omsmodel.tbl_moextendattr where not exists (select * from
nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_mobasicattr where dn in (select destNode from
omsmodel.tbl_MORElation where not exists (select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%') and type = 'Dependency';
delete from omsmodel.tbl_mobasicattr where not exists (select * from
nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_tobasicattr where not exists (select * from
nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
commit;
```

- **SQL Server database:**

```
delete from nemgr..tbl_ne_extinfo where not exists (select * from
omsmodel..tbl_mobasicattr m where m.dn = nedn)
go
delete from nemgr..tbl_ne_info where not exists (select * from
omsmodel..tbl_mobasicattr m where m.dn = nedn)
go
delete FROM omsmodel..tbl_moextendattr where dn in (select destNode from
omsmodel..tbl_morelation where srcnode in ((select m.dn from
omsmodel..tbl_mobasicattr m where not exists(select * from nemgr..tbl_ne_info n
where m.dn = n.nedn) and m.DN != '/NE=OMS' and m.DN like '%NE=%')) and type =
'Dependency')
go
delete from omsmodel..tbl_moextendattr where not exists(select * from
nemgr..tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%'
go
delete from omsmodel..tbl_mobasicattr where dn in (select destNode from
omsmodel..tbl_MORelation where not exists(select * from nemgr..tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%') and type = 'Dependency'
go
delete from omsmodel..tbl_mobasicattr where not exists(select * from
nemgr..tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%'
go
delete from omsmodel..tbl_tobasicattr where not exists(select * from
nemgr..tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%'
go
```

### Step 3 Start eSight services.

- Windows operating system:
  1. Choose **Start > All Programs > eSight > start eSight**.
- SUSE Linux operating system:
  1. **cd eSight\_ROOT/mttools/bin**
  2. **./run.sh**

----End

## 16.12 How Do I Solve the Problem When the eSight GUI Fails to Display Properly and the GUI Displays Page-wide Code When I Log Out?

### Symptom

The eSight GUI fails to display properly when I log in. When I log out, the GUI displays page-wide code.

### Possible Causes

The space of the disk where the eSight server installation directory is located is used up. No space is available for storing temporary files generated when the web server compiles web pages.

## Procedure

- Clean up the disk where the eSight server installation directory is located. The disk space required by the proper running of an eSight server varies according to eSight edition and ranges from 20 GB to 320 GB. For details, see the *eSight Release Notes*.

----End

## 16.13 How Do I Set SNMP Parameters on a PC?

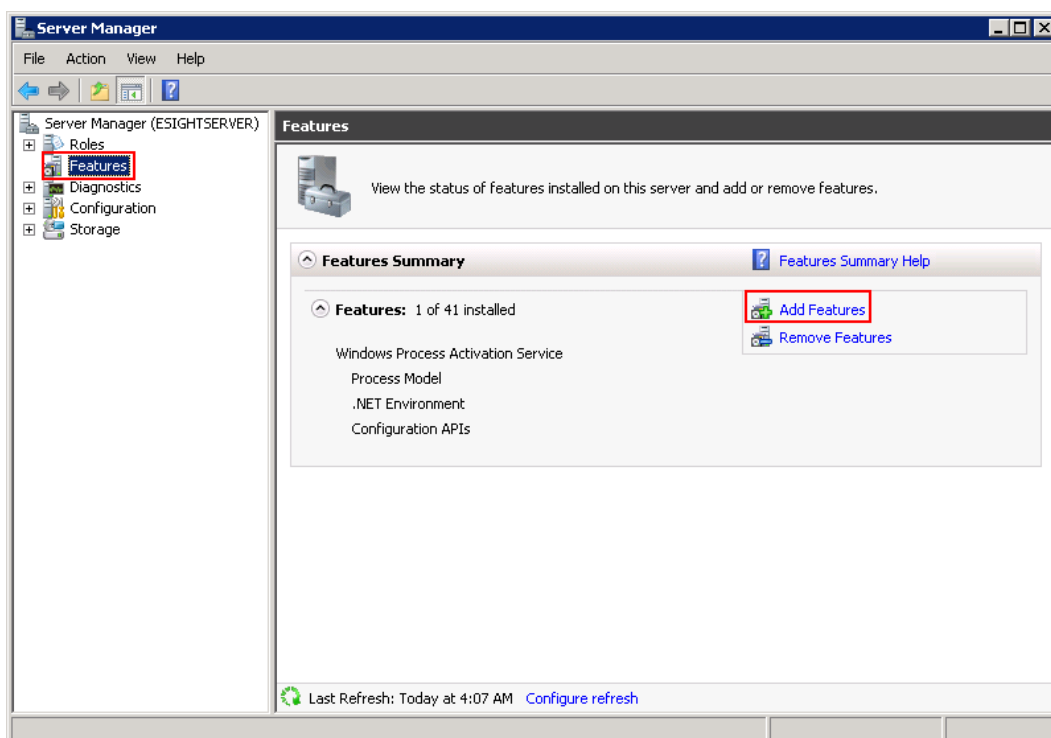
### Question

How do I set SNMP parameters on a personal computer (PC)?

### Answer

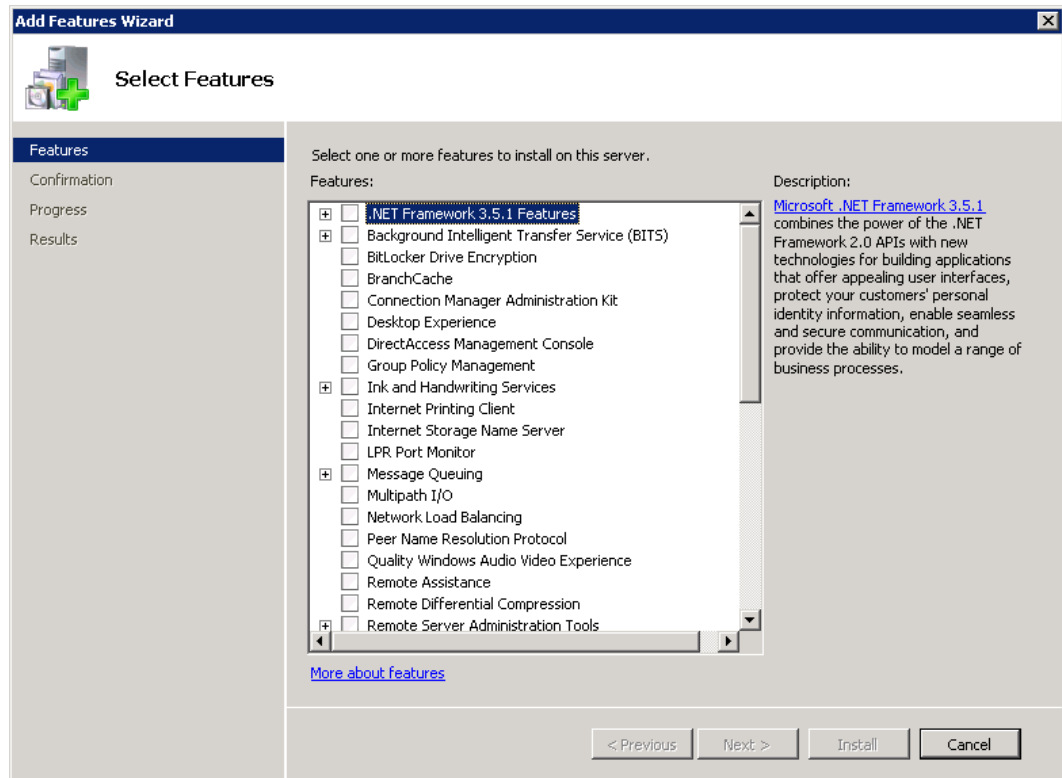
- In the Windows Server 2008 operating system:
  1. Choose **Start > Administrative Tools > Server Manager**.
  2. In the **Server Manager** window, choose **Features** from the navigation tree.

**Figure 16-40** Server Manager



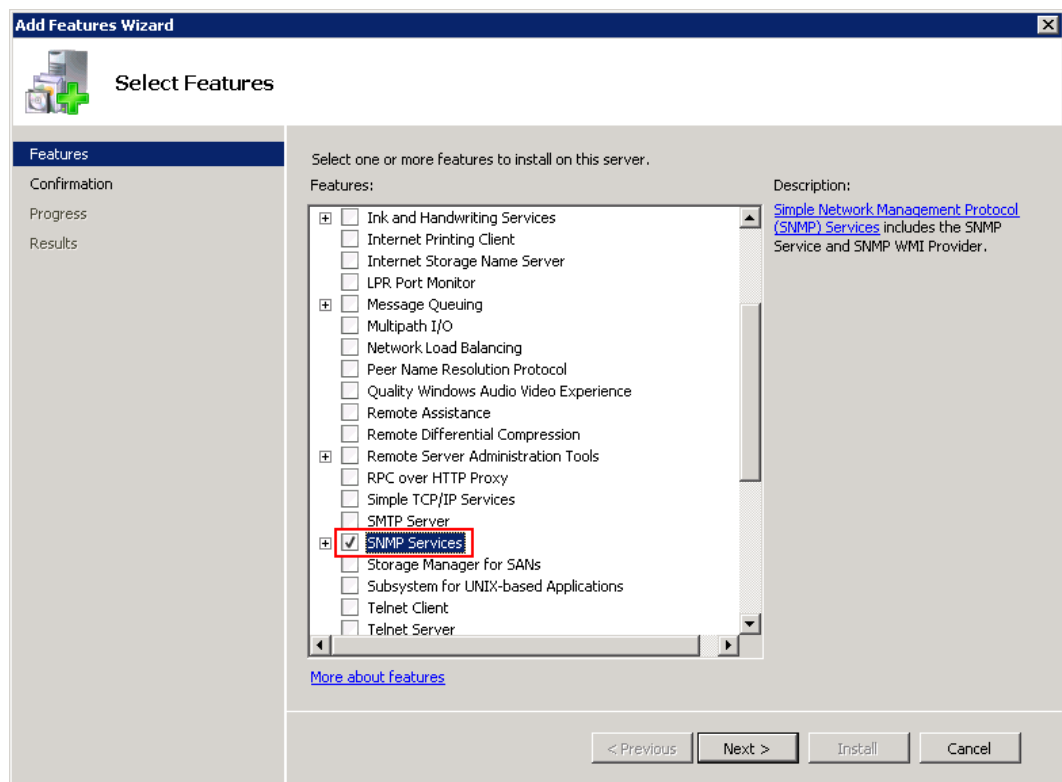
3. In the **Features** window, click **Add Features**.  
The **Add Features Wizard** dialog box is displayed.

**Figure 16-41** Add Features Wizard



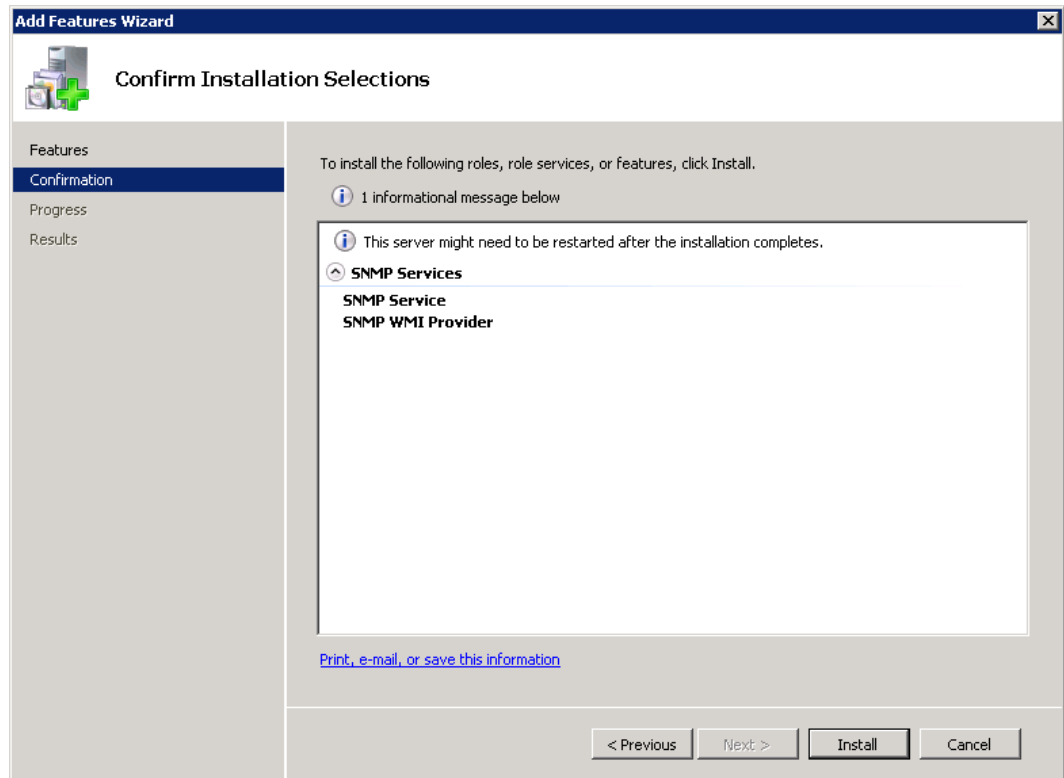
4. Select **SNMP services**, and click **Next**.



**Figure 16-42** Select Features

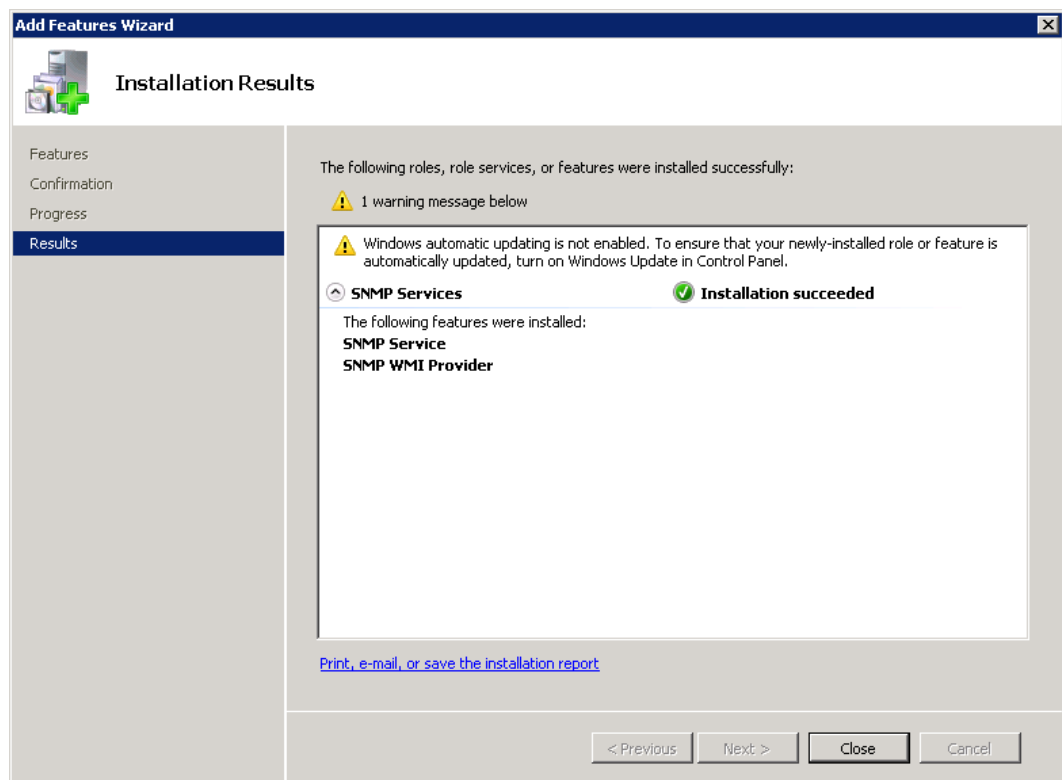
5. Click **Install**. The system starts to install the SNMP service.

**Figure 16-43** Confirm Installation Selections



6. Click **Close**.

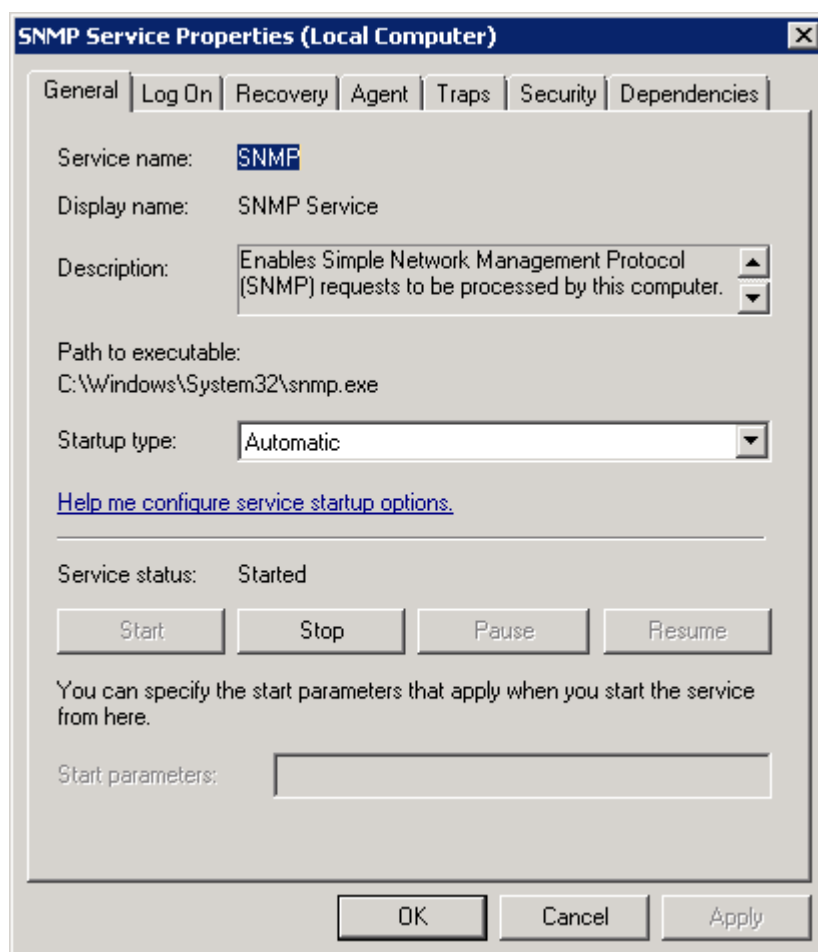
**Figure 16-44** Installation Results



7. Choose **Start > Administrative Tools > Services**.
8. In the **Services** window, right-click **SNMP Service**, and choose **Properties** from the shortcut menu.

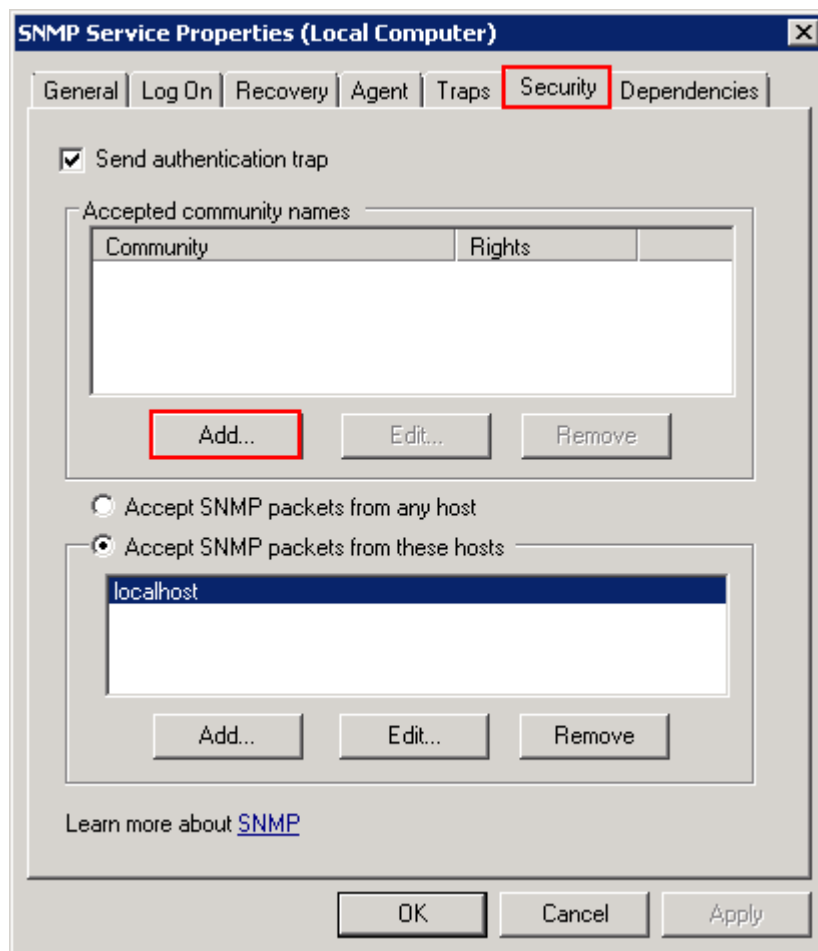
The **SNMP Service Properties** dialog box is displayed.

**Figure 16-45** SNMP Service Properties



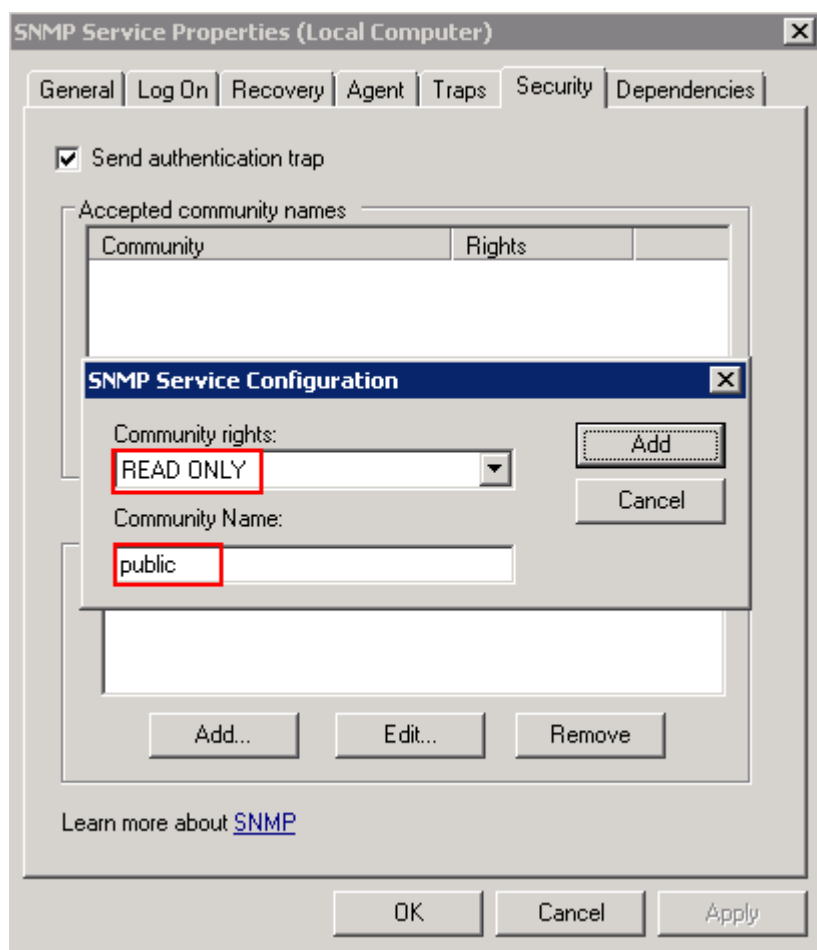
9. Click the **Security** tab.

**Figure 16-46** SNMP Service Security 1



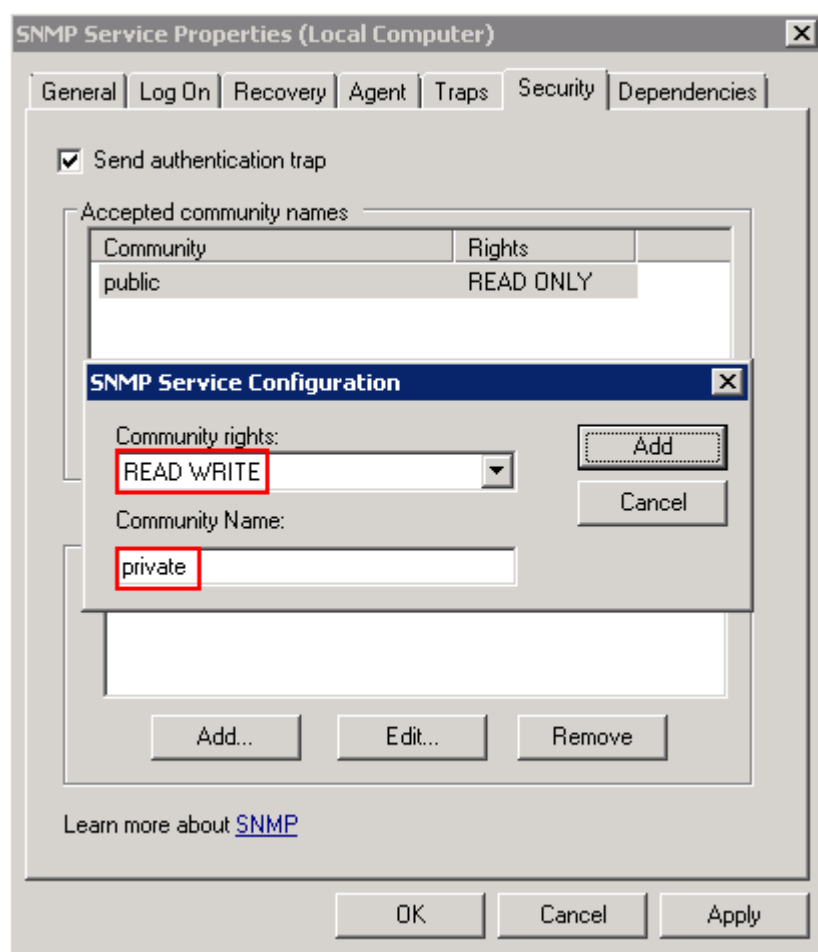
10. Click **Add**.  
The **SNMP Service Configuration** dialog box is displayed.
11. Set **Community rights** to **READ ONLY** and **Community Name** to **public**, and click **Add**.

**Figure 16-47** SNMP Configuration 1



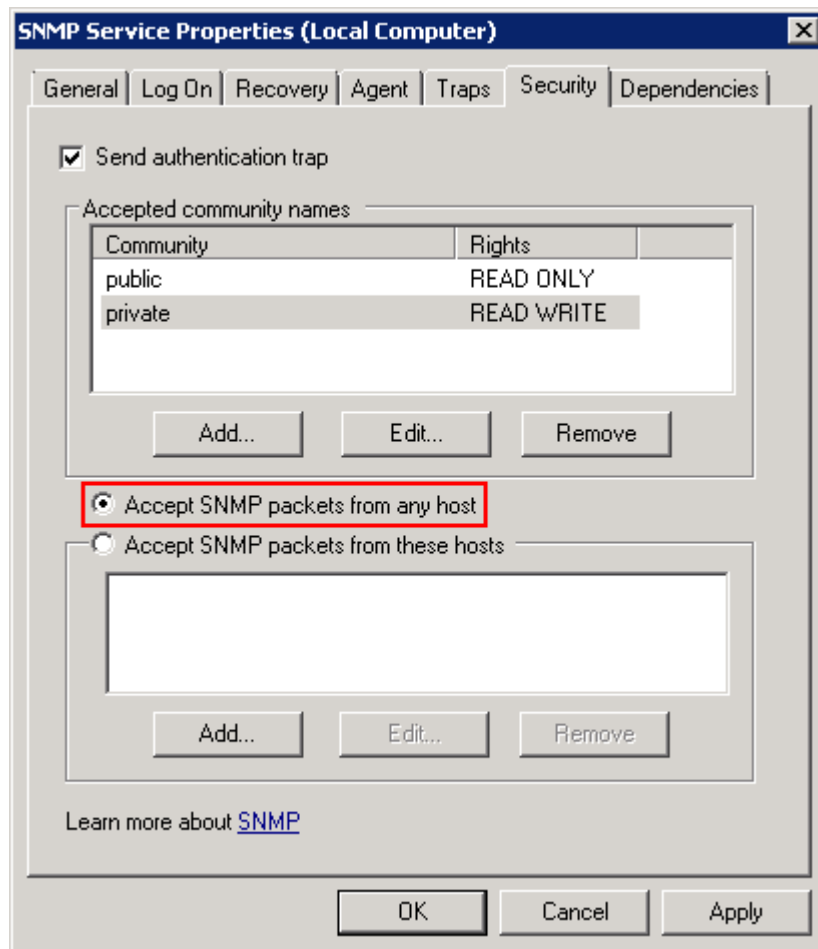
12. Click **Add**.  
The **SNMP Service Configuration** dialog box is displayed.
13. Set **Community rights** to **READ WRITE** and **Community Name** to **private**, and click **Add**.

**Figure 16-48** SNMP Configuration 2



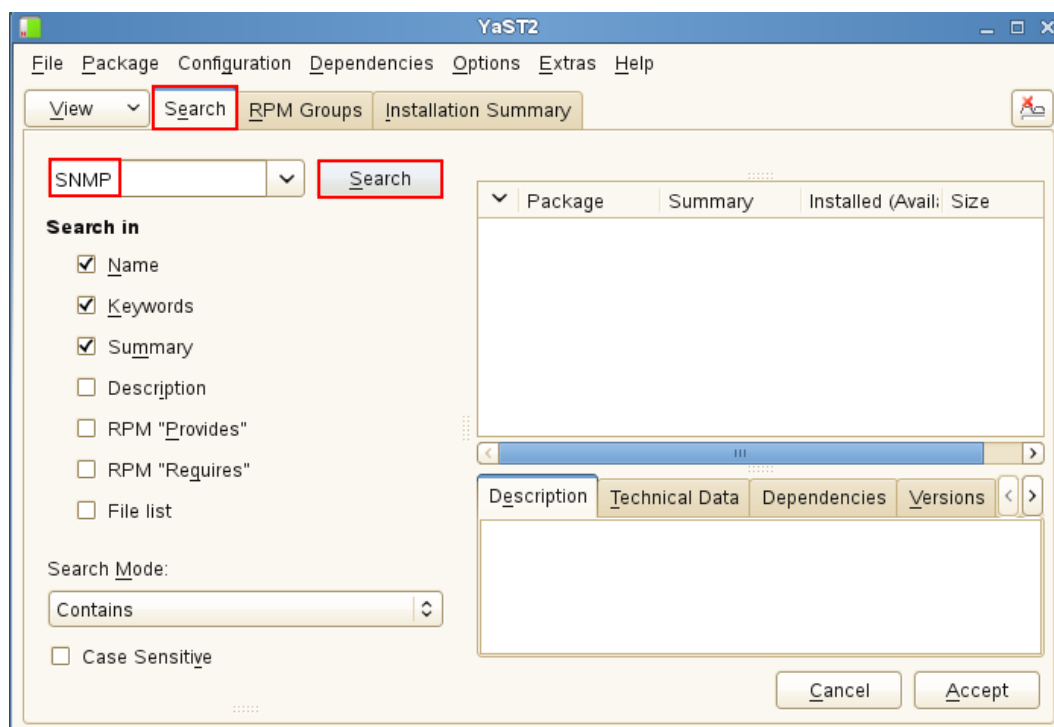
14. Select **Accept SNMP packets from any host**, and click **OK**.

**Figure 16-49** SNMP Service Security 2



- In the Linux operating system:
  1. Insert the SUSE Linux installation CD-ROM into the CD-ROM drive.
  2. Choose **Computer** > **Install Software**. The **YaST2** interface is displayed.
  3. Click the **Search** tab, set the search criteria to **SNMP**, and click **Search**.



**Figure 16-50** YaST2 Interface

4. Select SNMP components that you want to install, and click **Accept**.
5. After installing the SNMP components, run the following command to open the SNMP configuration file:  

```
vi /etc/snmp/snmpd.conf
```
6. Set **rocommunity** to **public** and **rwcommunity** to **private**.  
# on setting up groups and limiting MIBS.  
rocommunity public  
rwcommunity private
7. Enter **:wq** and press **Enter** to save and close the SNMP configuration file.
8. Access the **init.d** directory, and run the following command to restart the SNMP service:  

```
./snmpd restart
```

The following information indicates that SNMP parameters have been set:

```
Shutting down snmpd:
done
Starting snmpd
```

----End

## 16.14 How Do I Prevent Problems Caused by eSight Server System Time Change?

### Symptom

If the eSight server system time is changed, eSight may fail to work. For example, the topology is not refreshed.

### Procedure

**Step 1** Stop eSight services.

**Step 2** Restart eSight services.

----End

## 16.15 When I Use IE8 to Import Sheets, the System Displays an Incorrect Path. How Do I Solve the Problem?

### Symptom

When the security level of the browser is medium or high, eSight displays an incorrect path when you import sheets. However, sheets are imported successfully.

### Procedure

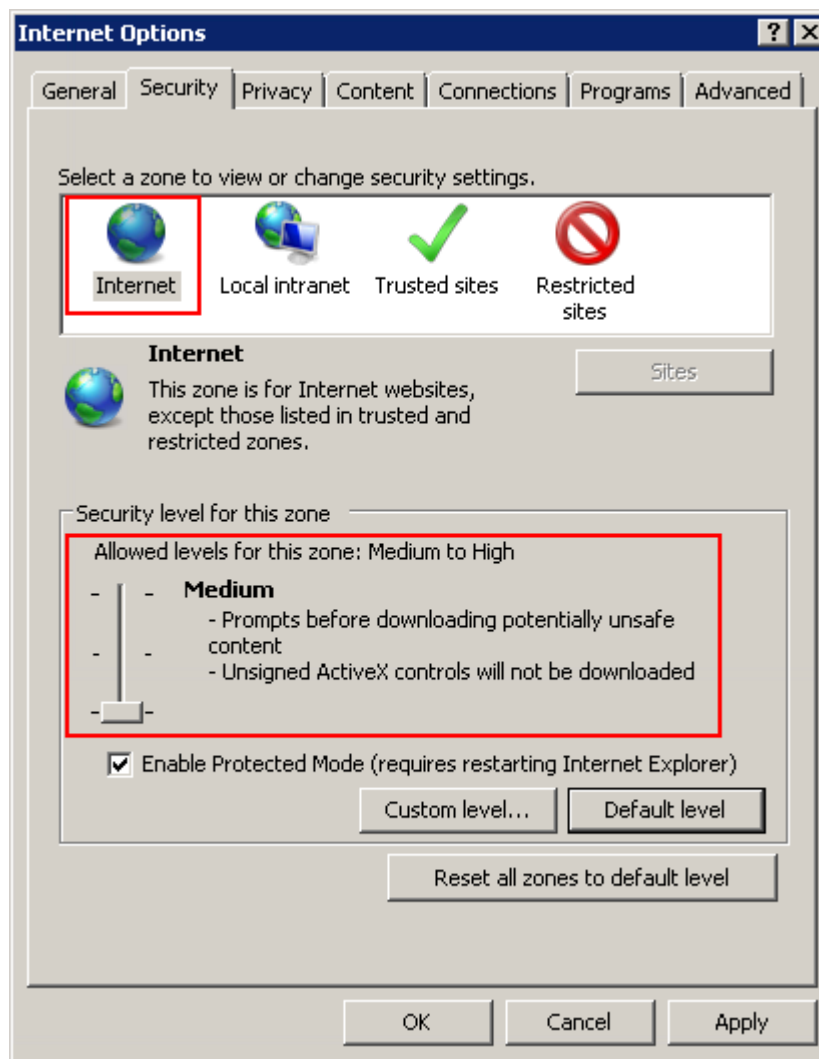
**Step 1** Open Internet Explorer 8.

**Step 2** Choose **Tools > Internet Options**.

**Step 3** In the **Internet Options** dialog box, choose **Security > Internet**.

**Step 4** Set **Allowed levels for this zone** to **Medium**, and click **OK**.

**Figure 16-51** Internet Options



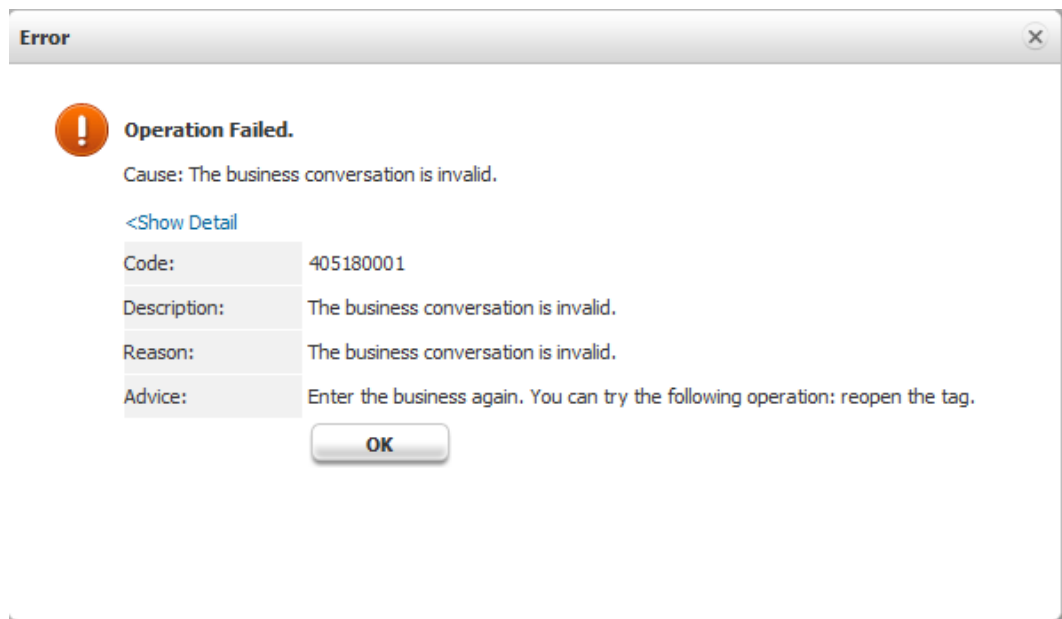
----End

## 16.16 How Do I Solve the Service Session Failure That Occurs When I Log In to eSight?

### Question

A user has already logged in to eSight. The user uses the same browser to log in to eSight on the same PC for a second time. A message indicating service session failure may be displayed on the first eSight page.

**Figure 16-52** Service session failure



## Answer

- Close the eSight page on which the error message is displayed.



## CAUTION

Do not use the same browser to log in to eSight on the same PC more than once.

---

----End

---

# A Glossary

---

## Numerics

|                   |                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1+1 backup</b> | A backup method in which two components mirror each other. If the active component goes down, the standby component takes over services from the active component to ensure that the system service is not interrupted. |
| <b>3GPP</b>       | 3rd Generation Partnership Project                                                                                                                                                                                      |

## A

|                   |                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>AAA</b>        | See <a href="#">Authentication, Authorization and Accounting</a> .                                                           |
| <b>AAA server</b> | The remote server that provides authentication, authorization, accounting, and value-added services for the dialed-in users. |
| <b>ABR</b>        | See <a href="#">area border router</a> .                                                                                     |
| <b>AC</b>         | See <a href="#">access control</a> .                                                                                         |
| <b>ACL</b>        | See <a href="#">access control list</a> .                                                                                    |
| <b>ACU</b>        | automatic calling unit                                                                                                       |
| <b>AD</b>         | active directory                                                                                                             |
| <b>ADAC</b>       | automatically detected and automatically cleared                                                                             |
| <b>ADMC</b>       | automatically detected and manually cleared                                                                                  |
| <b>AES</b>        | See <a href="#">Advanced Encryption Standard</a> .                                                                           |
| <b>AH</b>         | See <a href="#">Authentication Header</a> .                                                                                  |
| <b>AIS</b>        | alarm indication signal                                                                                                      |
| <b>ANCP</b>       | See <a href="#">Access Node Control Protocol</a> .                                                                           |
| <b>APID</b>       | access point identifier                                                                                                      |
| <b>APS</b>        | automatic protection switching                                                                                               |
| <b>ARP</b>        | See <a href="#">Address Resolution Protocol</a> .                                                                            |

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ARQ</b>                                                        | See <a href="#">automatic repeat request</a> .                                                                                                                                                                                                                                                                                                                                            |
| <b>AS</b>                                                         | See <a href="#">autonomous system</a> .                                                                                                                                                                                                                                                                                                                                                   |
| <b>ASBR</b>                                                       | See <a href="#">autonomous system boundary router</a> .                                                                                                                                                                                                                                                                                                                                   |
| <b>ASE</b>                                                        | amplified spontaneous emission                                                                                                                                                                                                                                                                                                                                                            |
| <b>ASIC</b>                                                       | See <a href="#">application-specific integrated circuit</a> .                                                                                                                                                                                                                                                                                                                             |
| <b>ASM</b>                                                        | See <a href="#">automatic storage management</a> .                                                                                                                                                                                                                                                                                                                                        |
| <b>ATAE</b>                                                       | See <a href="#">Advanced Telecommunications Application Environment</a> .                                                                                                                                                                                                                                                                                                                 |
| <b>ATM</b>                                                        | asynchronous transfer mode                                                                                                                                                                                                                                                                                                                                                                |
| <b>Access Node Control Protocol (ANCP)</b>                        | An IP-based protocol that operates between the access node (AN) and the network access server (NAS), over a DSL access and aggregation network.                                                                                                                                                                                                                                           |
| <b>Address Resolution Protocol (ARP)</b>                          | An Internet Protocol used to map IP addresses to MAC addresses. It allows hosts and routers to determine the link layer addresses through ARP requests and ARP responses.                                                                                                                                                                                                                 |
| <b>Advanced Encryption Standard (AES)</b>                         | An encryption algorithm that is originally used by some U.S. government departments to guarantee the security of some secret but unclassified material. Now, AES has become the most influential encryption standard all around the world. The AES algorithm is used to ensure the system security.                                                                                       |
| <b>Advanced Telecommunications Application Environment (ATAE)</b> | A carrier-class processing platform that is designed to meet the service application requirement of high performance, high specialization, and high integration.                                                                                                                                                                                                                          |
| <b>Authentication Header (AH)</b>                                 | A protocol that provides connectionless integrity, data origin authentication, and anti-replay protection for IP data.                                                                                                                                                                                                                                                                    |
| <b>Authentication, Authorization and Accounting (AAA)</b>         | A mechanism for configuring authentication, authorization, and accounting security services. Authentication refers to the verification of user identities and the related network services; authorization refers to the granting of network services to users according to authentication results; and accounting refers to the tracking of the consumption of network services by users. |
| <b>access control (AC)</b>                                        | A controlling mechanism that checks the request for access of external resources during the operation of the system.                                                                                                                                                                                                                                                                      |
| <b>access control list (ACL)</b>                                  | A list of entities, together with their access rights, which are authorized to have access to a resource.                                                                                                                                                                                                                                                                                 |
| <b>access security</b>                                            | The security of the measures taken to authenticate a user's access to the system.                                                                                                                                                                                                                                                                                                         |
| <b>active/standby switchover</b>                                  | A troubleshooting technology. When an active device becomes faulty, services and control functions are automatically switched over to the standby device to ensure the normal running of the services and functions.                                                                                                                                                                      |
| <b>administrative group</b>                                       | A 32-bit vector that represents a set of link attributes. In RFC 3209, administrative groups are called link-attributes.                                                                                                                                                                                                                                                                  |
| <b>application-specific integrated circuit (ASIC)</b>             | A special type of chip that starts out as a nonspecific collection of logic gates. Late in the manufacturing process, a layer is added to connect the gates for a specific function. By changing the pattern of connections, the manufacturer can make the chip suitable for many needs.                                                                                                  |
| <b>area border router</b>                                         | A router that can belong to more than two areas of which one area must be a backbone                                                                                                                                                                                                                                                                                                      |

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>(ABR)</b>                                    | area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>authentication server</b>                    | An entity that provides an Authentication Service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator.                                                                                                                                                                                                                                |
| <b>automatic repeat request (ARQ)</b>           | An error control method for data transmission in which the receiver detects transmission errors in a message and automatically requests a retransmission from the transmitter.                                                                                                                                                                                                                                                                                             |
| <b>automatic storage management (ASM)</b>       | A cluster volume manager and a file system for the Oracle database. The ASM provides asynchronous input/output (I/O) and simplifies database file storage and database management. Users can divide the available storage into disk groups. In this way, users need to manage only the disk groups rather than a large number of Oracle database files. The storage of database files in disk groups enhances the database performance and increases resource utilization. |
| <b>autonomous system (AS)</b>                   | A network set that uses the same routing policy and is managed by the same technology administration department. Each AS has a unique identifier that is an integer ranging from 1 to 65535. The identifier is assigned by IANA. An AS can be divided into areas.                                                                                                                                                                                                          |
| <b>autonomous system boundary router (ASBR)</b> | A router that exchanges routing information with other ASs.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>B</b>                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>B-VLAN</b>                                   | backbone virtual local area network                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>B/S</b>                                      | browser/server                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>BFD</b>                                      | See <a href="#">Bidirectional Forwarding Detection</a> .                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>BGP</b>                                      | Border Gateway Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>BITS</b>                                     | See <a href="#">building integrated timing supply</a> .                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>BOSS</b>                                     | See <a href="#">business and operation support system</a> .                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>BPDU</b>                                     | See <a href="#">bridge protocol data unit</a> .                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>BRAS</b>                                     | See <a href="#">broadband remote access server</a> .                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>BSSID</b>                                    | basic service set identifier                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>BW</b>                                       | business works                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Bidirectional Forwarding Detection (BFD)</b> | A simple Hello protocol, similar to the adjacent detection in the route protocol. Two systems periodically send BFD detection messages on the channel between the two systems. If one system does not receive the detection message from the other system for a long time, you can infer that the channel is faulty. Under some conditions, the TX and RX rates between systems need to be negotiated to reduce traffic load.                                              |
| <b>backup</b>                                   | A periodic operation performed on the data stored in the database for the purposes of database recovery in case that the database is faulty. The backup also refers to data synchronization between active and standby boards.                                                                                                                                                                                                                                             |
| <b>bit</b>                                      | The smallest unit of information handled by a hardware component. One bit expresses                                                                                                                                                                                                                                                                                                                                                                                        |

a 1 or a 0 in a binary numeral, or a true or a false logical condition, and is represented physically by an element such as a high or low voltage at one point in a circuit or a small spot on a disk magnetized one way or the other. A single bit conveys little information a human would consider meaningful. A group of eight bits, however, makes up a byte, which can be used to represent many types of information, such as a letter of the alphabet, a decimal digit, or other character.

**bit/s**

See [bits per second](#).

**bits per second (bit/s)**

A rate at which the individual bits are transmitted through a communication link or circuit. Its unit can be bit/s, kbit/s, and Mbit/s.

**bridge protocol data unit (BPDU)**

The data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol (STP) topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridges interfaces and placing redundant switch ports in a backup, or blocked, state.

**broadband remote access server (BRAS)**

A new type of access gateway for broadband networks. As a bridge between backbone networks and broadband access networks, BRAS provides methods for fundamental access and manages the broadband access network. It is deployed at the edge of network to provide broadband access services, convergence, and forwarding of multiple services, meeting the demands for transmission capacity and bandwidth utilization of different users. BRAS is a core device for the broadband users' access to a broadband network.

**broadcast domain**

A group of network stations that receives broadcast packets originating from any device within the group. The broadcast domain also refers to the set of ports between which a device forwards a multicast, broadcast, or unknown destination frame.

**building integrated timing supply (BITS)**

In the situation of multiple synchronous nodes or communication devices, one can use a device to set up a clock system on the hinge of telecom network to connect the synchronous network as a whole, and provide satisfactory synchronous base signals to the building integrated device. This device is called BITS.

**bus**

A path or channel for signal transmission. The typical case is that, the bus is an electrical connection that connects one or more conductors. All devices that are connected to a bus, can receive all transmission contents simultaneously.

**business and operation support system (BOSS)**

The operation support platform of an enterprise. It provides end-to-end business flow support for the carrier to handle routine tasks such as customer service, rating, billing, settlement and dunning.

**bypass tunnel**

A tunnel that is used to protect a group of MPLS tunnels in the facility backup. The MPLS tunnels protected share this tunnel. A bypass tunnel needs to be created beforehand.

**byte**

A unit of computer information equal to eight bits.

**C****CA**

See [call agent](#).

**CAC**

See [call admission control](#).

**CAM**

content addressable memory



|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CAPWAP</b>                             | See <a href="#">Control and Provisioning of Wireless Access Points</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>CAPWAP tunnel</b>                      | A tunnel transmitting management packets and data packets between the AC and the AP when the AP is registering with the AC. The management packets exchanged between the AC and the AP must be encapsulated in the CAPWAP tunnel for transmission. This means that a CAPWAP management tunnel needs to be set up, and such a tunnel requires no additional hardware. Whether the data packets exchanged between the AC and the AP need to be encapsulated in the CAPWAP tunnel depends on actual configuration scenarios. If yes, a CAPWAP data tunnel needs to be set up between the AC and the AP. This tunnel requires additional hardware, which implements tunnel capsulation and decapsulation. If no, data packets of the AP are directly forwarded. |
| <b>CAR</b>                                | committed access rate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>CC</b>                                 | See <a href="#">continuity check</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>CCM</b>                                | central control module                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>CD-ROM</b>                             | compact disc read-only memory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CDR</b>                                | See <a href="#">call detail record</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>CE</b>                                 | See <a href="#">customer edge</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>CES</b>                                | See <a href="#">circuit emulation service</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>CFM</b>                                | connectivity fault management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CG</b>                                 | center gap                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>CHAP</b>                               | See <a href="#">Challenge Handshake Authentication Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>CLC</b>                                | cluster line-card chassis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>CLI</b>                                | command-line interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>CLK</b>                                | clock card                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>CMI</b>                                | coded mark inversion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>CPLD</b>                               | complex programmable logical device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>CPU</b>                                | See <a href="#">central processing unit</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CR-LSP</b>                             | constraint-based routed label switched path                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>CRC</b>                                | See <a href="#">cyclic redundancy check</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CRD</b>                                | call rerouting distribution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>CRL</b>                                | See <a href="#">certificate revocation list</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>CSPF</b>                               | constraint shortest path first                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>CSS</b>                                | cascading style sheet                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>CSV</b>                                | comma-separated values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>CT</b>                                 | class type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Challenge Handshake Authentication</b> | A method to periodically verify the identity of the peer using a 3-way handshake. During the establishment of a link, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" function. The                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol (CHAP)</b>                                             | authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. CHAP provides protection against playback attack.                                                                                                                                                                                                                                                                        |
| <b>Control and Provisioning of Wireless Access Points (CAPWAP)</b> | A protocol that defines how communication is implemented between an access point (AP) and an access controller (AC) and provides a universal encapsulation and transmission mechanism for the interoperation between the AP and the AC.                                                                                                                                                                                                                                     |
| <b>Coordinated Universal Time (UTC)</b>                            | The world-wide scientific standard of timekeeping. It is based upon carefully maintained atomic clocks and is kept accurate to within microseconds worldwide.                                                                                                                                                                                                                                                                                                               |
| <b>call admission control (CAC)</b>                                | The function of configuring policies on the last-hop multicast Router connected to the receiver, intermediate multicast routers, and the first-hop Router connected to the source to limit the number of multicast entries that the routers can create. After multicast CAC is configured, operators can control the number of multicast groups that users can access on the IP core network.                                                                               |
| <b>call agent (CA)</b>                                             | An external call control unit for controlling telephony gateways. A CA provides signaling and call processing functions.                                                                                                                                                                                                                                                                                                                                                    |
| <b>call detail record (CDR)</b>                                    | A database record unit used to create billing records. A CDR contains details such as the called and calling parties, originating switch, terminating switch, call length, and time of day.                                                                                                                                                                                                                                                                                 |
| <b>central processing unit (CPU)</b>                               | The computational and control unit of a computer. The CPU is the device that interprets and executes instructions. The CPU has the ability to fetch, decode, and execute instructions and to transfer information to and from other resources over the computer's main data-transfer path, the bus.                                                                                                                                                                         |
| <b>certificate revocation list (CRL)</b>                           | A list of all canceled certificates. A time-stamped list of certificates that have been revoked by the Certification Authority (CA). The CRL is signed by the issuing CA and is made available to entities that need to reply on a certificate for authentication.                                                                                                                                                                                                          |
| <b>channel</b>                                                     | A telecommunication path of a specific capacity and/or at a specific speed between two or more locations in a network. Channels can be established through wire, radio (microwave), fiber or a combination of the three. The amount of information transmitted per second in a channel is the information transmission speed, expressed in bits per second. For example, b/s, kb/s, Mb/s, Gb/s, and Tb/s.                                                                   |
| <b>circuit emulation service (CES)</b>                             | A function with which the E1/T1 data can be transmitted through ATM networks. At the transmission end, the interface module packs timeslot data into ATM cells. These ATM cells are sent to the reception end through the ATM network. At the reception end, the interface module re-assigns the data in these ATM cells to E1/T1 timeslots. The CES technology guarantees that the data in E1/T1 timeslots can be recovered to the original sequence at the reception end. |
| <b>cluster</b>                                                     | A mechanism adopted to improve the system performance. Several devices of the same type form a cluster. The exterior of a cluster is some like a kind of equipment. In the interior of a cluster, the nodes share the load.                                                                                                                                                                                                                                                 |
| <b>community name</b>                                              | Name of an application entity in the SNMP protocol. A community name together with certain additional information from a sender are used to verify whether the sender is a community member.                                                                                                                                                                                                                                                                                |
| <b>continuity check (CC)</b>                                       | Ethernet CFM can detect the connectivity between MEPs. The detection is achieved after MEPs transmit Continuity Check Messages (CCMs) periodically.                                                                                                                                                                                                                                                                                                                         |
| <b>control channel</b>                                             | The channel used to transmit digital control information from the base station to a cell                                                                                                                                                                                                                                                                                                                                                                                    |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | phone or vice-versa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>convergence layer</b>              | A "bridge" between the access layer and the core layer. The convergence layer provides the convergence and forwarding functions for the access layer. It processes all the traffic from the access layer devices, and provides the uplinks to the core layer. Compared with the access layer, the convergence layer devices should have higher performance, fewer interfaces and higher switching rate. In the real network, the convergence layer refers to the network between UPEs and PE-AGGs.                                                                                                                |
| <b>crystal oscillator</b>             | An oscillator that produces electrical oscillations at a frequency determined by the physical characteristics of a piezoelectric quartz crystal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>customer edge (CE)</b>             | A part of BGP/MPLS IP VPN model. It provides interfaces for direct connection to the Service Provider (SP) network. A CE can be a router, switch, or host.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>cyclic redundancy check (CRC)</b>  | A procedure used in checking for errors in data transmission. CRC error checking uses a complex calculation to generate a number based on the data transmitted. The sending device performs the calculation before transmission and includes it in the packet that it sends to the receiving device. The receiving device repeats the same calculation after transmission. If both devices obtain the same result, it is assumed that the transmission was error free. The procedure is known as a redundancy check because each transmission includes not only data but extra (redundant) error-checking values. |
| <b>D</b>                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>DB</b>                             | database                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>DC</b>                             | direct current                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>DD</b>                             | database description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>DES</b>                            | See <a href="#">Data Encryption Standard</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>DHCP</b>                           | See <a href="#">Dynamic Host Configuration Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>DIMM</b>                           | See <a href="#">dual in-line memory module</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>DMZ</b>                            | See <a href="#">demilitarized zone</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>DNS</b>                            | See <a href="#">domain name server</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>DNS server</b>                     | A device that can provide domain name resolution for the client on the network                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>DOD</b>                            | See <a href="#">direct outward dialing</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>DPI</b>                            | deep packet inspection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>DR</b>                             | See <a href="#">designated router</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>DRR</b>                            | dynamic rate repartitioning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>DSCP</b>                           | See <a href="#">differentiated services code point</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>DSP</b>                            | See <a href="#">digital signal processor</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>DST</b>                            | daylight saving time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Data Encryption Standard (DES)</b> | A specification for encryption of computer data developed by IBM and adopted by the U.S. government as a standard in 1976. DES uses a 56-bit key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Dynamic Host</b>                   | A client-server networking protocol. A DHCP server provides configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configuration Protocol (DHCP)</b>             | parameters specific to the DHCP client host requesting, generally, information required by the host to participate on the Internet network. DHCP also provides a mechanism for allocation of IP addresses to hosts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>data bus</b>                                  | A line or set of lines that connects multiple data processing units for the reception and transmission of the data between those units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>data flow</b>                                 | A process that involves processing the data extracted from the source system, such as filtering, integration, calculation, and summary, finding and solving data inconsistency, and deleting invalid data so that the processed data meets the requirements of the destination system for the input data.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>database server</b>                           | The database management software running on one or more servers in a LAN. The database server provides services for users' applications. These services include query, update, event management, index, cache, query optimization, security, and multiuser access control.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>demilitarized zone (DMZ)</b>                  | A buffer area between an insecure system and the secure system and is used to solve the problem that the external network equipped with a firewall cannot access the internal network server. The DMZ is located between the internal network and the external network. In the DMZ, some public server facilities, such as the enterprise Web server and FTP server, can be located. The DMZ effectively protects the internal network.                                                                                                                                                                                                                                              |
| <b>designated router (DR)</b>                    | A functional entity in the TCP/IP network. A DR is selected by the OSPF Hello protocol to prevent repeated link status exchanges between routers in an Open Shortest Path First (OSPF) area. All routers in an OSPF area are connected to a DR. When routing data updates in routers, a message about link status is sent to the DR, and the DR sends the message to routers. Therefore, bandwidth resources can be saved.                                                                                                                                                                                                                                                           |
| <b>differentiated services code point (DSCP)</b> | According to the QoS classification standard of the Differentiated Service (Diff-Serv), the type of services (ToS) field in the IP header consists of six most significant bits and two currently unused bits, which are used to form codes for priority marking. Differentiated services code point (DSCP) is the six most important bits in the ToS. It is the combination of IP precedence and types of service. The DSCP value is used to ensure that routers supporting only IP precedence can be used because the DSCP value is compatible with IP precedence. Each DSCP maps a per-hop behavior (PHB). Therefore, terminal devices can identify traffic using the DSCP value. |
| <b>digital signal processor (DSP)</b>            | A microprocessor designed specifically for digital signal processing, generally in real time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>direct outward dialing (DOD)</b>              | A facility of a PABX that allows internal users to make outgoing calls without operator intervention.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>domain name server (DNS)</b>                  | A functional entity in the TCP/IP network. With deployment of the DNS, subscribers can access related servers using corresponding domain names. In the TCP/IP network, a domain name maps an IP address. Domain names are easier to remember but serves in the network communicate with each other using IP addresses. Therefore the DNS is used to convert domain names to corresponding IP addresses.                                                                                                                                                                                                                                                                              |
| <b>downstream</b>                                | In an access network, the direction of transmission toward the subscriber end of the link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>downstream interface</b>                      | The interface that forwards multicast data. The router or the receiver host that the sent multicast data reaches is called downstream router or downstream host. The network segment where the downstream interface resides is called downstream network segment.                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dual in-line memory module (DIMM)</b>                           | A circuit board on which RAM memory chips are mounted. A DIMM is a small circuit board that can hold a group of memory chips. A DIMM is capable of transferring 64 bits instead of 32 bits that each SIMM can transfer. Pentium processors require a 64-bit path to memory so SIMMs must be installed two at a time as opposed to one DIMM at a time.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>dump</b>                                                        | To export alarm data from the database to the customized file. Meanwhile the exported data is cleared in the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>E</b>                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>EBGP</b>                                                        | External Border Gateway Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>ECC</b>                                                         | See <a href="#">error checking and correcting</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>EEPROM</b>                                                      | See <a href="#">electrically erasable programable read-only memory</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>EFM</b>                                                         | Ethernet in the First Mile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>EMC</b>                                                         | See <a href="#">electromagnetic compatibility</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>EPLD</b>                                                        | See <a href="#">erasable programmable logical device</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>EPON</b>                                                        | See <a href="#">Ethernet passive optical network</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>ESN</b>                                                         | See <a href="#">equipment serial number</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>ESP</b>                                                         | See <a href="#">Encapsulating Security Payload</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>ESS</b>                                                         | See <a href="#">extended service set</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Encapsulating Security Payload (ESP)</b>                        | A key protocol in the IP Security (IPsec) architecture. ESP adopts encryption and authentication mechanisms. It is used in transport mode or tunnel mode to authenticate the source of IP packets, and ensure data integrity, anti-replay, and confidentiality. ESP provides data confidentiality and integrity by encrypting the data to be protected and placing the encrypted data in the data part of the IP ESP. Based on security requirements of subscribers, this mechanism can be used to encrypt either a transport-layer segment or an IP data packet. A transport-layer segment includes Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP). |
| <b>Ethernet</b>                                                    | A LAN technology that uses Carrier Sense Multiple Access/Collision Detection. The speed of an Ethernet interface can be 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s or 10000 Mbit/s. An Ethernet network features high reliability and is easy to maintain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Ethernet passive optical network (EPON)</b>                     | A passive optical network based on Ethernet. It is a new generation broadband access technology that uses a point-to-multipoint structure and passive fiber transmission. It supports upstream/downstream symmetrical rates of 1.25 Gbit/s and a reach distance of up to 20 km. In the downstream direction, the bandwidth is shared based on encrypted broadcast transmission for different users. In the upstream direction, the bandwidth is shared based on TDM. EPON meets the requirements for high bandwidth.                                                                                                                                                                                                                                             |
| <b>electrically erasable programable read-only memory (EEPROM)</b> | A type of EPROM that can be erased with an electrical signal. It is useful for stable storage for long periods without electricity while still allowing reprogramming. EEPROMs contain less memory than RAM, take longer to reprogram, and can be reprogrammed only a limited number of times before wearing out.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>electromagnetic</b>                                             | A condition which prevails when telecommunications equipment is performing its                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>compatibility (EMC)</b>                         | individually designed function in a common electromagnetic environment without causing or suffering unacceptable degradation due to unintentional electromagnetic interference to or from other equipment in the same environment.                                                                                                                                                                                                                                                                                         |
| <b>equipment serial number (ESN)</b>               | A string of characters that identify a piece of equipment and ensures correct allocation of a license file to the specified equipment. It is also called "equipment fingerprint".                                                                                                                                                                                                                                                                                                                                          |
| <b>erasable programmable logical device (EPLD)</b> | A logical array device which can be used to implement the required functions by programming the array. In addition, a user can modify and program the array repeatedly until the program meets the requirement.                                                                                                                                                                                                                                                                                                            |
| <b>error checking and correcting (ECC)</b>         | A technique used for detecting and correcting errors by adding check bits to the source bits. If the source data has eight bits, five check bits are required to perform error checking and correcting. When the data bits are doubled every time, one more check bit is required. Compared with the parity check, the ECC can not only detect but also correct errors. This improves the reliability of data storage. This technique can be used in the ECC memory to improve the security and reliability of the memory. |
| <b>explicit path</b>                               | The displayed path is one constraint configured for LSP. It is the confirmation and constraint for the LSR on LSP. The types of the displayed path contain the strict included, loose included, and excluded. If the constraint information accurately specifies the LSR on LSP, the LSP is the strict included explicit Path. If the downstream LSR is ambiguously defined, the established LSP is the loose included explicit path. If the constraint information excludes some node, the path is the excluded path.     |
| <b>extended service set (ESS)</b>                  | A set of one or more interconnected basic service sets (BSSs) that appears as a single BSS to the logical link control (LLC) layer at any station (STA) associated with one of those BSSs.                                                                                                                                                                                                                                                                                                                                 |
| <b>F</b>                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>FAD</b>                                         | fabric adapter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>FCB</b>                                         | fan control board                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FDI</b>                                         | See <a href="#">forward defect indication</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>FE</b>                                          | See <a href="#">fast Ethernet</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>FEC</b>                                         | See <a href="#">forwarding equivalence class</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>FIB</b>                                         | See <a href="#">forward information base</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>FIT</b>                                         | failures in time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>FPGA</b>                                        | See <a href="#">field programmable gate array</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>FPIC</b>                                        | flexible plug-in card                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>FQ</b>                                          | See <a href="#">fair queue</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>FR</b>                                          | See <a href="#">frame relay</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FRR</b>                                         | See <a href="#">fast reroute</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>FSM</b>                                         | finite state machine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>FTP</b>                                         | File Transfer Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FTP server (FTPS)</b>                    | A file server that uses the File Transfer Protocol (FTP) to permit users to upload or download files through the Internet or any other TCP/IP network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>FTPS</b>                                 | See <a href="#">FTP server</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>FUP</b>                                  | See <a href="#">fair usage policy</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>fair queue (FQ)</b>                      | A mechanism for queue scheduling in which network resource is allocated equally so that delay and jitter time for all traffic are optimal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>fair usage policy (FUP)</b>              | An operational strategy taken in the mobile broadband market, is designed to address the problem that network resources are overused by some subscribers. FUP ensures equality of resource usage between subscribers when network resources are limited. FUP enables carriers to restrict a subscriber's total network resource usage in a specific period of time and to implement access control on the subscriber after the resource usage of the subscriber exceeds a specified limit. When the resource usage exceeds the limit, FUP can be implemented to restrict the transmission rate for the subscriber, terminate services for the subscriber, or charge the subscriber extra fees. FUP complies with the principle of network neutrality and is not intended to restrict services of specific protocols or applications. FUP restricts service requests from subscribers who use a bandwidth-hungry service so frequently that the traffic volume or access duration of the subscriber is far above the average level. |
| <b>fast Ethernet (FE)</b>                   | Any network that supports transmission rate of 100 Mbit/s. The Fast Ethernet is 10 times faster than 10BaseT, and inherits frame format, MAC addressing scheme, MTU, and so on. Fast Ethernet is extended based on the IEEE802.3 standard, and it uses the following three types of transmission media: 100BASE-T4 (4 pairs of phone twisted-pair cables), 100BASE-TX (2 pairs of data twisted-pair cables), and 100BASE-FX (2-core optical fibers).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>fast reroute (FRR)</b>                   | A technology to locally protect MPLS TE network. Only the interface with the speed of 100 Mbit/s can support FRR. If the switching speed of FRR can reach 50 ms, the packet loss decreases when some faults occur on the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>field programmable gate array (FPGA)</b> | A type of semi-customized circuit used in the application specific integrated circuit (ASIC) field. It is developed on the basis of the programmable components, such as the PAL, GAL, and EPLD. It not only remedies the defects of customized circuits but also overcomes the disadvantage of the original programmable components in terms of the limited number of gate arrays.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>firewall</b>                             | A combination of a series of components set between different networks or network security domains. By monitoring, limiting, and changing the data traffic across the firewall, it masks the interior information, structure and running state of the network as much as possible to protect the network security.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>forward defect indication (FDI)</b>      | A packet generated and traced forward to the sink node of the LSP by the node that first detects defects. It includes fields to indicate the nature of the defect and its location. Its primary purpose is to suppress alarms being raised at affected higher level client LSPs and (in turn) their client layers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>forward information base (FIB)</b>       | A table that provides information for network hardware (bridges and routers) for them to forward data packets to other networks. The information contained in a routing table differs according to whether it is used by a bridge or a router. A bridge relies on both the source (originating) and destination addresses to determine where and how to forward a packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>forwarding equivalence class</b>         | A class-based forwarding technology that classifies the packets with the same forwarding mode. Packets with the same FEC are processed similarly on an MPLS network. The division of FECs is flexible, and can be a combination of the source                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>(FEC)</b>                            | address, destination address, source port, destination port, protocol type, and VPN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>frame relay (FR)</b>                 | A packet-switching protocol used for WANs. Frame relay transmits variable-length packets at up to 2 Mbit/s over predetermined, set paths known as PVCs (permanent virtual circuits). It is a variant of X.25 but sacrifices X.25's error detection for the sake of speed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>G</b>                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>GE</b>                               | See <a href="#">gigabit Ethernet</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>GEM</b>                              | GPON encapsulation mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>GGSN</b>                             | See <a href="#">gateway GPRS support node</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>GPRS tunneling protocol (GTP)</b>    | GPRS Tunneling Protocol (GTP), an IP-based protocol, is used for general packet radio service (GPRS) communication in Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks. The GTP includes GTP-C and GTP-U. GTP-C is used to transmit signaling for path management, tunnel management, mobility management, and location management. GTP-C performs controls on tunnels in which subscriber data is transferred. GTP-U is used to encapsulate subscriber data and transport subscriber data in tunnels. For details about GTP, see 3GPP TS 29.060.                                                                                                                                                   |
| <b>GR</b>                               | See <a href="#">graceful restart</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>GTP</b>                              | See <a href="#">GPRS tunneling protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>GUI</b>                              | graphical user interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>gateway</b>                          | A device that connects two network segments using different protocols. It is used to translate the data in the two network segments.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>gateway GPRS support node (GGSN)</b> | A functional entity that provides packet data services. It is in charge of the routing and encapsulation of the packet data between the General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) network and the external PDN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>gigabit Ethernet (GE)</b>            | A collection of technologies for transmitting Ethernet frames at a rate of a gigabit per second, as defined by the IEEE 802.3z standard. GE is compatible with 10 Mbit/s and 100 Mbit/s Ethernet. It runs at 1000 Mbit/s. Gigabit Ethernet uses a private medium, and it does not support coaxial cables or other cables. It also supports the channels in the bandwidth mode. If Gigabit Ethernet is, however, deployed to be the private bandwidth system with a bridge (switch) or a router as the center, it gives full play to the performance and the bandwidth. In the network structure, Gigabit Ethernet uses full duplex links that are private, causing the length of the links to be sufficient for backbone applications in a building and campus. |
| <b>graceful restart (GR)</b>            | In IETF, protocols related to Internet Protocol/Multiprotocol Label Switching (IP/MPLS) such as Open Shortest Path First (OSPF), Intermediate System-Intermediate System (IS-IS), Border Gateway Protocol (BGP), Label Distribution Protocol (LDP), and Resource Reservation Protocol (RSVP) are extended to ensure that the forwarding is not interrupted when the system is restarted. This reduces the flapping of the protocols at the control plane when the system performs an active/standby switchover. This series of standards is called graceful restart.                                                                                                                                                                                            |



**H**

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HA</b>                                         | See <a href="#">high availability</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>HA system</b>                                  | high availability system                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>HCT</b>                                        | health check tool                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>HDLC</b>                                       | High-Level Data Link Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>HGMP</b>                                       | Huawei Group Management Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>HTML</b>                                       | Hypertext Markup Language                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>HTTP</b>                                       | See <a href="#">Hypertext Transfer Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>HTTPS</b>                                      | See <a href="#">Hypertext Transfer Protocol Secure</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hypertext Transfer Protocol (HTTP)</b>         | An application-layer protocol used for communications between web servers and browsers or other programs. HTTP adopts the request-response mode. A client sends a request to the server. The request consists of two parts: request header and MIME-like message. The request header contains request method, uniform resource locator (URL), and protocol version. The MIME-like message contains request modifiers, client information, and possible body content. Upon receiving the request, the server responds with a status line. The status line includes the message's protocol version, a success or error code, and a MIME-like message, which contains server information, entity meta-information, and possible entity-body content. For details about HTTP, see RFC2616. |
| <b>Hypertext Transfer Protocol Secure (HTTPS)</b> | An HTTP protocol that runs on top of transport layer security (TLS) and Secure Sockets Layer (SSL). It is used to establish a reliable channel for encrypted communication and secure identification of a network web server. For details, see RFC2818.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>high availability (HA)</b>                     | A scheme in which two modules operate in active/standby mode to achieve high availability. When the active module fails, the standby module automatically takes over the system functions of the active module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>hop</b>                                        | A network connection between two distant nodes. For Internet operation a hop represents a small step on the route from one main computer to another.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>host name</b>                                  | A fully qualified domain name (FQDN) of a functional entity, which is used for routing. It is planned by carriers uniformly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**I**

|             |                                                                         |
|-------------|-------------------------------------------------------------------------|
| <b>IANA</b> | See <a href="#">Internet Assigned Numbers Authority</a> .               |
| <b>ICMP</b> | See <a href="#">Internet Control Message Protocol</a> .                 |
| <b>ID</b>   | See <a href="#">identity</a> .                                          |
| <b>IEEE</b> | See <a href="#">Institute of Electrical and Electronics Engineers</a> . |
| <b>IGMP</b> | See <a href="#">Internet Group Management Protocol</a> .                |
| <b>IGP</b>  | See <a href="#">Interior Gateway Protocol</a> .                         |
| <b>IKE</b>  | See <a href="#">Internet Key Exchange</a> .                             |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP</b>                                                       | Internet Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IP Security (IPSec)</b>                                      | A protocol family defined by the Internet Engineering Task Force (IETF). By authenticating and encrypting each IP packet of a data stream, this protocol family provides high quality, interoperable, and cryptology-based security for IP packets.                                                                                                                                                                                                                             |
| <b>IP address</b>                                               | A 32-bit (4-byte) binary digit that uniquely identifies a host (computer) connected to the Internet for communication with other hosts in the Internet by transferring packets. An IP address is expressed in dotted decimal notation, consisting of decimal values of its 4 bytes, separated by periods (.), for example, 127.0.0.1. The first three bytes of an IP address identify the network to which the host is connected, and the last byte identifies the host itself. |
| <b>IPE</b>                                                      | in-path equipment                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IPSec</b>                                                    | See <a href="#">IP Security</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IPv4</b>                                                     | See <a href="#">Internet Protocol version 4</a> .                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IPv6</b>                                                     | See <a href="#">Internet Protocol version 6</a> .                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IS-IS</b>                                                    | See <a href="#">Intermediate System to Intermediate System</a> .                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>ISAKMP</b>                                                   | See <a href="#">Internet Security Association and Key Management Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>ISO</b>                                                      | International Organization for Standardization                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>ISP</b>                                                      | See <a href="#">Internet service provider</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>ISSU</b>                                                     | See <a href="#">in-service software upgrade</a> .                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Institute of Electrical and Electronics Engineers (IEEE)</b> | A society of engineering and electronics professionals based in the United States but boasting membership from numerous other countries. The IEEE focuses on electrical, electronics, computer engineering, and science-related matters.                                                                                                                                                                                                                                        |
| <b>Interior Gateway Protocol (IGP)</b>                          | A routing protocol that is used within an autonomous system. The IGP runs in small-sized and medium-sized networks. The commonly used IGPs are the routing information protocol (RIP), the interior gateway routing protocol (IGRP), the enhanced IGRP (EIGRP), and the open shortest path first (OSPF).                                                                                                                                                                        |
| <b>Intermediate System to Intermediate System (IS-IS)</b>       | A protocol used by network devices (routers) to determine the best way to forward datagram or packets through a packet-based network.                                                                                                                                                                                                                                                                                                                                           |
| <b>Internet Assigned Numbers Authority (IANA)</b>               | A department operated by the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.                                                                                                                                                                                        |
| <b>Internet Control Message Protocol (ICMP)</b>                 | A network-layer (ISO/OSI level 3) Internet protocol that provides error correction and other information relevant to IP packet processing. For example, it can let the IP software on one machine inform another machine about an unreachable destination. See also communications protocol, IP, ISO/OSI reference model, packet (definition 1).                                                                                                                                |
| <b>Internet Group Management Protocol (IGMP)</b>                | One of the TCP/IP protocols for managing the membership of Internet Protocol multicast groups. It is used by IP hosts and adjacent multicast routers to establish and maintain multicast group memberships.                                                                                                                                                                                                                                                                     |
| <b>Internet Key Exchange (IKE)</b>                              | A hybrid protocol that implements Oakley key exchange and SKEME key exchange in the ISAKMP frame. Both Oakley and SKEME define a key exchange method, including the structure of the valid payload, valid payload of transmitted information,                                                                                                                                                                                                                                   |

handling procedure of the key, and method to use the key.

**Internet Protocol version 4 (IPv4)**

The current version of the Internet Protocol (IP). IPv4 utilizes a 32bit address which is assigned to hosts. An address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods and may range from 0.0.0.0 through to 255.255.255.255. Each IPv4 address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork.

**Internet Protocol version 6 (IPv6)**

An update version of IPv4, which is designed by the Internet Engineering Task Force (IETF) and is also called IP Next Generation (IPng). It is a new version of the Internet Protocol. The difference between IPv6 and IPv4 is that an IPv4 address has 32 bits while an IPv6 address has 128 bits.

**Internet Security Association and Key Management Protocol (ISAKMP)**

A protocol that allows the message receiver to obtain a public key and use digital certificates to authenticate the sender's identity.

**Internet service provider (ISP)**

An organization that offers users access to the Internet and related services.

**identity (ID)**

The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.

**in-service software upgrade (ISSU)**

An upgrade mode. In this mode, the active and standby SCC boards are reset separately during the activation process, without interrupting services. In addition, the system checks information such as NE status, basic services, and routing relationship automatically.

**interface status**

The running status of an interface, which can be normal, blocked, disabled, or not learning MAC address.

**J****JTAG**

See [Joint Test Action Group](#).

**Joint Test Action Group (JTAG)**

An organization composed by several main electronic manufactures with the purpose of establishing PCB and IC standards. JTAG, also as an international hardware test specification (compatible with IEEE 1149.1) proposed by this organization, is used to test chip interiors.

**K****KPI**

key performance indicator

**L****L2TP**

Layer 2 Tunneling Protocol

**L2TP access concentrator (LAC)**

A node that acts as an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC resides between an LNS and a remote system to exchange packets

|                                                     |                                                                                                                                                                                                                      |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     | between them.                                                                                                                                                                                                        |
| <b>L2TP network server (LNS)</b>                    | A node that acts as an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. |
| <b>L2VPN</b>                                        | Layer 2 virtual private network                                                                                                                                                                                      |
| <b>L3VPN</b>                                        | Layer 3 virtual private network                                                                                                                                                                                      |
| <b>LA</b>                                           | line amplifier                                                                                                                                                                                                       |
| <b>LAC</b>                                          | See <a href="#">L2TP access concentrator</a> .                                                                                                                                                                       |
| <b>LACP</b>                                         | See <a href="#">Link Aggregation Control Protocol</a> .                                                                                                                                                              |
| <b>LAG</b>                                          | See <a href="#">link aggregation group</a> .                                                                                                                                                                         |
| <b>LAN</b>                                          | See <a href="#">local area network</a> .                                                                                                                                                                             |
| <b>LCD</b>                                          | liquid crystal display                                                                                                                                                                                               |
| <b>LCP</b>                                          | Link Control Protocol                                                                                                                                                                                                |
| <b>LDAP</b>                                         | See <a href="#">Lightweight Directory Access Protocol</a> .                                                                                                                                                          |
| <b>LDP</b>                                          | Label Distribution Protocol                                                                                                                                                                                          |
| <b>LIG</b>                                          | lawful interception gateway                                                                                                                                                                                          |
| <b>LIU</b>                                          | logical interface unit                                                                                                                                                                                               |
| <b>LLDP</b>                                         | See <a href="#">Link Layer Discovery Protocol</a> .                                                                                                                                                                  |
| <b>LNS</b>                                          | See <a href="#">L2TP network server</a> .                                                                                                                                                                            |
| <b>LOS</b>                                          | See <a href="#">loss of signal</a> .                                                                                                                                                                                 |
| <b>LPU</b>                                          | line interface processing unit                                                                                                                                                                                       |
| <b>LSA</b>                                          | link-state advertisement                                                                                                                                                                                             |
| <b>LSDB</b>                                         | link state database                                                                                                                                                                                                  |
| <b>LSP</b>                                          | See <a href="#">label switched path</a> .                                                                                                                                                                            |
| <b>LSR</b>                                          | See <a href="#">label switching router</a> .                                                                                                                                                                         |
| <b>Layer 2 multicast</b>                            | A technology that maps IP multicast addresses to multicast MAC addresses. When Ethernet is used as the link layer, Layer 2 multicast uses multicast MAC addresses for traffic transmission.                          |
| <b>Lightweight Directory Access Protocol (LDAP)</b> | A TCP/IP based network protocol that enables access to a DSA. It involves some reduced functionality from X.500 DAP specification.                                                                                   |
| <b>Link Aggregation Control Protocol (LACP)</b>     | A method of bundling a group of physical interfaces together as a logical interface to increase bandwidth and reliability. For related protocols and standards, refer to IEEE 802.3ad.                               |
| <b>Link Layer Discovery Protocol (LLDP)</b>         | The Link Layer Discovery Protocol (LLDP) is an L2D protocol defined in IEEE 802.1ab. Using the LLDP, the NMS can rapidly obtain the Layer 2 network topology and changes in topology when the network scales expand. |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>label switched path (LSP)</b>    | A sequence of hops (R0...Rn) in which a packet travels from R0 to Rn through label switching mechanisms. A label-switched path can be chosen dynamically, based on common routing mechanisms or through configuration.                                                                                                                                                                          |
| <b>label switching router (LSR)</b> | Basic element of an MPLS network. All LSRs support the MPLS protocol. The LSR is composed of two parts: control unit and forwarding unit. The former is responsible for allocating the label, selecting the route, creating the label forwarding table, creating and removing the label switch path; the latter forwards the labels according to groups received in the label forwarding table. |
| <b>license</b>                      | A permission that the vendor provides for the user with a specific function, capacity, and duration of a product. A license can be a file or a serial number. Usually the license consists of encrypted codes. The operation authority granted varies with the level of the license.                                                                                                            |
| <b>linear MSP</b>                   | linear multiplex section protection                                                                                                                                                                                                                                                                                                                                                             |
| <b>link aggregation group (LAG)</b> | An aggregation that allows one or more links to be aggregated together to form a link aggregation group so that a MAC client can treat the link aggregation group as if it were a single link.                                                                                                                                                                                                  |
| <b>local MEP</b>                    | An MEP of a device on a network enabled with Ethernet CFM.                                                                                                                                                                                                                                                                                                                                      |
| <b>local area network (LAN)</b>     | A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building. It features high speed and low error rate. Ethernet, FDDI, and Token Ring are three technologies used to implement a LAN. Current LANs are generally based on switched Ethernet or Wi-Fi technology and running at 1,000 Mbit/s (that is, 1 Gbit/s).             |
| <b>logical interface</b>            | An interface that does not exist physically and comes into being through configuration. It can also exchange data.                                                                                                                                                                                                                                                                              |
| <b>loss of signal (LOS)</b>         | No transitions occurring in the received signal.                                                                                                                                                                                                                                                                                                                                                |

## M

|                    |                                                                 |
|--------------------|-----------------------------------------------------------------|
| <b>MA</b>          | maintenance association                                         |
| <b>MAC</b>         | See <a href="#">Media Access Control</a> .                      |
| <b>MAC address</b> | A link layer address or physical address. It is six bytes long. |
| <b>MCE</b>         | MAC control element                                             |
| <b>MD</b>          | See <a href="#">maintenance domain</a> .                        |
| <b>MD5</b>         | See <a href="#">message digest algorithm 5</a> .                |
| <b>MDC</b>         | message discrimination                                          |
| <b>ME</b>          | See <a href="#">managed element</a> .                           |
| <b>MEG</b>         | See <a href="#">maintenance entity group</a> .                  |
| <b>MEP</b>         | maintenance association end point                               |
| <b>MIB</b>         | See <a href="#">management information base</a> .               |
| <b>MIN</b>         | mobile identification number                                    |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MLD</b>                                                      | See <a href="#">multicast listener discovery</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>MLR</b>                                                      | media loss ratio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>MOS</b>                                                      | mean opinion score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>MPLS</b>                                                     | See <a href="#">Multiprotocol Label Switching</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>MPLS TE</b>                                                  | multiprotocol label switching traffic engineering                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>MPLS TP</b>                                                  | See <a href="#">Multiprotocol Label Switching traffic policing</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>MPLS VPN</b>                                                 | See <a href="#">multiprotocol label switching virtual private network</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>MPU</b>                                                      | main processing unit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>MSDP</b>                                                     | See <a href="#">Multicast Source Discovery Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>MSTP</b>                                                     | See <a href="#">Multiple Spanning Tree Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>MTU</b>                                                      | See <a href="#">maximum transmission unit</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Media Access Control (MAC)</b>                               | A protocol at the media access control sublayer. The protocol is at the lower part of the data link layer in the OSI model and is mainly responsible for controlling and connecting the physical media at the physical layer. When transmitting data, the MAC protocol checks whether to be able to transmit data. If the data can be transmitted, certain control information is added to the data, and then the data and the control information are transmitted in a specified format to the physical layer. When receiving data, the MAC protocol checks whether the information is correct and whether the data is transmitted correctly. If the information is correct and the data is transmitted correctly, the control information is removed from the data and then the data is transmitted to the LLC layer. |
| <b>Multicast Source Discovery Protocol (MSDP)</b>               | A protocol that is applicable only to the PIM-SM domain and meaningful only for the Any-Source Multicast (ASM) model. After the MSDP peer relationship is set up between RPs of different PIM-SM domains, multicast source information can be shared between PIM-SM domains, and the inter-domain multicast can be implemented. After the MSDP peer relationship is set up between RPs of the same PIM-SM domain, multicast source information can be shared in the PIM-SM domain, and anycast RP can be implemented.                                                                                                                                                                                                                                                                                                   |
| <b>Multiple Spanning Tree Protocol (MSTP)</b>                   | A protocol that can be used in a loop network. Using an algorithm, the MSTP blocks redundant paths so that the loop network can be trimmed as a tree network. In this case, the proliferation and endless cycling of packets is avoided in the loop network. The protocol that introduces the mapping between VLANs and multiple spanning trees. This solves the problem that data cannot be normally forwarded in a VLAN because in STP/RSTP, only one spanning tree corresponds to all the VLANs.                                                                                                                                                                                                                                                                                                                     |
| <b>Multiprotocol Label Switching (MPLS)</b>                     | A technology that uses short tags of fixed length to encapsulate packets in different link layers, and provides connection-oriented switching for the network layer on the basis of IP routing and control protocols. It improves the cost performance and expandability of networks, and is beneficial to routing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Multiprotocol Label Switching traffic policing (MPLS TP)</b> | It is a scheme that supervises the specific traffic entering the communication devices. By policing the speed of traffic that enters the network, it "punishes" the traffic out of the threshold, so the traffic going into network is limited to a reasonable range, protecting the network resources and the interests of the carriers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>mVRRP</b>                                                    | management Virtual Router Redundancy Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>maintenance domain</b>                                       | The network or the part of the network for which connectivity is managed by                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>(MD)</b>                                                             | connectivity fault management (CFM). The devices in a maintenance domain are managed by a single Internet service provider (ISP).                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>maintenance entity group (MEG)</b>                                   | <p>A MEG consists of MEs that meet the following criteria:</p> <ul style="list-style-type: none"><li>• Exist within the same management edges.</li><li>• Have the same MEG hierarchy.</li><li>• Belong to the same P2P or P2MP connection.</li></ul>                                                                                                                                                                                                                                                                            |
| <b>managed element (ME)</b>                                             | A particular entity or resource in a networked system environment. It can also represent a physical piece of equipment on the network, the components of the device on the network, or parts of the network itself.                                                                                                                                                                                                                                                                                                             |
| <b>management information base (MIB)</b>                                | A type of database used for managing the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.                                                                                                                                                                                                                                                                                                                 |
| <b>management rights</b>                                                | The rights enabling a user to manage the specified devices and boards or the group of a user to manage specified domains.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>maximum transmission unit (MTU)</b>                                  | The largest packet of data that can be transmitted on a network. MTU size varies, depending on the network—576 bytes on X.25 networks, for example, 1500 bytes on Ethernet, and 17,914 bytes on 16 Mbit/s token ring. Responsibility for determining the size of the MTU lies with the link layer of the network. When packets are transmitted across networks, the path MTU, or PMTU, represents the smallest packet size (the one that all networks can transmit without breaking up the packet) among the networks involved. |
| <b>message digest algorithm 5 (MD5)</b>                                 | A hash function that is used in a variety of security applications to check message integrity. MD5 processes a variable-length message into a fixed-length output of 128 bits. It breaks up an input message into 512-bit blocks (sixteen 32-bit little-endian integers). After a series of processing, the output consists of four 32-bit words, which are then cascaded into a 128-bit hash number.                                                                                                                           |
| <b>monitored object</b>                                                 | A physical or a logical network entity to be monitored. It defines what is monitored in integrated network monitoring. A monitored object can be a physical object or a logical object.                                                                                                                                                                                                                                                                                                                                         |
| <b>multi-hop</b>                                                        | In the IP network, one hop means that a packet arrives at the destination with a route forwarding. Single-hop means that a packet arrives at the destination with the route forwarding that occurs only once. Multi-hop means that a packet arrives at the destination with the route forwarding that occurs several times.                                                                                                                                                                                                     |
| <b>multicast</b>                                                        | A process of transmitting data packets from one source to many destinations. The destination address of the multicast packet uses Class D address, that is, the IP address ranges from 224.0.0.0 to 239.255.255.255. Each multicast address represents a multicast group rather than a host.                                                                                                                                                                                                                                    |
| <b>multicast listener discovery (MLD)</b>                               | A protocol used by an IPv6 router to discover the multicast listeners on their directly connected network segments, and to set up and maintain member relationships. On IPv6 networks, after MLD is configured on the receiver hosts and the multicast router to which the hosts are directly connected, the hosts can dynamically join related groups and the multicast router can manage members on the local network.                                                                                                        |
| <b>multiprotocol label switching virtual private network (MPLS VPN)</b> | An Internet Protocol (IP) virtual private network (VPN) based on the multiprotocol label switching (MPLS) technology. It applies the MPLS technology for network routers and switches, simplifies the routing mode of core routers, and combines traditional routing technology and label switching technology. It can be used to construct the broadband Intranet and Extranet to meet various service requirements.                                                                                                           |

**N**

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NAP</b>                               | network access point                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>NAS</b>                               | network access server                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>NDP</b>                               | See <a href="#">Neighbor Discovery Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                     |
| <b>NE</b>                                | network element                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>NIC</b>                               | network interface card                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>NM</b>                                | network management                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>NMC</b>                               | network management center                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>NP</b>                                | See <a href="#">network processor</a> .                                                                                                                                                                                                                                                                                                                                                                               |
| <b>NPE</b>                               | network provider edge                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>NQA</b>                               | network quality analysis                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>NSE</b>                               | nonlinear schrodinger equation                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>NTA</b>                               | See <a href="#">network traffic analyzer</a> .                                                                                                                                                                                                                                                                                                                                                                        |
| <b>NTC</b>                               | See <a href="#">network traffic collector</a> .                                                                                                                                                                                                                                                                                                                                                                       |
| <b>NVRAM</b>                             | nonvolatile random access memory                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Neighbor Discovery Protocol (NDP)</b> | A protocol that is used to discover the information of the neighboring Huawei device that is connected with the local device.                                                                                                                                                                                                                                                                                         |
| <b>NetFlow</b>                           | NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information. NetFlow has become an industry standard for network traffic monitoring and as a Bandwidth Monitor Tool. Netflow is supported by many platforms which include Cisco switches, Juniper switches, vSphere 5, Linux, FreeBSD, NetBSD and OpenBSD.                                                                         |
| <b>Netstream</b>                         | As a measurement and release technique based on network stream information, NetStream can categorize and measure the traffic on the network and the utilization of resources. It performs management and charging for various services and based on different QoS.                                                                                                                                                    |
| <b>network layer</b>                     | Layer 3 of the seven-layer OSI model of computer networking. The network layer provides routing and addressing so that two terminal systems are interconnected. In addition, the network layer provides congestion control and traffic control. In the TCP/IP protocol suite, the functions of the network layer are specified and implemented by IP protocols. Therefore, the network layer is also called IP layer. |
| <b>network processor (NP)</b>            | An integrated circuit which has a feature set specifically targeted at the networking application domain. Network Processors are typically software programmable devices and would have generic characteristics similar to general purpose CPUs that are commonly used in many different types of equipment and products.                                                                                             |
| <b>network traffic analyzer (NTA)</b>    | Network traffic analysis tool that obtains statistical data from the NTC (Network Traffic Collector). The statistical data is a basis for flow evidence, capacity planning, and attack detection.                                                                                                                                                                                                                     |
| <b>network traffic</b>                   | Application running in Unix or Windows, which is responsible for receiving and                                                                                                                                                                                                                                                                                                                                        |



|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>collector (NTC)</b>                        | processing UDP packets from the NTE (Network Traffic Exporter). Then it sends statistical data to the NTA for further analysis.                                                                                                                                                                                                                                                                                                             |
| <b>O</b>                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>OA</b>                                     | optical amplifier                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>OAM</b>                                    | See <a href="#">operation, administration and maintenance</a> .                                                                                                                                                                                                                                                                                                                                                                             |
| <b>OAMPDU</b>                                 | operation, administration and maintenance protocol data unit                                                                                                                                                                                                                                                                                                                                                                                |
| <b>OB</b>                                     | outside broadcast                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>OCS</b>                                    | See <a href="#">Online Charging System</a> .                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>ODR</b>                                    | origin dependent routing                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>OFC</b>                                    | optical fiber communication conference and exhibit                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>OID</b>                                    | object identifier                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>OLT</b>                                    | optical line terminal                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>OMC</b>                                    | See <a href="#">operation and maintenance center</a> .                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>ONLY</b>                                   | See <a href="#">One Number Link You</a> .                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>ONU</b>                                    | See <a href="#">optical network unit</a> .                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>OPM</b>                                    | optical performance monitor                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>OSPF</b>                                   | See <a href="#">Open Shortest Path First</a> .                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>OWD</b>                                    | one-way delay                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>One Number Link You (ONLY)</b>             | The function provided for enterprises by the mCentrex service that allows one extension number to map multiple terminal numbers. The terminals can ring in sequence or simultaneously.                                                                                                                                                                                                                                                      |
| <b>Online Charging System (OCS)</b>           | A system that implements the convergence of online charging and offline charging, voice service charging and data service charging, prepaid subscriber management and postpaid subscriber management. The OCS provides the functions such as rating, subscriber balance management, and real-time monitoring.                                                                                                                               |
| <b>Open Shortest Path First (OSPF)</b>        | A link-state, hierarchical interior gateway protocol (IGP) for network routing. Dijkstra's algorithm is used to calculate the shortest path tree. It uses cost as its routing metric. A link state database is constructed with the network topology which is identical on all routers in the area.                                                                                                                                         |
| <b>operation and maintenance center (OMC)</b> | An element within a network management system responsible for the operations and maintenance of a specific element or group of elements. For example an OMC-Radio may be responsible for the management of a radio subsystem where as an OMC-Switch may be responsible for the management of a switch or exchange. However, these will in turn be under the control of a NMC (Network Management Centre) which controls the entire network. |
| <b>operation log</b>                          | A list of information about operation events.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>operation, administration and</b>          | A group of network support functions that monitor and sustain segment operation, support activities that are concerned with, but not limited to, failure detection,                                                                                                                                                                                                                                                                         |

|                                   |                                                                                                                                                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>maintenance (OAM)</b>          | notification, location, and repairs that are intended to eliminate faults and keep a segment in an operational state, and support activities required to provide the services of a subscriber access network to users/subscribers. |
| <b>optical fiber</b>              | A thin filament of glass or other transparent material, through which a signal-encoded light beam may be transmitted using total internal reflection.                                                                              |
| <b>optical network unit (ONU)</b> | A form of Access Node that converts optical signals transmitted via fiber to electrical signals that can be transmitted via coaxial cable or twisted pair copper wiring to individual subscribers.                                 |
| <b>P</b>                          |                                                                                                                                                                                                                                    |
| <b>P2P</b>                        | See <a href="#">point-to-point service</a> .                                                                                                                                                                                       |
| <b>PAP</b>                        | See <a href="#">Password Authentication Protocol</a> .                                                                                                                                                                             |
| <b>PC</b>                         | personal computer                                                                                                                                                                                                                  |
| <b>PCB</b>                        | See <a href="#">printed circuit board</a> .                                                                                                                                                                                        |
| <b>PCI</b>                        | See <a href="#">peripheral component interconnect</a> .                                                                                                                                                                            |
| <b>PCS</b>                        | personal communications service                                                                                                                                                                                                    |
| <b>PD</b>                         | product daemon                                                                                                                                                                                                                     |
| <b>PDF</b>                        | See <a href="#">policy decision function</a> .                                                                                                                                                                                     |
| <b>PDSN</b>                       | See <a href="#">packet data serving node</a> .                                                                                                                                                                                     |
| <b>PDU</b>                        | protocol data unit                                                                                                                                                                                                                 |
| <b>PE</b>                         | See <a href="#">provider edge</a> .                                                                                                                                                                                                |
| <b>PHB</b>                        | See <a href="#">per-hop behavior</a> .                                                                                                                                                                                             |
| <b>PIC</b>                        | parallel interference cancellation                                                                                                                                                                                                 |
| <b>PIM</b>                        | Protocol Independent Multicast                                                                                                                                                                                                     |
| <b>PIM-SM</b>                     | Protocol Independent Multicast - Sparse Mode                                                                                                                                                                                       |
| <b>PLL</b>                        | See <a href="#">phase-locked loop</a> .                                                                                                                                                                                            |
| <b>PON</b>                        | passive optical network                                                                                                                                                                                                            |
| <b>POS</b>                        | See <a href="#">packet over SDH/SONET</a> .                                                                                                                                                                                        |
| <b>PPP</b>                        | Point-to-Point Protocol                                                                                                                                                                                                            |
| <b>PR</b>                         | See <a href="#">public relations</a> .                                                                                                                                                                                             |
| <b>PRI</b>                        | primary rate interface                                                                                                                                                                                                             |
| <b>PSN</b>                        | See <a href="#">packet switched network</a> .                                                                                                                                                                                      |
| <b>PSP</b>                        | principal state of polarization                                                                                                                                                                                                    |
| <b>PSU</b>                        | power supply unit                                                                                                                                                                                                                  |
| <b>PTN</b>                        | packet transport network                                                                                                                                                                                                           |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PTP</b>                                       | See <a href="#">point to point</a> .                                                                                                                                                                                                                                                                                                                                                             |
| <b>PTP clock</b>                                 | See <a href="#">Precision Time Protocol clock</a> .                                                                                                                                                                                                                                                                                                                                              |
| <b>PVC</b>                                       | See <a href="#">permanent virtual circuit</a> .                                                                                                                                                                                                                                                                                                                                                  |
| <b>PW</b>                                        | See <a href="#">pseudo wire</a> .                                                                                                                                                                                                                                                                                                                                                                |
| <b>PWE3</b>                                      | See <a href="#">pseudo wire emulation edge-to-edge</a> .                                                                                                                                                                                                                                                                                                                                         |
| <b>Password Authentication Protocol (PAP)</b>    | A method of verifying the identity of a user who attempts to log in to a PPP server. This protocol is adopted when a stricter authentication protocol, such as CHAP, cannot take effect, or the user name and password submitted by the user for authentication must be forwarded to other programs without being encrypted.                                                                     |
| <b>PoE</b>                                       | power over Ethernet                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Precision Time Protocol clock (PTP clock)</b> | A type of high-decision clock defined by the IEEE 1588 V2 standard. The IEEE 1588 V2 standard specifies the precision time protocol (PTP) in a measurement and control system. The PTP protocol ensures clock synchronization precise to sub-microseconds.                                                                                                                                       |
| <b>packet data serving node (PDSN)</b>           | A gateway used to connect the mobile network and the IP backbone network. It provides access to packet data service for mobile subscribers.                                                                                                                                                                                                                                                      |
| <b>packet forwarding</b>                         | An action performed by a router to forward a received datagram, where the destination IP address does not match the IP address of the router, to another router or destination host on the router list.                                                                                                                                                                                          |
| <b>packet loss</b>                               | The discarding of data packets in a network when a device is overloaded and cannot accept any incoming data at a given moment.                                                                                                                                                                                                                                                                   |
| <b>packet over SDH/SONET (POS)</b>               | A MAN and WAN technology that provides point-to-point data connections. The POS interface uses SDH/SONET as the physical layer protocol, and supports the transport of packet data (such as IP packets) in MAN and WAN.                                                                                                                                                                          |
| <b>packet per second (pps)</b>                   | Packet per second though the network card. Unit of data service bandwidth.                                                                                                                                                                                                                                                                                                                       |
| <b>packet switched network (PSN)</b>             | A telecommunications network that works in packet switching mode.                                                                                                                                                                                                                                                                                                                                |
| <b>partial route calculation (RPC)</b>           | A type of route calculation that is similar to that of PRC. Only the routes that change are calculated. Instead of calculating the node path, PRC updates the leaf routes according to the SPT calculated by I-SPF.                                                                                                                                                                              |
| <b>patch</b>                                     | An independent software unit used for fixing the bugs in software.                                                                                                                                                                                                                                                                                                                               |
| <b>per-hop behavior (PHB)</b>                    | IETF Diff-Serv workgroup defines forwarding behaviors of network nodes as per-hop behaviors (PHB), such as, traffic scheduling and policing. A device in the network should select the proper PHB behaviors, based on the value of DSCP. At present, the IETF defines four types of PHB. They are class selector (CS), expedited forwarding (EF), assured forwarding (AF), and best-effort (BE). |
| <b>peripheral component interconnect (PCI)</b>   | A standard designed for the bus connecting the computer main board to peripheral devices. The PCI1.0 standard was released by Intel in 1992 and related standards have been released by PCI-SIG since 1993. Peripheral component interconnect (PCI) delivers I/O functionality for computers ranging from servers to workstations, PCs, laptop PCs and mobile devices.                           |
| <b>permanent virtual circuit (PVC)</b>           | A circuit that can be established as an option to provide a dedicated circuit link between two facilities. PVC configuration is usually preconfigured by the service                                                                                                                                                                                                                             |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | provider. Unlike SVCs, PVCs are usually very seldom broken/disconnected. A permanent virtual circuit (PVC) is a virtual circuit established for repeated/continuous use between the same DTE. In a PVC, the long-term association is identical to the data transfer phase of a virtual call. Permanent virtual circuits eliminate the need for repeated call set-up and clearing.               |
| <b>phase-locked loop (PLL)</b>                   | A circuit that consists essentially of a phase detector which compares the frequency of a voltage-controlled oscillator with that of an incoming carrier signal or reference-frequency generator; the output of the phase detector, after passing through a loop filter, is fed back to the voltage-controlled oscillator to keep it exactly in phase with the incoming or reference frequency. |
| <b>physical link</b>                             | The link between two physical network elements (NEs). When the user creates NEs or refreshes the device status, the system automatically creates the physical link according to the topology structure information on the device. The remark information of a physical link can be modified, but the physical link cannot be deleted.                                                           |
| <b>physical view</b>                             | The default view that is used to display all devices and the topology partition (according to the area or the maintenance relation) in the network.                                                                                                                                                                                                                                             |
| <b>ping</b>                                      | A method used to test whether a device in the IP network is reachable according to the sent ICMP Echo messages and received response messages.                                                                                                                                                                                                                                                  |
| <b>point to point (PTP)</b>                      | A type of service in which data is sent from a single network termination to another network termination.                                                                                                                                                                                                                                                                                       |
| <b>point-to-point service (P2P)</b>              | A service between two terminal users. In P2P services, senders and recipients are terminal users.                                                                                                                                                                                                                                                                                               |
| <b>policy</b>                                    | A set of rules that are applied when the conditions for triggering an event are met.                                                                                                                                                                                                                                                                                                            |
| <b>policy decision function (PDF)</b>            | A functional entity used to set policies according to the sessions and related information obtained from the P-CSCF. The PDF is a policy decision point of the SBLP control.                                                                                                                                                                                                                    |
| <b>pool</b>                                      | A state in the life cycle of a subscriber. If a subscriber in the disabled state does not recharge before the end of the validity period, the subscriber enters the pool state. A subscriber in the pool state cannot perform any operations. The system deletes all information of the subscriber and reclaims the number after the pool period.                                               |
| <b>power module</b>                              | A module that provides power supply to other boards or modules.                                                                                                                                                                                                                                                                                                                                 |
| <b>pps</b>                                       | See <a href="#">packet per second</a> .                                                                                                                                                                                                                                                                                                                                                         |
| <b>printed circuit board (PCB)</b>               | A board used to mechanically support and electrically connect electronic components using conductive pathways, tracks, or traces, etched from copper sheets laminated onto a non-conductive substrate.                                                                                                                                                                                          |
| <b>provider edge (PE)</b>                        | A device that is located in the backbone network of the MPLS VPN structure. A PE is responsible for managing VPN users, establishing LSPs between PEs, and exchanging routing information between sites of the same VPN. A PE performs the mapping and forwarding of packets between the private network and the public channel. A PE can be a UPE, an SPE, or an NPE.                          |
| <b>pseudo wire (PW)</b>                          | An emulated connection between two PEs for transmitting frames. The PW is established and maintained by PEs through signaling protocols. The status information of a PW is maintained by the two end PEs of a PW.                                                                                                                                                                               |
| <b>pseudo wire emulation edge-to-edge (PWE3)</b> | An end-to-end Layer 2 transmission technology. It emulates the essential attributes of a telecommunication service such as ATM, FR or Ethernet in a packet switched network                                                                                                                                                                                                                     |

(PSN). PWE3 also emulates the essential attributes of low speed time division multiplexing (TDM) circuit and SONET/SDH. The simulation approximates to the real situation.

**public relations (PR)** Communication with various sectors of the public to influence their attitudes and opinions in the interest of promoting a person, product or idea.

## Q

**QoS** See [quality of service](#).

**quality of service (QoS)** A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

## R

**RADIUS** See [Remote Authentication Dial-In User Service](#).

**RADIUS authentication** An authentication mode in which the BRAS sends the user name and the password to the RADIUS server by using the RADIUS protocol. The RADIUS server authenticates the user, and then returns the result to the BRAS.

**RDI** remote defect indication

**RDS** See [replicated data set](#).

**RF** See [radio frequency](#).

**RIP** See [Routing Information Protocol](#).

**RMEP** remote maintenance association end point

**RMON** See [remote monitor](#).

**RP** routing performer

**RPC** See [partial route calculation](#).

**RPR** resilient packet ring

**RPT** rendezvous point tree

**RPU** See [resource process unit](#).

**RRPP** See [Rapid Ring Protection Protocol](#).

**RSSI** See [received signal strength indicator](#).

**RSVP** See [Resource Reservation Protocol](#).

**RSVP-TE** See [Resource ReserVation Protocol-Traffic Engineering](#).

**RTD** See [round-trip delay](#).

**RTN** radio transmission node

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RX</b>                                                          | receive                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Rapid Ring Protection Protocol (RRPP)</b>                       | An Ethernet ring-specific link layer protocol. It cannot only prevent data loop from causing broadcast storm efficiently when the Ethernet ring is complete, but also restore communication channels among nodes on the Ethernet ring rapidly when a link is torn down.                                                                                                                                                  |
| <b>Remote Authentication Dial-In User Service (RADIUS)</b>         | A security service that authenticates and authorizes dial-up users and is a centralized access control mechanism. RADIUS uses the User Datagram Protocol (UDP) as its transmission protocol to ensure real-time quality. RADIUS also supports the retransmission and multi-server mechanisms to ensure good reliability.                                                                                                 |
| <b>Resource Reservation Protocol-Traffic Engineering (RSVP-TE)</b> | An extension to the RSVP protocol for setting up label switched paths (LSPs) in MPLS networks. The RSVP-TE protocol is used to establish and maintain the LSPs by initiating label requests and allocating label binding messages. It also supports LSP rerouting and LSP bandwidth increasing.                                                                                                                          |
| <b>Resource Reservation Protocol (RSVP)</b>                        | A network control protocol like Internet Control Message Protocol (ICMP) and designed for Integrated Service and used to reserve resources on every node along a path. RSVP operates on the transport layer; however, RSVP does not transport application data.                                                                                                                                                          |
| <b>Routing Information Protocol (RIP)</b>                          | A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known to waste bandwidth.                                                                                                                   |
| <b>radio frequency (RF)</b>                                        | A type of electric current in the wireless network using AC antennas to create an electromagnetic field. It is the abbreviation of high-frequency AC electromagnetic wave. The AC with the frequency lower than 1 kHz is called low-frequency current. The AC with frequency higher than 10 kHz is called high-frequency current. RF can be classified into such high-frequency current.                                 |
| <b>received signal strength indicator (RSSI)</b>                   | The received wide band power, including thermal noise and noise generated in the receiver, within the bandwidth defined by the receiver pulse shaping filter, for TDD within a specified timeslot. The reference point for the measurement shall be the antenna                                                                                                                                                          |
| <b>remote alarm notification</b>                                   | A function with which the remote maintenance personnel are informed of alarms through Emails or short messages.                                                                                                                                                                                                                                                                                                          |
| <b>remote monitor (RMON)</b>                                       | A widely used network management standard defined by the IETF, and it enhances the MIB II standard greatly. It is mainly used to monitor the data traffic over a network segment or the entire network. RMON is completely based on the SNMP architecture, including the NMS and the Agent running on each network device.                                                                                               |
| <b>replicated data set (RDS)</b>                                   | VVR replicates data from a primary host, where the application is running, to one or more secondary hosts. A Replicated Volume Group (RVG) on the primary host and its counterparts on the secondary hosts make up a Replicated Data Set (RDS). An RDS is not a VolumeManager object but just a concept used in VVR. An RDS enables grouping of the RVG on the primary host and its counterparts on the secondary hosts. |
| <b>resource process unit (RPU)</b>                                 | A progress configured on the board where the resource manager subsystem (RMS) resides. It provides functions such as policy packaging, resource calculation, and preservation.                                                                                                                                                                                                                                           |
| <b>round-trip delay (RTD)</b>                                      | The time from first bit/byte of the Ranging-request in the downstream frame till the reception of the Ranging-transmission's last bit/byte. It is used for the calculation of the Equalization-Delay.                                                                                                                                                                                                                    |

**router ID** A unique identifier of a router in an AS, which is an integer of 32 bits.

## S

**SA** See [source active](#).

**SAS** serial attached SCSI

**SC** square connector

**SCC** synchronous common channel

**SDH** See [synchronous digital hierarchy](#).

**SDRAM** See [synchronous dynamic random access memory](#).

**SEC** security screening

**SEE** See [service execution environment](#).

**SF** sampling frequency

**SFTP** See [Secure File Transfer Protocol](#).

**SGIP** Short Message Gateway Interface Protocol

**SIG** See [security immunity gateway](#).

**SLA** See [service level agreement](#).

**SMS** short message service

**SMTP** See [Simple Mail Transfer Protocol](#).

**SNMP** See [Simple Network Management Protocol](#).

**SNP** special number presentation

**SP** See [service provider](#).

**SPE** See [superstratum provider edge](#).

**SPI** See [security parameter index](#).

**SPR** See [subscription profile repository](#).

**SPS** See [security policy server](#).

**SQ** See [subscriber queue](#).

**SQL** structured query language

**SRAM** See [static random access memory](#).

**SRC** sales retention cost

**SRU** SHDSL regenerator unit

**SSH** See [Secure Shell](#).

**SSL** See [Secure Sockets Layer](#).

**SSM** See [Synchronization Status Message](#).

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SSO</b>                                       | stateful switchover                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>STP</b>                                       | Spanning Tree Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>SVC</b>                                       | See <a href="#">switched virtual circuit</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Secure File Transfer Protocol (SFTP)</b>      | A network protocol designed to provide secure file transfer over SSH.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Secure Shell (SSH)</b>                        | A set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. A feature to protect information and provide powerful authentication function for a network when a user logs in to the network through an insecure network. It prevents IP addresses from being deceived and plain text passwords from being captured.                                                                                                                                                                                            |
| <b>Secure Sockets Layer (SSL)</b>                | A security protocol that works at a socket level. This layer exists between the TCP layer and the application layer to encrypt/decode data and authenticate concerned entities.                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Simple Mail Transfer Protocol (SMTP)</b>      | The TCP/IP protocol which facilitates the transfer of electronic-mail messages, specifies how two systems are to interact, and the format of messages used to control the transfer of electronic mail.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Simple Network Management Protocol (SNMP)</b> | A network management protocol of TCP/IP. It enables remote users to view and modify the management information of a network element. This protocol ensures the transmission of management information between any two points. The polling mechanism is adopted to provide basic function sets. According to SNMP, agents, which can be hardware as well as software, can monitor the activities of various devices on the network and report these activities to the network console workstation. Control information about each device is maintained by a management information block. |
| <b>Synchronization Status Message (SSM)</b>      | A message that carries quality levels of timing signals on a synchronous timing link. Nodes on an SDH network and a synchronization network acquire upstream clock information through this message. Then the nodes can perform proper operations on their clocks, such as tracing, switching, or converting to holdoff, and forward the synchronization information to downstream nodes.                                                                                                                                                                                                |
| <b>sFlow</b>                                     | See <a href="#">sampled flow</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>sampled flow (sFlow)</b>                      | sFlow is a technology for monitoring traffic in data networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent and a central sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring. sFlow Datagrams are used to immediately forward the sampled traffic statistics to an sFlow Collector for analysis.                                                                                                                                                                         |
| <b>security immunity gateway (SIG)</b>           | A gateway that checks the security status of the computer network by monitoring the source of the network worm virus, that is, the PCs. It prompts an unsecure PC to reinforce the system or kill the virus. It also isolates or restricts the computer already infected with the worm virus in network access according to the security access strategy.                                                                                                                                                                                                                                |
| <b>security parameter index (SPI)</b>            | A pointer that references the session key and algorithm used to protect the data being transported. The index is defined during the SA (Security Association) and described in the ESP (Encapsulating Security Payload) or AH (Authentication Header) extension to the IP header.                                                                                                                                                                                                                                                                                                        |
| <b>security policy server (SPS)</b>              | A user management and strategy control center in the scheme. It implements user management, security strategy management, security status evaluation, security                                                                                                                                                                                                                                                                                                                                                                                                                           |



|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | cooperation control, and security event audit. It is the core part of the EAD solution.                                                                                                                                                                                                                                                                                                                                         |
| <b>service data</b>                          | The user and/or network information required for the normal functioning of services.                                                                                                                                                                                                                                                                                                                                            |
| <b>service execution environment (SEE)</b>   | A platform that is developed over the enhanced network intelligent platform (ENIP) CORE. The open messaging enabler (OME) is the core of the SEE.                                                                                                                                                                                                                                                                               |
| <b>service level</b>                         | The level of service quality of an evaluated party in a specified period, determined by an evaluating party.                                                                                                                                                                                                                                                                                                                    |
| <b>service level agreement (SLA)</b>         | A service agreement between a customer and a service provider. SLA specifies the service level for a customer. The customer can be a user organization (source domain) or another differentiated services domain (upstream domain). An SLA may include traffic conditioning rules which constitute a traffic conditioning agreement as a whole or partially.                                                                    |
| <b>service provider (SP)</b>                 | An entity that offers service subscriptions to individual subscribers and contracts with carriers to implement services for a specific DN. A service provider may contract with more than one carrier.                                                                                                                                                                                                                          |
| <b>shortcut menu</b>                         | A menu that is displayed when right-clicking an object's name or icon. This is also referred to as a context menu.                                                                                                                                                                                                                                                                                                              |
| <b>source active (SA)</b>                    | A type of the MSDP message. An SA message contains multiple groups of (S,G) information or encapsulates a Register message. MSDP peers exchange (S,G) information to share the multicast source information.                                                                                                                                                                                                                    |
| <b>static random access memory (SRAM)</b>    | A type of random access memory. Its contents can be saved only if the SRAM is provided with the uninterrupted power supply. Unlike the DRAM, the SRAM does not need to be refreshed repeatedly.                                                                                                                                                                                                                                 |
| <b>station</b>                               | A terminal, such as a laptop or a PC, with a wireless network interface card (NIC).                                                                                                                                                                                                                                                                                                                                             |
| <b>subnet</b>                                | A type of smaller networks that form a larger network according to a rule, for example, according to different districts. This facilitates the management of the large network.                                                                                                                                                                                                                                                 |
| <b>subnet mask</b>                           | The technique used by the IP protocol to determine which network segment packets are destined for. The subnet mask is a binary pattern that is stored in the client machine, server or router matches with the IP address.                                                                                                                                                                                                      |
| <b>subscriber queue (SQ)</b>                 | A virtual queue. Each SQ maps eight types of FQ priority and can be configured with one to eight FQs. Idle queues cannot be used by other SQs. One to eight FQs share the total SQ bandwidth.                                                                                                                                                                                                                                   |
| <b>subscription profile repository (SPR)</b> | A data source that stores subscription profiles and provides interfaces for other network elements (NEs) to access the subscription data. For example, the policy and charging rules function (PCRF) can access the internal SPR (USCDB) over the DCI interface or access the external SPR over the LDAP or SOAP interface.                                                                                                     |
| <b>superstratum provider edge (SPE)</b>      | Core devices that are located within a VPLS full-meshed network. The UPE devices that are connected with the SPE devices are similar to the CE devices. The PWs set up between the UPE devices and the SPE devices serve as the ACs of the SPE devices. The SPE devices must learn the MAC addresses of all the sites on UPE side and those of the UPE interfaces that are connected with the SPE. SPE is sometimes called NPE. |
| <b>switched virtual circuit (SVC)</b>        | A logical connection between two nodes on a packet-switching network that is established only when data is to be transmitted.                                                                                                                                                                                                                                                                                                   |
| <b>synchronous digital hierarchy (SDH)</b>   | A transmission scheme that follows ITU-T G.707, G.708, and G.709. It defines the transmission features of digital signals such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and                                                                                                                                                                         |

B-ISDN. It interleaves the bytes of low-speed signals to multiplex the signals to high-speed counterparts, and the line coding of scrambling is used only for signals. SDH is suitable for the fiber communication system with high speed and a large capacity since it uses synchronous multiplexing and flexible mapping structure.

**synchronous dynamic random access memory (SDRAM)**

A new type of DRAM that can run at much higher clock speeds than conventional memory. SDRAM actually synchronizes itself with the CPU's bus and is capable of running at 100 MHz, about three times faster than conventional FPM RAM, and about twice as fast as EDO DRAM or BEDO DRAM. SDRAM is replacing EDO DRAM in computers.

**T****TC**

See [topology checksum](#).

**TCP**

See [Transmission Control Protocol](#).

**TCP/IP**

Transmission Control Protocol/Internet Protocol

**TE**

terminal equipment

**TFTP**

See [Trivial File Transfer Protocol](#).

**TLV**

See [type-length-value](#).

**TNS**

transit network selection

**TOP**

task oriented practice

**TTL**

See [time to live](#).

**TX**

transmit

**Telnet**

A standard terminal emulation protocol in the TCP/IP protocol stack. Telnet allows users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

**ToS**

type of service

**Transmission Control Protocol (TCP)**

The protocol within TCP/IP that governs the breakup of data messages into packets to be sent using Internet Protocol (IP), and the reassembly and verification of the complete messages from packets received by IP. A connection-oriented, reliable protocol (reliable in the sense of ensuring error-free delivery), TCP corresponds to the transport layer in the ISO/OSI reference model.

**Trivial File Transfer Protocol (TFTP)**

A small and simple alternative to FTP for transferring files. TFTP is intended for applications that do not need complex interactions between the client and server. TFTP restricts operations to simple file transfers and does not provide authentication. TFTP is small enough to be contained in ROM to be used for bootstrapping diskless machines.

**threshold**

An amount, limit or level on a scale. Changes will occur with a threshold reached.

**time to live (TTL)**

A technique used in best-effort delivery systems to prevent packets that loop endlessly. The TTL is set by the sender to the maximum time the packet is allowed to be in the network. Each router in the network decrements the TTL value when the packet arrives, and discards any packet if the TTL counter reaches zero.

**topology**

The configuration or layout of a network formed by the connections between devices on a local area network (LAN) or between two or more LANs.

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>topology checksum (TC)</b>       | Frames that are used to check whether the database of the neighboring station and the topology database of the local station are the same. This helps to check whether the RPR ring network topology is stable.                                                                                                                                                                                                                                               |
| <b>topology view</b>                | A basic component for the man-machine interface. The topology view directly displays the networking of a network as well as the alarm and communication status of each network element and subnet. The topology view reflects the basic running conditions of the network.                                                                                                                                                                                    |
| <b>traffic</b>                      | The product of the number of calls made and received and the average duration of each call in a measurement period.                                                                                                                                                                                                                                                                                                                                           |
| <b>transaction</b>                  | A business between a carrier and customer, such as payment and account adjustment.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>tunnel</b>                       | A channel on the packet switching network that transmits service traffic between PEs. In VPN, a tunnel is an information transmission channel between two entities. The tunnel ensures secure and transparent transmission of VPN information. In most cases, a tunnel is an MPLS tunnel.                                                                                                                                                                     |
| <b>tunnel ID</b>                    | A group of information, including the token, slot number of an outgoing interface, tunnel type, and location method.                                                                                                                                                                                                                                                                                                                                          |
| <b>tunnel iteration</b>             | A process in which a route is iterated to a tunnel.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>type-length-value (TLV)</b>      | An encoding type that features high efficiency and expansibility. It is also called Code-Length-Value (CLV). T indicates that different types can be defined through different values. L indicates the total length of the value field. V indicates the actual data of the TLV and is most important. TLV encoding features high expansibility. New TLVs can be added to support new features, which is flexible in describing information loaded in packets. |
| <b>U</b>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>UDP</b>                          | See <a href="#">User Datagram Protocol</a> .                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>UPE</b>                          | user-end provider edge                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>UPS</b>                          | uninterruptible power supply                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>URI</b>                          | See <a href="#">uniform resource identifier</a> .                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>URL</b>                          | uniform resource locator                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>URPF</b>                         | See <a href="#">unicast reverse path forwarding</a> .                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>USAU</b>                         | See <a href="#">universal signaling access unit</a> .                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>USB</b>                          | See <a href="#">Universal Serial Bus</a> .                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>UTC</b>                          | See <a href="#">Coordinated Universal Time</a> .                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Universal Serial Bus (USB)</b>   | A serial bus standard to interface devices. It was designed for computers such as PCs and the Apple Macintosh, but its popularity has prompted it to also become commonplace on video game consoles and PDAs.                                                                                                                                                                                                                                                 |
| <b>User Datagram Protocol (UDP)</b> | A TCP/IP standard protocol that allows an application program on one device to send a datagram to an application program on another. User Datagram Protocol (UDP) uses IP to deliver datagram. UDP provides application programs with the unreliable connectionless packet delivery service. There is a possibility that UDP messages will                                                                                                                    |

|                                               |                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | be lost, duplicated, delayed, or delivered out of order. The destination device does not confirm whether a data packet is received.                                                                                                                                                                                    |
| <b>unicast reverse path forwarding (URPF)</b> | A feature that helps to prevent network attacks based on spoofed IP source addresses.                                                                                                                                                                                                                                  |
| <b>uniform resource identifier (URI)</b>      | A string of characters for identifying an abstract or physical resource.                                                                                                                                                                                                                                               |
| <b>universal signaling access unit (USAU)</b> | As a signaling access unit of telecom devices in the intelligent network (IN), the USAU converts the signaling protocols between telecom devices, and supports TDM-based narrowband No.7 signaling network and IP-based broadband SIGTRAN network.                                                                     |
| <b>upstream</b>                               | In an access network, the direction that is far from the subscriber end of the link.                                                                                                                                                                                                                                   |
| <b>upstream interface</b>                     | The interface through which the local router receives multicast data. The router or the multicast source that forwards multicast data to the local router is called the upstream router or upstream multicast source. The network segment where the upstream interface resides is called the upstream network segment. |
| <b>V</b>                                      |                                                                                                                                                                                                                                                                                                                        |
| <b>VA</b>                                     | value assurance                                                                                                                                                                                                                                                                                                        |
| <b>VAP</b>                                    | virtual access point                                                                                                                                                                                                                                                                                                   |
| <b>VB</b>                                     | virtual bridge                                                                                                                                                                                                                                                                                                         |
| <b>VC</b>                                     | virtual concatenation                                                                                                                                                                                                                                                                                                  |
| <b>VCS</b>                                    | Veritas Cluster Server                                                                                                                                                                                                                                                                                                 |
| <b>VGMP</b>                                   | VRRP Group Management Protocol                                                                                                                                                                                                                                                                                         |
| <b>VLAN</b>                                   | virtual local area network                                                                                                                                                                                                                                                                                             |
| <b>VLANIF interface</b>                       | A type of Layer 3 VLAN interface. A VLANIF interface uniquely corresponds to one VLAN ID. IP addresses can be configured on VLANIF interfaces for the Layer 3 communication among VLANs.                                                                                                                               |
| <b>VLL</b>                                    | virtual leased line                                                                                                                                                                                                                                                                                                    |
| <b>VP</b>                                     | See <a href="#">virtual path</a> .                                                                                                                                                                                                                                                                                     |
| <b>VPLS</b>                                   | See <a href="#">virtual private LAN service</a> .                                                                                                                                                                                                                                                                      |
| <b>VPN</b>                                    | virtual private network                                                                                                                                                                                                                                                                                                |
| <b>VPN instance</b>                           | An entity that is set up and maintained by PEs for directly-connected sites. Each site has its VPN instance on a PE. A VPN instance is also called the VPN Routing and Forwarding (VRF) table. A PE has multiple forwarding tables, including a public-network routing table and one or multiple VRFs.                 |
| <b>VRF</b>                                    | VPN routing and forwarding                                                                                                                                                                                                                                                                                             |
| <b>VRP</b>                                    | See <a href="#">Versatile Routing Platform</a> .                                                                                                                                                                                                                                                                       |
| <b>VRRP</b>                                   | See <a href="#">Virtual Router Redundancy Protocol</a> .                                                                                                                                                                                                                                                               |
| <b>VSI</b>                                    | See <a href="#">virtual switch instance</a> .                                                                                                                                                                                                                                                                          |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VTY</b>                                       | See <a href="#">virtual type terminal</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Versatile Routing Platform (VRP)</b>          | A fruit of Huawei's many years of research and application experience in the field of network. VRP is a network OS incorporating Huawei's proprietary intellectual properties and capable of supporting various network systems of Huawei. It features a powerful IP forwarding engine as its core, and a perfect integration of real time OS technology, equipment and network management technology and various network application technologies through an advanced architectural design. As a scalable platform capable of sustained evolution with open interfaces, it supports a large number of protocols and features with great flexibility. With this platform, you can build an end-end, secure network of high efficiency, great intelligence, and easy manageability. Huawei has obtained a lot of experience in network running through the massive application of its network products and gained sufficient knowledge of various customer requirements. Such experience and knowledge serve as the basis for the design of the VRP so that the platform can adapt to most of the application environments through its support of diverse protocols and features. |
| <b>Virtual Router Redundancy Protocol (VRRP)</b> | A protocol used for multicast or multicast LANs such as an Ethernet. A group of routers (including an active router and several backup routers) in a LAN is regarded as a virtual router, which is called a backup group. The virtual router has its own IP address. The host in the network communicates with other networks through this virtual router. If the active router in the backup group fails, one of the backup routers in this backup group becomes active and provides routing service for the host in the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>VoIP</b>                                      | See <a href="#">voice over IP</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>virtual NE</b>                                | An object similar to a common NE and is also displayed with an icon on a view. A virtual NE, however, is only an NE simulated according to the practical situation, which does not represent an actual NE. Therefore, the actual status of this NE cannot be queried and its alarm status cannot be displayed with colors. Usually, a virtual NE provides the trail management function for the NEs or subnetworks that the NMS cannot manage, or provides the end-to-end service configuration method and the trail management capability when the equipment is interconnected with third-party NEs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>virtual link</b>                              | The logical connection between topological objects in the NMS topology view.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>virtual path (VP)</b>                         | A bundle of virtual channels, all of which are switched transparently across an ATM network based on a common VPI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>virtual private LAN service (VPLS)</b>        | A type of point-to-multipoint L2VPN service provided over the public network. VPLS enables geographically isolated user sites to communicate with each other through the MAN/WAN as if they are on the same LAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>virtual switch instance (VSI)</b>             | An instance through which the physical access links of VPLS can be mapped to the virtual links. Each VSI provides independent VPLS service. VSI has Ethernet bridge function and can terminate PW.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>virtual system</b>                            | A system that is identified by an additional system ID and used to generate extended LSP fragments. These fragments carry the additional system IDs in their LSP IDs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>virtual type terminal (VTY)</b>               | A logical terminal line that is used to access the device through Telnet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>voice over IP (VoIP)</b>                      | An IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in a digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public switched telephone network (PSTN).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## W

|                                           |                                                                                                                                                                                                                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN</b>                                | See <a href="#">wide area network</a> .                                                                                                                                                                                                                       |
| <b>WAPI</b>                               | WLAN Authentication and Privacy Infrastructure                                                                                                                                                                                                                |
| <b>WEP</b>                                | wired equivalent privacy                                                                                                                                                                                                                                      |
| <b>WLAN</b>                               | See <a href="#">wireless local area network</a> .                                                                                                                                                                                                             |
| <b>WTR</b>                                | See <a href="#">wait to restore</a> .                                                                                                                                                                                                                         |
| <b>wait to restore (WTR)</b>              | The number of minutes to wait before services are switched back to the working line.                                                                                                                                                                          |
| <b>wide area network (WAN)</b>            | A network composed of computers which are far away from each other which are physically connected through specific protocols. WAN covers a broad area, such as a province, a state or even a country.                                                         |
| <b>wireless local area network (WLAN)</b> | A hybrid of the computer network and the wireless communication technology. It uses wireless multiple address channels as transmission media and carries out data interaction through electromagnetic wave to implement the functions of the traditional LAN. |

## X

|             |                                               |
|-------------|-----------------------------------------------|
| <b>XAUI</b> | 10 gigabit Ethernet Attachment Unit Interface |
|-------------|-----------------------------------------------|