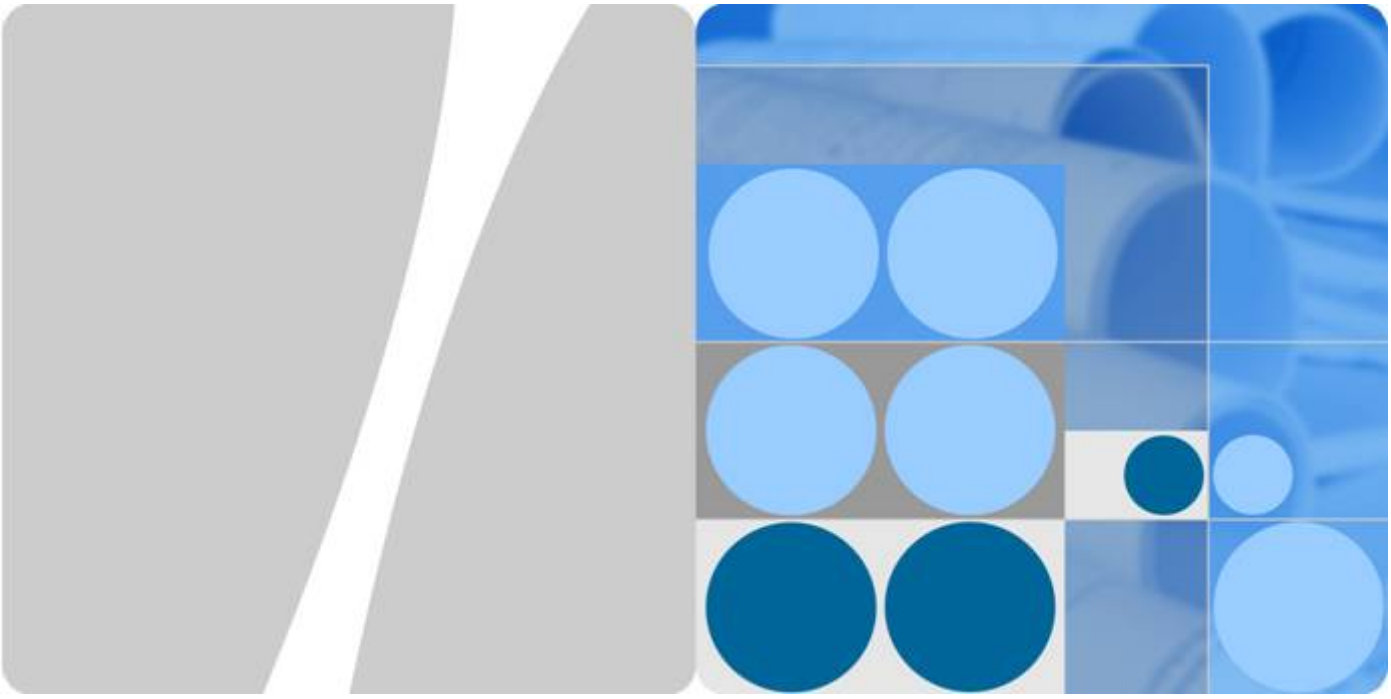


Huawei eSight

V200R002C00

Operation Guide

Issue 02

Date 2012-03-15

HUAWEI TECHNOLOGIES CO., LTD.

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 the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

Copyright © Huawei Technologies Co., Ltd.

Contents

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

1 Getting Started

About This Chapter

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

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.

Copyright © Huawei Technologies Co., Ltd.

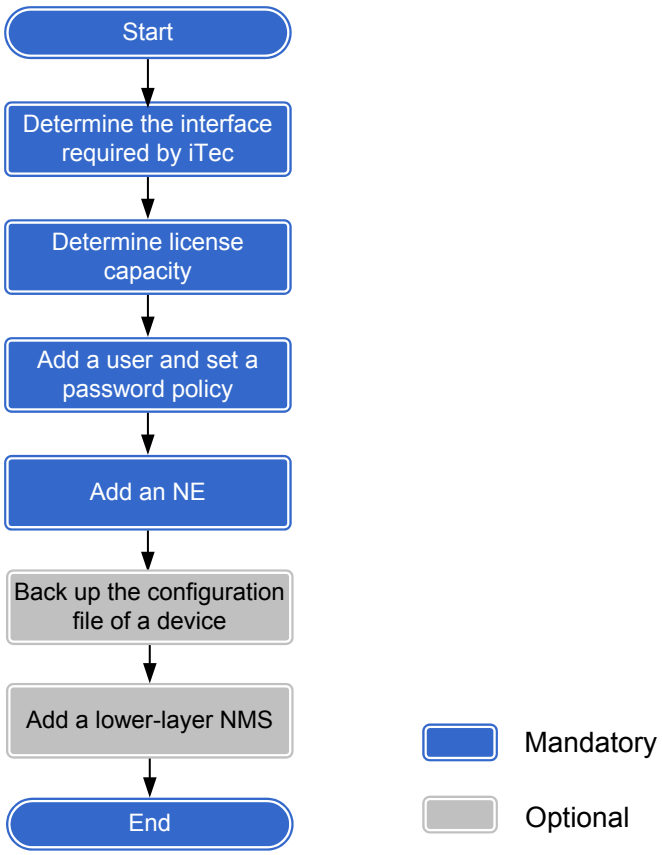
1.1 Commissioning

1.1.1 Commissioning Process

This topic verifies eSight basic functions.

Figure 1-1 shows the commissioning process.

Figure 1-1 Commissioning process



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.

Copyright © Huawei Technologies Co., Ltd.

Operation	Remarks
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.
5. (Optional) **1.1.9 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.
6. (Optional) **1.1.10 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.

Copyright © Huawei Technologies Co., Ltd.

The eSight service ports are listed as follows:

- **Ports Between the Server and an NE (Server Side)**
- **Ports Between the Server and Client (Server Side)**
- **Ports Between the Server and OSS (Server Side)**
- **Ports Between the Server and OSS (OSS Side)**
- **Ports Between Server Processes**
- **Other Ports**

1.1.2.2 Ports Between the eSight Server and NEs

This topic describes ports between the eSight server and NEs.

When a firewall is deployed between the eSight server and NEs, you must enable the required ports on the eSight server.

Table 1-1 lists the ports to be enabled on the eSight server so that NEs can penetrate the firewall and connect to the eSight server.

Table 1-1 Ports for connecting the eSight server to NEs

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
eSight server	A random port number greater than 1024	TCP	NE	23	Telnet port number for configuring NE services.	Yes
eSight server	A random port number greater than 1024	UDP	NE	161	Port number used by NEs to receive SNMP requests in NE service configuration.	Yes
NE	A random port number greater than 1024	TCP	eSight server	21	Port number used by the FTP server to transfer files.	Yes

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
NE	A random port number greater than 1024	SNMP	eSight server	162	Port number used by eSight to receive alarm traps from managed devices.	Yes
NE	A random port number greater than 1024	SNMP	eSight server	10162	Port number used by eSight to receive alarm traps from managed devices.	No
NE	A random port number greater than 1024	TCP	eSight server	39008	Port number used by the Mediation SOAP adapter.	No
NE	A random port number greater than 1024	TCP	eSight server	31022	Port number used by the SFTP server to transfer files.	Yes
NE	A random port number greater than 1024	TCP	eSight server	31023	Port number used by the FTP server to transfer files.	Yes

1.1.2.3 Ports Between the eSight Server and Web Browsers

This topic describes ports between the eSight server and web browsers.

Copyright © Huawei Technologies Co., Ltd.

When a firewall is deployed between the eSight server and web browsers, you must enable the required ports on the eSight server so that web browsers can connect to ports listed in **Table 1-2**.

Table 1-2 Ports for connecting web browsers to the eSight server

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
Web browser (eSight)	A random port number greater than 1024	HTTP	eSight server	8080	Port number used by the eSight web service.	Yes
Web browser (eSight)	A random port number greater than 1024	HTTPS	eSight server	8443	Security port for logging in to eSight.	Yes
Web browser (eSight)	A random port number greater than 1024	HTTPS	eSight server	8445	Security port for logging in to Maintenance Tools.	Yes
Web browser (eSight)	A random port number greater than 1024	HTTP	eSight server	8888	HTTP port used by the graphical command-line interface to configure NEs in batches and manage NEs.	Yes
Web browser (eSight)	A random port number greater than 1024	HTTP	eSight server	8889	Port number used by the Maintenance Tools web service.	Yes

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
Web browser (eSight)	A random port number greater than 1024	HTTP	eSight server	38080	Port number for accessing the online help and Fault Collection Tool and downloading reports.	Yes
Web browser (eSight)	A random port number greater than 1024	HTTPS	eSight server	38443	Port number for accessing the online help.	Yes

1.1.2.4 Ports Between the eSight Server and an OSS

This topic describes ports between the eSight server and an operations support system (OSS).

When a firewall is deployed between the eSight server and an OSS, you must enable required ports so that the OSS can penetrate the firewall and connect to the ports listed in **Table 1-3**.

Table 1-3 Ports to be enabled on the eSight server to connect to an OSS

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
eSight server	6666	UDP	OSS	A random port number	Port number for sending traps to an OSS.	Yes

eSight**Table 1-4** lists the ports to be enabled in an OSS to connect to the eSight server.

Copyright © Huawei Technologies Co., Ltd.

Table 1-4 eSightPorts to be enabled in an OSS to connect to the eSight server

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
OSS	A random port number greater than 1024	TCP	eSight server	21	FTP port used by eSight to transfer files to an OSS.	Yes
OSS	A random port number greater than 1024	UDP	eSight server	4700	Port number used by eSight to receive SNMP commands from an OSS.	Yes

1.1.2.5 Ports Between eSight Server Internal Processes

This topic describes ports between eSight server internal processes.

Ports between eSight server internal processes are used for communication only between eSightserver internal processes. You can use the port scanning tool to view these ports.

Table 1-5 lists the ports between eSight server internal processes.

Table 1-5 eSightPorts between eSight server internal processes

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Destination Port on the Firewall
eSight server	A random port number greater than 1024	TCP	eSight server	30999	Virgo shell port.	No

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Destination Port on the Firewall
eSight server	A random port number greater than 1024	TCP	eSight server	31000	OSGI debugging port.	No
eSight server	A random port number greater than 1024	TCP	eSight server	31003	Port number for managing SSO Server access security.	No
eSight server	A random port number greater than 1024	TCP	eSight server	31004	JSON bus port.	No
eSight server	A random port number greater than 1024	TCP	eSight server	31005	Hession bus port.	No
eSight server	31007	TCP	eSight Med Center	31006	Port number for connecting Med Node and Med Center.	No
eSight server	31009, 31011	TCP	eSight server	31010, 31012	Socket port used for license.	No
eSight server	10001, 10003	TCP	eSight server	10002, 10004	Socket port used for license.	No
eSight server	A random port number greater than 1024	TCP	eSight server	32403	OMS status monitoring port.	No

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Destination Port on the Firewall
eSight server	A random port number	TCP	eSight server	33306	Port number used by the MySQL process to connect to the MySQL database.	Yes
eSight server	A random port number greater than 1024	TCP	eSight server	38085	Port number for stopping the HedEx web service.	No
eSight server	A random port number greater than 1024	TCP	eSight server	40000	JMX port.	No
eSight server	5656	TCP	eSight server	5656	Socket port used for communication by eSight and the smart configuration tool.	Yes
eSight server	A random port number greater than 1024	TCP	eSight server	8081	Web service port number for communication between Maintenance Tools and the eSight server.	Yes
eSight server	A random port number greater than 1024	TCP	eSight server	8444	Port number for logging in to Maintenance Tools.	Yes

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Destination Port on the Firewall
eSight server	A random port number greater than 1024	TCP	eSight server	32001	OSGI debugging port number for communication between Maintenance Tools and the eSight server.	No
eSight server	A random port number greater than 1024	TCP	eSight server	32006	OMS status monitoring port for communication between Maintenance Tools and the eSight server.	No
eSight server	A random port number greater than 1024	TCP	eSight server	40001	JMX port number for communication between Maintenance Tools and the eSight server.	No
eSight server	A random port number greater than 1024	TCP	eSight server	32004	OSGI debugging port used by Maintenance Tools.	No
eSight server	A random port number greater than 1024	TCP	eSight server	32008	Port number used by Maintenance Tools to monitor OMS status.	No
eSight server	A random port number greater than 1024	TCP	eSight server	33336	JSON bus port used by Maintenance Tools.	No

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Destination Port on the Firewall
eSight server	A random port number greater than 1024	TCP	eSight server	33337	Hession bus port used by Maintenance Tools.	No
eSight server	A random port number greater than 1024	TCP	eSight server	40002	JMX port used by Maintenance Tools.	No

1.1.2.6 Ports Between the eSight Server and Other Applications

This topic describes ports between the eSight server and other applications.

Table 1-6 lists the ports between the eSight server and other applications.

Table 1-6 Ports between the eSight server and other applications

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
eSight server	A random port number greater than 1024	TCP	Email server	25	Simple Mail Transfer Protocol (SMTP) port.	Yes

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol	Destination End	Destination Port	Port Description	Enable the Port on the Firewall of the Destination End
eSight server	A random port number greater than 1024	TCP	Short message service gateway (SMSGW)	5018	SMPP 3.3/3.4 port. SMPP refers to Short Message Peer to Peer.	Yes
eSight server	A random port number greater than 1024	TCP	Short message service center (SMSC)	5090	SMPP 3.3/3.4 port.	Yes
eSight server	A random port number greater than 1024	TCP	SMSGW	7890	CMPP 2.0/2.1 port. CMPP refers to China Mobile Peer to Peer Protocol.	Yes
eSight server	A random port number greater than 1024	TCP	SMSGW	7891	CMPP 3.0 port.	Yes
eSight server	A random port number greater than 1024	TCP	SMSGW	8801	SGIP 1.2 port. SGIP refers to Short Message Gateway Interface Protocol.	Yes

1.1.3 Determining License Capacity

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

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

You have imported a license file into eSight.

Context

Table 1-7 describes the license information.

Table 1-7 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	Fault management
	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

Copyright © Huawei Technologies Co., Ltd.

1.1.4 Runtime Environment Requirements

This topic describes the runtime environment requirements. To help you better operate the eSight, the following runtime environment requirements must be met.

Table 1-8 lists the runtime environment requirements of the eSight.

Table 1-8 Runtime environment requirements

Configuration Item	Minimum Configuration Requirements
Hardware configuration requirements	Inter(R) Pentium(R) Dual CPU E2180 @ 2.00GHz, 2 GB
Operating system	Windows 7, Windows 2008 or Suse 11
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: 1. Open Windows Internet Explorer 8.0, and choose **Tools** > **Compatibility View Settings** from the main menu. 2. In the **Compatibility View Settings** dialog box, deselect **Display intranet sites in Compatibility** and **Display all websites in Compatibility View**. ● By default, Windows Server 2008 provides a high level of security policy. Therefore, if your client runs Windows Server 2008, you can log in to the eSight only on this client in Windows Internet Explorer 8.0. To modify the security policy, contact the operating system administrator.
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.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

- After the first successful login, you need to change the password to ensure the eSight security.
- 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*/, and press **Enter**.

For example, http://12.10.10.1:8086/. The eSight login page is displayed.

NOTE

- The default port number of the eSight is **8086**.
- 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 **13.5.3 Importing a License File** and **13.5.2 Obtaining an ESN** respectively.

Step 2 Enter the **User name** and **Password**.

Step 3 Click **Login**.

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 supported by the current eSight edition, the eSight displays a message indicating that you cannot log in. In this case, contact the system administrator.

----End

Logging Out of the eSight

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

Log out of the eSight.

----End

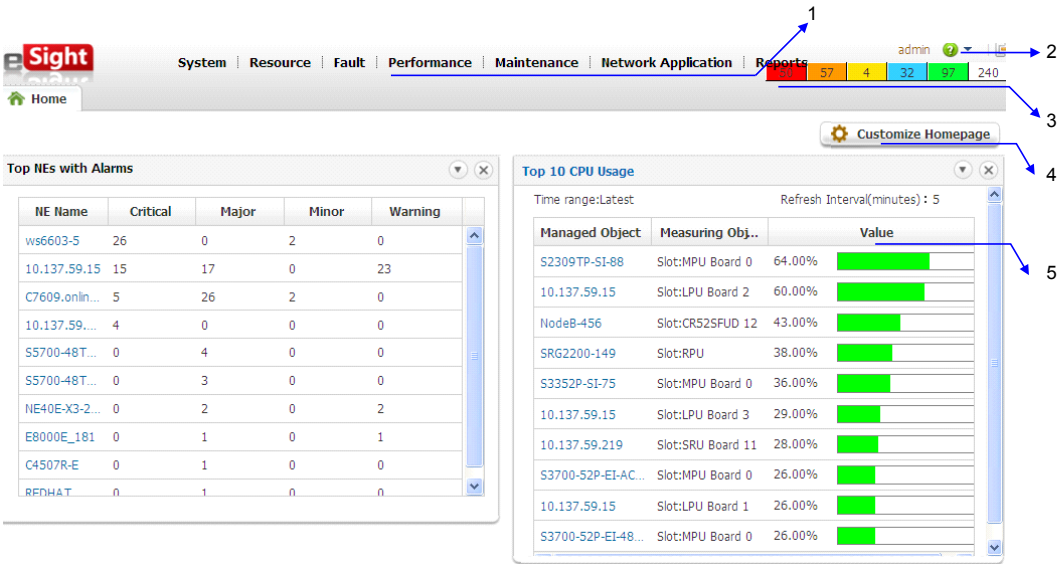
1.1.6 Main Page

This topic describes eSight main page.

Figure 1-2 shows eSight main page.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 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 a user. 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.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- 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

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.

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

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

Step 4 On the **Create User** page, set the basic information.

1. In the **Basic Info** step, set **User name**, **Password**, **Confirm password**, and **Description**, and set **Account status** to **Enabled**.
2. Click **Next**.

Step 5 On the **Create User** page, set a role for the user. The user has the management rights and operation rights of the role.

1. In the **Roles** step, select the role.

   NOTE

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

Step 6 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.

1. In the **Access Control Policies** step, select a login time control policy and an IP address range.

   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**.
2. Click **Finish**.

----End

Follow-up Procedure

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

Copyright © Huawei Technologies Co., Ltd.

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 Role** page, view the details of the user.
Modify user information	You can modify user information as required. 1. Click  in the **Operation** column where the required user information is located, and then modify it. 2. On the **Modify User** page, modify the settings of **Basic Info**, **Roles**, and **Access Control Policies**. For details about how to change the value of **Basic Info**, see **Step 4**; for details about how to change the value of **Roles**, see **Step 5**; for details about how to change the value of **Control Policies**, see **Step 6**. 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 **Reset Password** dialog box, set **Reset 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.

Copyright © Huawei Technologies Co., Ltd.

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

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**.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 In the **Resource Management** window, select the parent object for the NE to be added, and then click **Create Resource**.

Step 3 On the **Select Object Type** page, select an NE type under **Physical Devices**.

Step 4 On the **Configure Parameters** page, set the basic information and SNMP protocol for the NE.

NOTE

If you configure simple network management protocol (SNMP) parameters for an NE, click **Save Protocol Template** to save the settings as an SNMP parameter configuration template. If you need to configure SNMP parameters again, click **Select Protocol Template** to select the saved protocol template to apply.

Step 5 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

Follow-up Procedure

The following table describes the operations that you can perform after you manually create an NE in the eSight.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. Click the name of the required NE. The eSight displays all information about the NE.
Modify NE information	In the eSight, you can modify the name of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the configuration parameters of the NE. 3. Then click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. ● To delete an NE, click  in the **Operation** column where the NE is located. ● To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

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 side change, you must set the NE SNMP parameters concurrently on the eSight side.

Prerequisites

An NE 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 Choose **Resource** > **Equipment Resources** from the main menu.

Step 2 Select one or more NEs and click **Set SNMP Parameters**.

Step 3 In the displayed **Set SNMP Parameters** 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.

Copyright © Huawei Technologies Co., Ltd.

- **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 interva(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 **OK**.

----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 side change, you must set the NE Telnet parameters concurrently on eSight.

Prerequisites

An NE is added to eSight.

Procedure

Step 1 Choose **Resource** > **Equipment Resources** from the main menu.

Step 2 Select one or more NEs and click **Set Telnet Parameters**.

Step 3 In the displayed **Set Telnet Parameters** window, set the Telnet parameters.

Step 4 Click **OK**.

----End

1.1.9 Back Up Device Configuration Files

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

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

eSight communicates with NEs normally.

The FTP service is configured and started. For details on how to configure the FTP service, see **11.2 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**.

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

1.1.10 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.

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

Step 3 Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

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 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 1-9 describes the basic concepts about security management.

Table 1-9 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. Roles possess application-level operation rights related to system management, fault management, and performance management. Managing user rights based on roles makes rights management more effective. The default super administrator role, **Administrators**, has the operation rights of all managed domains.
Managed domain	A managed domain is a group of managed objects. Users can perform operations on the NEs in a managed domain only when they have the operation rights of the managed domain.
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. That is, if a user is granted with resource management permission, the user has permission to perform operations on the NEs within 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.

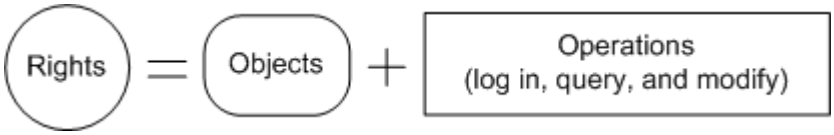
Copyright © Huawei Technologies Co., Ltd.

Rights

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

Figure 1-3 shows the rights elements: objects and operations.

Figure 1-3 Rights elements



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

Figure 1-4 shows the operations that can be performed on the eSight.

Figure 1-4 Operations that can be performed on the eSight

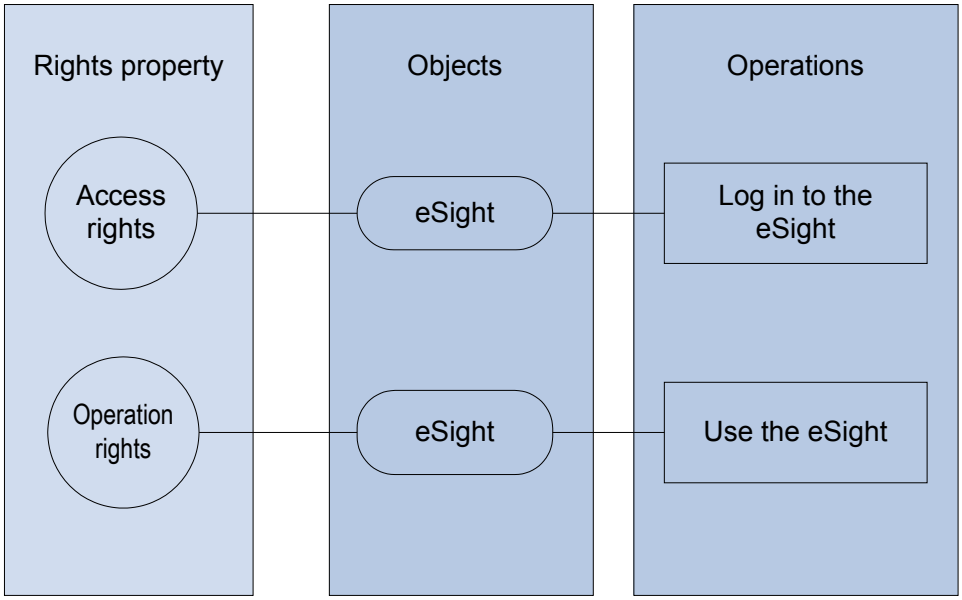


Table 1-10 describes the rights of the eSight users.

Table 1-10 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.

Copyright © Huawei Technologies Co., Ltd.

Rights	Operation	Description
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 topology objects. Before performing operations, users must log in to the eSight.

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.

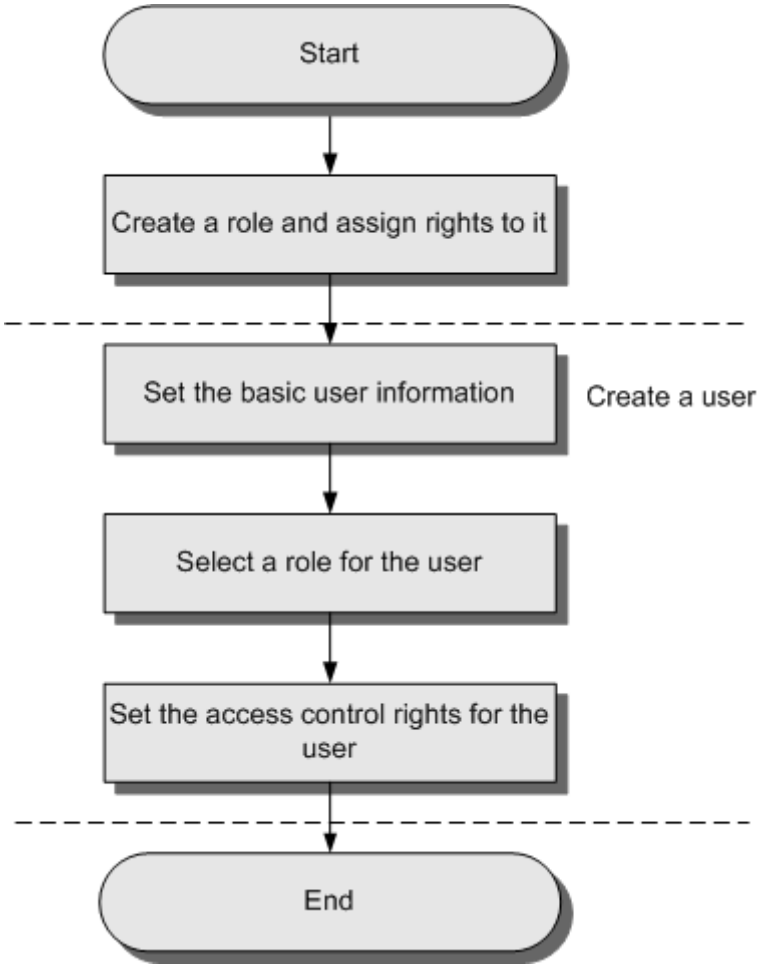
After some operations and objects are allocated to a role, the role has the rights of the operations on the objects. If a user is added to the role, the user has the rights of the role. The eSight provides two authorization modes: select roles while creating users and select users while creating rules.

- 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 1-5** shows the process of selecting roles while creating users.

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

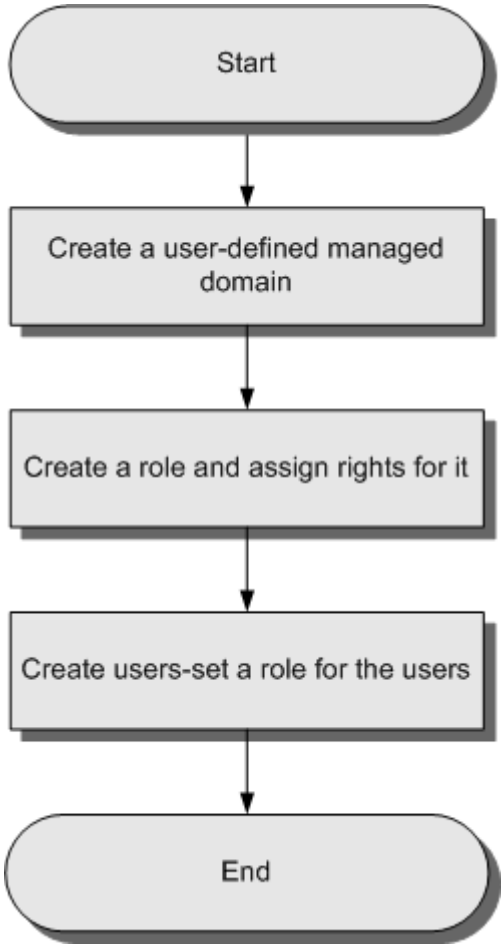
Figure 1-5 Common authorization process



In the process shown in **Figure 1-5**, 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 1-6** shows the authorization process by creating managed domains.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-6 Complete authorization process

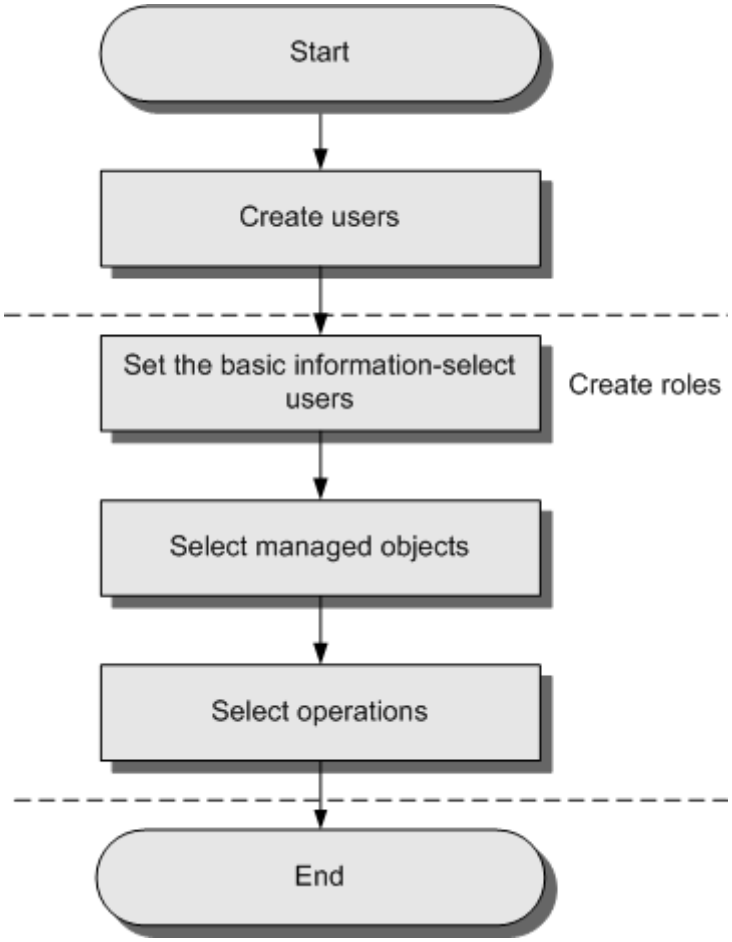


- Select users while creating roles.

  Users are already created. If you select users when creating roles, the selected users have the rights of the roles after successfully creation. **Figure 1-7** shows the process of selecting users while creating roles.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-7 Process



1.2.2 Basic Concepts About 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 1-11** describes the basic concepts about topology management.

Table 1-11 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.

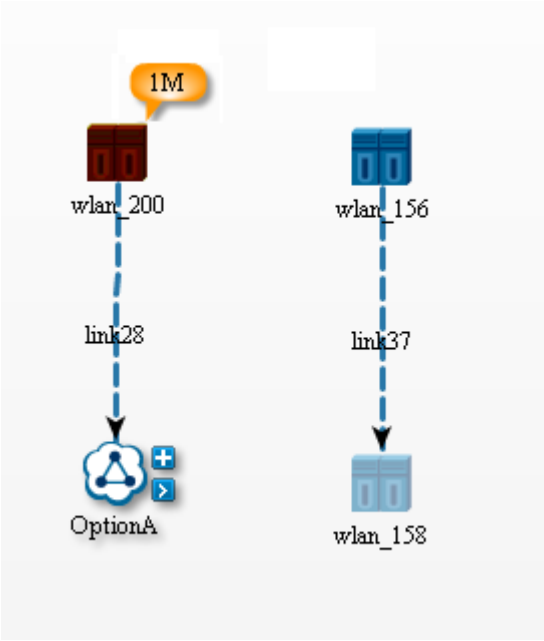
Copyright © Huawei Technologies Co., Ltd.

Concept	Description
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.

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 1-8** shows a physical view.

Figure 1-8 Physical View



Copyright © Huawei Technologies Co., Ltd.

Table 1-12 describes the topology object icons.

Table 1-12 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 1-13 describes the pop-up icons.

Table 1-13 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.

1.2.3 Basic Concepts of Resource

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 1-14 describes the basic concepts about resource management.

Table 1-14 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.

Copyright © Huawei Technologies Co., Ltd.

1.2.4 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 1-15**. You can take different measures for different severities of alarms.

Table 1-15 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 1-16** describes the four alarm status.

  Table 1-16 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 1-17 describes the alarm status change description.

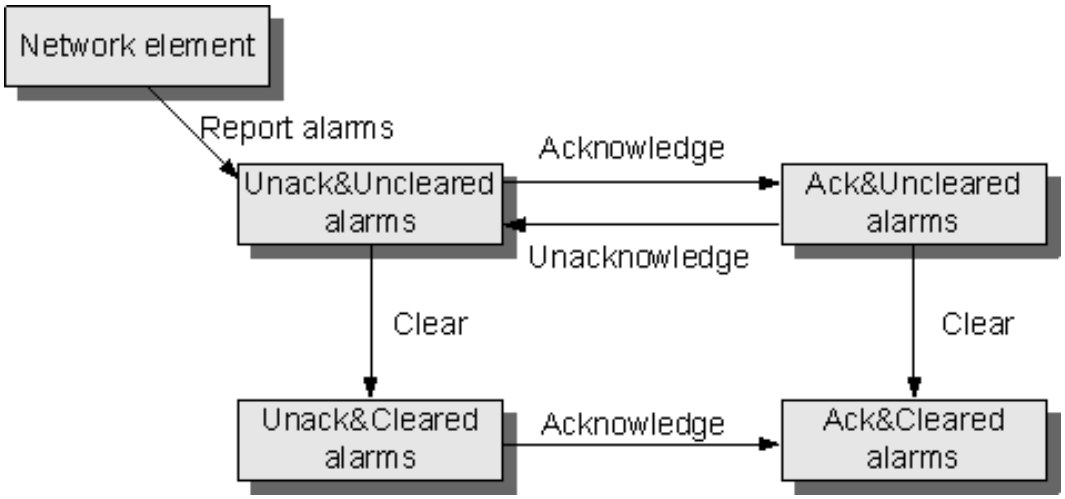
Copyright © Huawei Technologies Co., Ltd.

Table 1-17 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 1-9 shows the relationship between alarm status.

Figure 1-9 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.

Copyright © Huawei Technologies Co., Ltd.

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 Performance Management Concepts

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 1-18 describes the basic concepts about performance management.

Table 1-18 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

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

Copyright © Huawei Technologies Co., Ltd.

the Web. The report system provides the functions such as monitoring, analyzing, optimizing, and formulating polices for network performance, storage, and alarms. The report system supports both instant reports and periodical reports and has an excellent report forwarding mechanism by using emails. The report system features powerful data collection and display capabilities.

Instant Report and Periodical Report

The report system can generate instant reports and periodical reports.

- Instant report

  The report system manages instant reports. You can export instant reports to files in Excel, Word, PDF, and PowerPoint formats.

- Periodical reports

  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.

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.
- 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 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.

Copyright © Huawei Technologies Co., Ltd.

Feature	Description
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 Service Management Concepts

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

Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

1.2.9 Basic Concepts of Smart Configuration Tool

This topic describes terms relevant to the smart configuration tool.

Automatic NE Configuration

With the automatic NE configuration function, software commissioning engineers can enable the NE management channel without going to the site. This reduces deployment costs.

Script 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.

One-Click Batch Delivery of Parameters Using a Plan Sheet

The smart configuration tool allows you to export a profile 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.

General Profile

eSight provides predefined general profiles based on configuration scenarios. You can select a predefined profile and set parameters to generate scripts.

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 1-19shows the basic concepts of backing up and restoring device configuration files.

Table 1-19 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 File to Baseline File	You can save a device configuration file to baseline file for future configuration file restoration.

Copyright © Huawei Technologies Co., Ltd.

1.2.11 What Is 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

Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

2.1 Overview of Security Management Operations

This topic describes the security management operations.

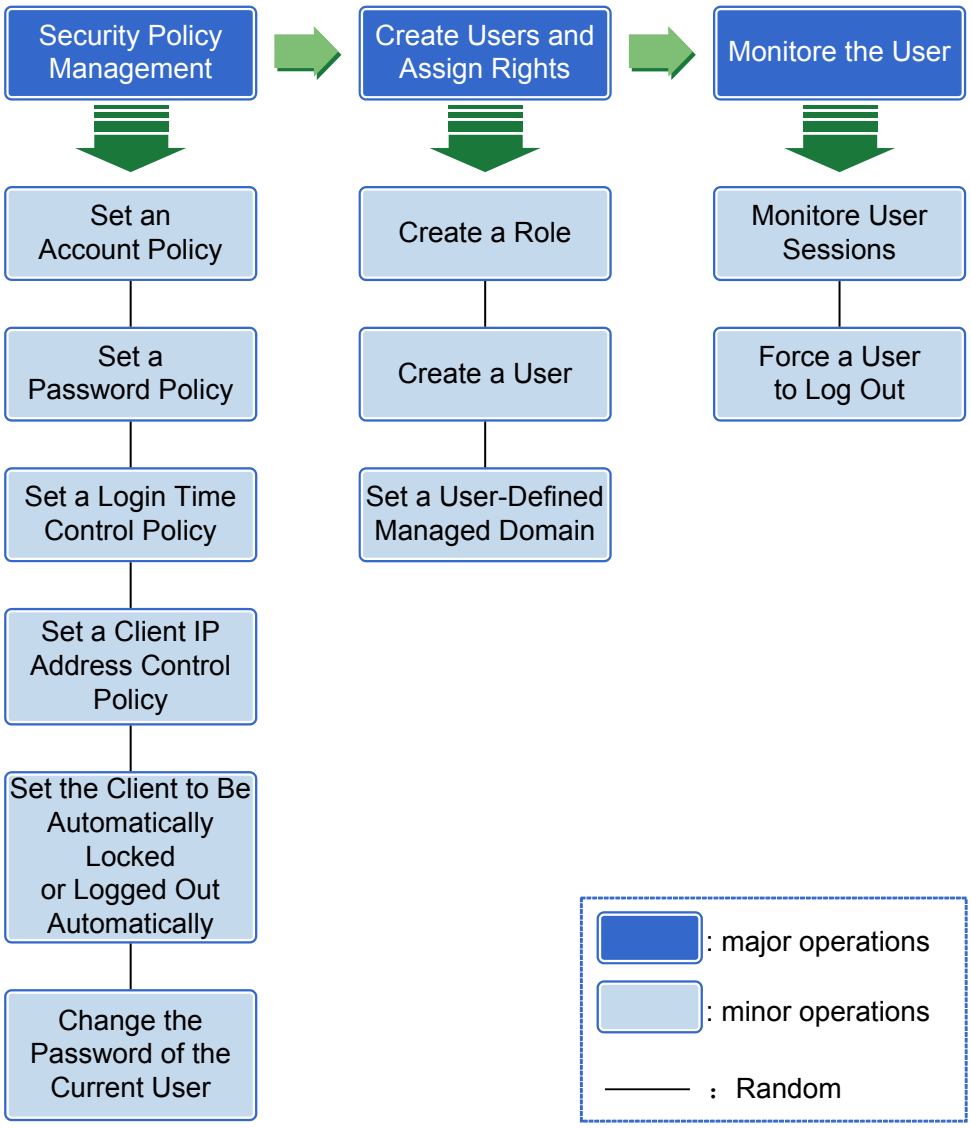
Context

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 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



Copyright © Huawei Technologies Co., Ltd.

Table 2-1 describes the security management operations.

Table 2-1 Security management operations

Operation	Description	Navigation Path
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.	**System** > **Security Management** > **Security Policies** > **Account Policy**
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.	**System** > **Security Management** > **Security Policies** > **Password Policy**
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.	**System** > **Security Management** > **Access Control Policies** > **Login Time Control Policy**
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 within the specified period of time.	**System** > **Security Management** > **Access Control Policies** > **Client IP Address Control Policy**
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.	**System** > **User Settings** > **Basic Settings** > **Idle Time Setting**
2.2.5 Changing a User Password	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.	**System** > **User Settings** > **Basic Settings** > **Change Password**
2.3.4 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.	**System** > **Security Management** > **Rights Assignment** > **Role**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
2.3.5 Creating a User	This topic describes how to create a user. 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.	**System** > **Security Management** > **Rights Assignment** > **User**
2.3.3 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.	**System** > **Security Management** > **Advaned** > **User-Defined Managed Domains**
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.	**System** > **Security Management** > **Security Monitoring** > **User Session Monitoring**
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.	**System** > **Security Management** > **Security Monitoring** > **User Session Monitoring**

2.2 Security Policy Management

Security policies include **Account Policy**, **Password Policy**, and **Account 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.

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

Copyright © Huawei Technologies Co., Ltd.

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

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.

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

Copyright © Huawei Technologies Co., Ltd.

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

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.

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

Copyright © Huawei Technologies Co., Ltd.

Set a Login Time Control Policy	Operation
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 within the specified period of time.

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.

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

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

Copyright © Huawei Technologies Co., Ltd.

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 using specified IP addresseseSight. 1. Click **Create**. 2. On the **Create 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 IP Address 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.

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

Copyright © Huawei Technologies Co., Ltd.

Step 3 On the **Idle Time Setting** page, select **Idle 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 a User Password

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 eSightUser Password**
- **Changing the Password of the AdministratorUser for Windows**
- **Changing the Password of the rootUser 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.

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, set **Old password**, **New password**, and **Confirm password**.
  4. Click **Apply**.

----End

Copyright © Huawei Technologies Co., Ltd.

Changing the Password of the AdministratorUser for Windows

You are advised to change the initial password the first time you log in to the 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.

Background

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

  NOTE

  eSight_ROOT is the eSight installation directory.
- The password for FTP or FTPS is stored in **ftpusers.properties** in **eSight_ROOT\AppBase\etc**.

  NOTE

  eSight_ROOT is the eSight installation directory.

Copyright © Huawei Technologies Co., Ltd.

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

cd /d eSight_ROOT\AppBase\tools\encrypt

Step 2 Run the following command to generate the ciphertext:

encrypt.bat 0 password

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

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.

Step 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.

Background

- The initial password for SBUS is **admin**.
- The encrypt tool is stored in **eSight_ROOT\AppBase\tools\encrypt**.

  NOTE

  eSight_ROOT is the eSight installation directory.
- The password for SBUS is stored in **oms.xml** in **eSight_ROOT\AppBase\etc**.

  NOTE

  eSight_ROOT is the eSight installation directory.

Procedure

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

cd /d eSight_ROOT\AppBase\tools\encrypt

NOTE

eSight_ROOT is the eSight installation directory.

Step 2 Run the following command to generate the ciphertext:

encrypt.bat 0 old password

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

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 password.

Step 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.

Copyright © Huawei Technologies Co., Ltd.

Background

- The initial user name for northbound SNMP V3 is **nbi**, and its initial password is **12345678**.
- The encrypt tool is stored in **eSight_ROOT\AppBase\tools\encrypt**.

  NOTE

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

Procedure

- Change the authentication key.
  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 old password
  3. Replace the password stored in the specified path with the generated password.

     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 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\AppBase\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 password.

     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 password.
  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 OS Users and Their Rights

This topic describes the operating system (OS) users and their rights in the eSight.

Copyright © Huawei Technologies Co., Ltd.

- Table 2-2 describes the Windows users and their rights in the eSight.

Table 2-2 Windows users and their rights in the eSight

User	Description
Administrator	Default user of the OS. As an administrator, the Administrator user has the highest right of the OS. The Administrator user can control all OS resources, create users, assign rights to other users, and perform all the functions provided by the OS. In addition, the Administrator user is responsible for installing and uninstalling of the eSight application software, starting and stopping of the eSight services.

- Table 2-3 describes the Linux users and their rights in the eSight.

Table 2-3 Linux users and their rights in the eSight

User	Description
root	Default user of the OS. As an administrator, the **root** user has the highest right of the OS. The **root** user can control all OS resources, create users, assign rights to other users, and perform all the functions provided by the OS. In addition, the **root** user is responsible for installing and uninstalling of the eSightapplication software.
root	The default user password is **Changeme123**. This user has permission to operate and maintain the eSight server.

2.3.2 eSight Users and Their Rights

This topic describes eSight users and their rights. The eSight users can perform operations on the eSight client.

Table 2-4 describes the eSight users and their rights.

Table 2-4 eSight users and their rights

User	Description
admin	**admin** is the default superuser provided by the eSight, and its initial password is **Changeme123**. **admin** has the management rights of all devices and operation rights of all eSight clients.

Copyright © Huawei Technologies Co., Ltd.

2.3.3 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.

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

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

Operation	Method
Create a user-defined managed domain	Create a user-defined managed domain as required to manage managed objects in a centralized manner. 1. Click **Create**. 2. On the **Create a user-defined managed domain** page, Set **Name** and **Description**. 3. Click **Add**. In the **Select Managed Objects** dialog box, select managed objects. 4. Click **OK**.
View a user-defined managed domain	You can learn about the details by viewing a user-defined managed domain. Click the required managed domain name in the **Managed Domain** column. On the **View User-Defined Managed Domain** page, view the details of the managed domain.
Modify a user-defined managed domain	You can modify a user-defined managed domain as required. 1. Click in the **Operation** column where the required managed domain is located. 2. On the **Modify User-Defined Managed Domain** page, modify the user-defined managed domain. 3. Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Operation	Method
Delete a user-defined managed domain	You can delete an unused user-defined managed domain. 1. Click in the **Operation** column where the required managed domain is located. 2. Click **Yes** in the **Confirm** dialog box.

----End

2.3.4 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.

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

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

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

1. In the **Basic Info** step, set **Role name** and **Description**.
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 also delete the selected users from the list of selected users.
   - 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.

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

   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 **2.3.3 Setting a User-Defined Managed Domain**.
2. In the **Select Managed Objects** dialog box, select managed objects.
3. Click **Next**.

Copyright © Huawei Technologies Co., Ltd.

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

1. In the **Select Operations** step, click **Add**.
2. In the **Select Operations** dialog box, select operations.
3. Click **Next**.

Step 7 Summary.

1. In the **Summary** step, check the role settings.
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. In the **Role Name** column, click the required role name. On the **View Role** page, view the details of the role.
Modify role information	You can modify role information as required. 1. Click in the **Operation** column where the required role information is located. 2. On the **Modify Role** page, change the values of **Description**, **Users**, **Managed Objects**, and **Operation Rights**. For details about how to change the value of **Users**, see **Step 4** under **Create Role**; for details about how to change the value of **Managed Objects**, see **Step 5** under **Create Role**; for details about how to change the value of **Operation Rights**, see **Step 6** under **Create Role**. 3. Click **OK**.
Delete a role	You can delete an unused role. 1. Click in the **Operation** column where the required role information is located. 2. In the **Confirm** dialog box, click **Yes**.

2.3.5 Creating a User

This topic describes how to create a user. 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.

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- 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

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.

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

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

Step 4 On the **Create User** page, set the basic information.

1. In the **Basic Info** step, set **User name**, **Password**, **Confirm password**, and **Description**, and set **Account status** to **Enabled**.
2. Click **Next**.

Step 5 On the **Create User** page, set a role for the user. The user has the management rights and operation rights of the role.

1. In the **Roles** step, select the role.

   NOTE

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

Step 6 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.

1. In the **Access Control Policies** step, select a login time control policy and an IP address range.

   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**.
2. Click **Finish**.

----End

Follow-up Procedure

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

Copyright © Huawei Technologies Co., Ltd.

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 Role** page, view the details of the user.
Modify user information	You can modify user information as required. 1. Click  in the **Operation** column where the required user information is located, and then modify it. 2. On the **Modify User** page, modify the settings of **Basic Info**, **Roles**, and **Access Control Policies**. For details about how to change the value of **Basic Info**, see **Step 4**; for details about how to change the value of **Roles**, see **Step 5**; for details about how to change the value of **Control Policies**, see **Step 6**. 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 **Reset Password** dialog box, set **Reset 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.

Copyright © Huawei Technologies Co., Ltd.

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. To ensure security of the eSight, the eSight provides forcible exit, which prevents unauthorized sessions and operations of users.

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.

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

Step 3 On the **User Session Monitoring** page, view the session information about online users.

NOTE

You can click **Refresh** to refresh the user session information.

----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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

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

Step 3 Click 

in the **Operation** column where the required user information is located.

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.

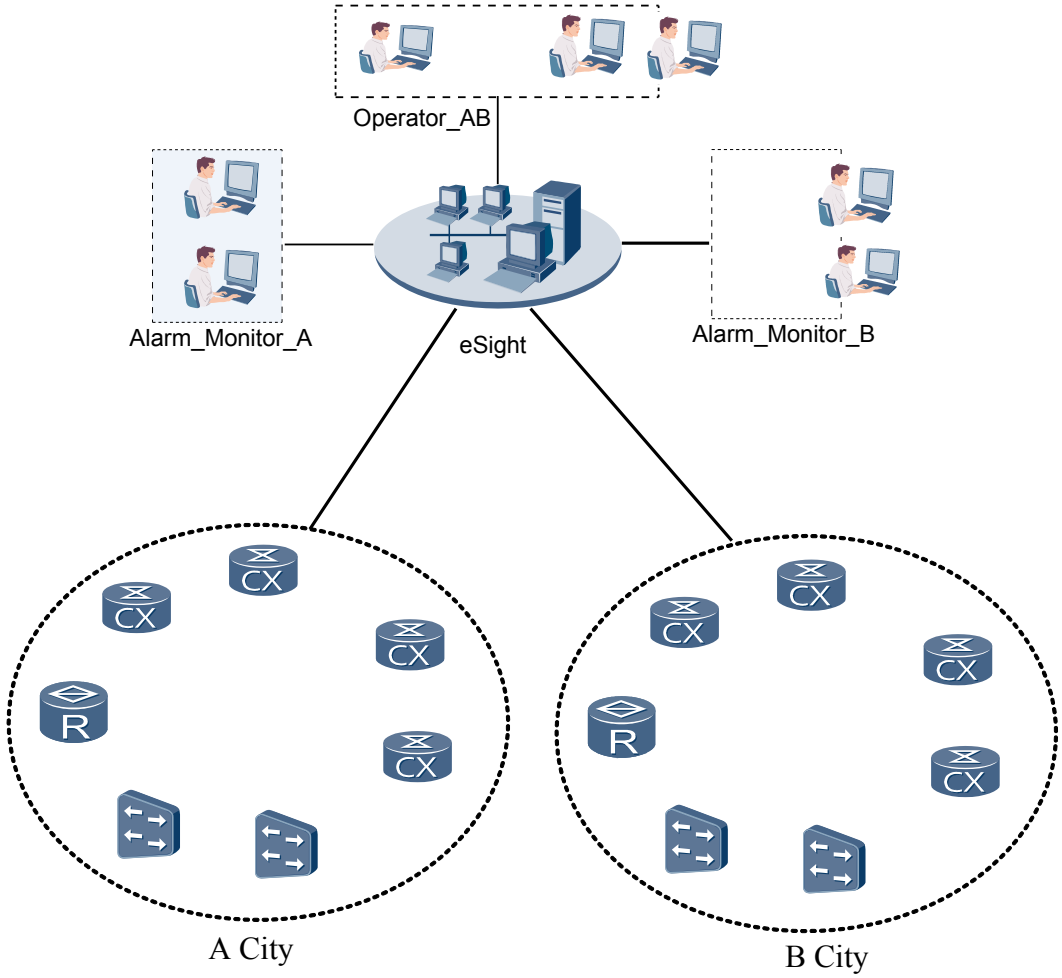
Application Scenario

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

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 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 2-5 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.

Copyright © Huawei Technologies Co., Ltd.

Role	Function	Managed Domain	Operated Rights
Alarm monitor of City A	Monitors alarms of the NEs in city A.	NEs in city A	Browses the masked alarms. Browses historical alarms 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 Browses historical alarms Browses the event list

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

Table 2-6 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:

1. Create two user-defined managed domains: city A and city B.
   a. from the main menuChoose **System** > **Security Management**.
   b. In the **Security Management** window, choose **Advanced** > **User-Defined Managed Domains**.
   c. On the **User-Defined Managed Domains** page, click **Create**. Then set **Name** to **City A** and click **Add**.
   d. In the **Select Managed Objects** dialog box, select all the NEs in city A.
   e. Click **OK**. All the NEs in city A are added to the user-defined managed domain for city A.
   f. Perform steps **1.1** through **1.5** to create a user-defined managed domain for city B and add all the NEs in city B to the user-defined managed domain.
2. Create alarm monitoring roles for city A and city B respectively, and assign the management rights and operations for the roles.
   a. from the main menuChoose **System** > **Security Management**. In the **Security Management** window, choose **Rights Assignment** > **Role**.
   b. On the **Role** page, click **Create**. In the **Basic Info** step, set **Role name** to **Alarm monitor of City A**, and click **Next**.

Copyright © Huawei Technologies Co., Ltd.

c. 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 2-5**, and click **OK**.

f. Click **Next**.

g. Click **Finish**. The alarm monitoring role for city A is created successfully.

h. Perform steps **2.1** through **2.7** 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. from the main menuChoose **System** > **Security Management**. 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 **3.1** through **3.5** 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.

Copyright © Huawei Technologies Co., Ltd.

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 NE 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.

3.3 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.

3.4 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 Link Management

Copyright © Huawei Technologies Co., Ltd.

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.

3.10 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.

3.11 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.

Copyright © Huawei Technologies Co., Ltd.

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 **1.2.3 Basic Concepts of Resource**. 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

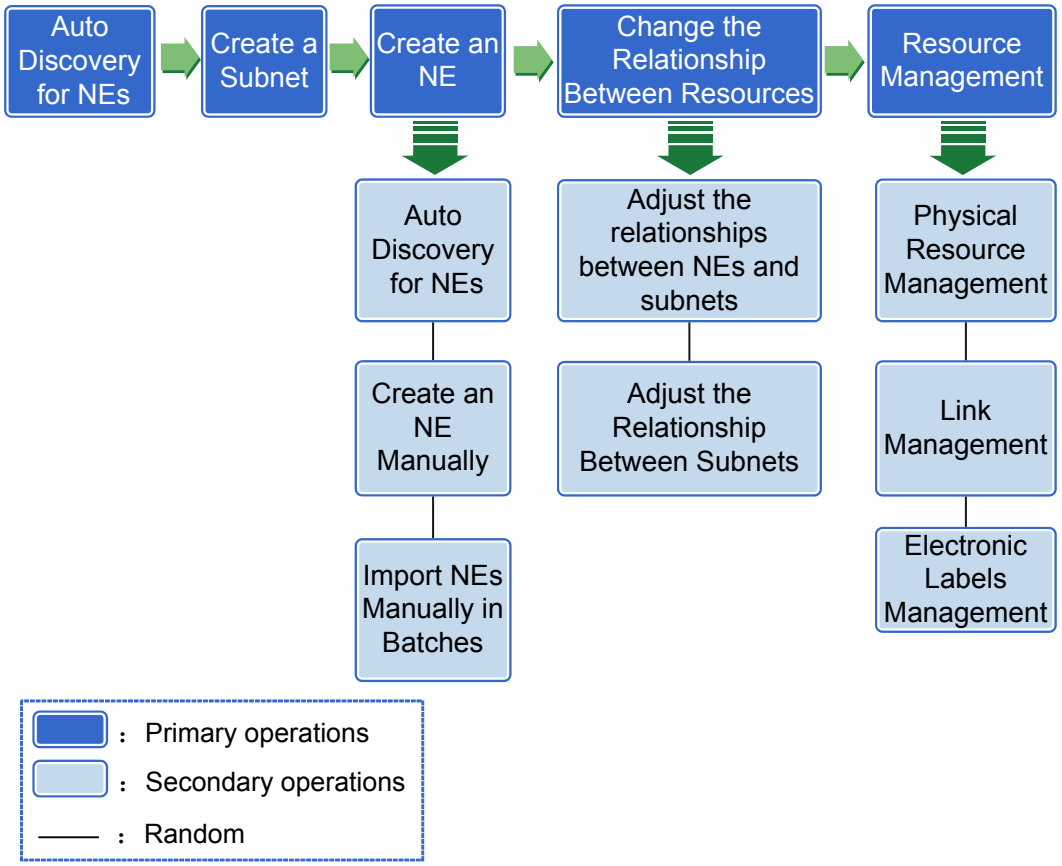


Table 3-1 describes the resource management operations.

Copyright © Huawei Technologies Co., Ltd.

Table 3-1 Resource management operations

Operation	Description	Navigation Path
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
Adjusting the Relationship Between an NE and a Subnet	This topic describes how to adjust the relationships between NEs and subnets as required when the network structure changes.	**Resource** > **Resource Management**
Adjusting the Relationship Between Subnets	This topic describes how to adjust the relationships between subnets and subnets as required when the network structure changes.	**Resource** > **Resource Management**
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.	**Resource** > **Equipment Resources**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
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.	**Resource** > **Link Management**
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.	**Resource** > **Electronic Label**

3.2 NE 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** > **Resource Management** from the main menu.

Step 2 On the managed objects page on the right of the **Resource Management** window, click **Auto Discovery**.

Step 3 On the auto-discovery page, click **Network Segment Discovery**.

Step 4 On the **Network Segment Discovery** page, set network segment discovery parameters and SNMP parameters.

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. For details, see **Save Protocal Template**.

Step 5 **Optional:** Select **Add the discovered objects automatically to the NMS**.

NOTE

- If **Add the discovered objects automatically to the NMS** is selected, the discovered NEs are automatically added. The **Step 7** is skipped.
- If **Add the discovered objects automatically to the NMS** is not selected, you need to execute the **Step 7** to add the discovered NEs.

Copyright © Huawei Technologies Co., Ltd.

Step 6 Click **Discover**.

The discovered NEs are displayed in the list.

NOTE

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

Step 7 Select NEs in the list and click **Create**.

If **Add the discovered objects automatically to the 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.

Step 8 Click **Finish**.

The system returns to the **Resource Management** page, and the added NEs are displayed in the managed object list on the rights.

----End

Follow-up Procedure

The following table describes the operations that you can perform after you add the automatically discovered NEs to the eSight.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. In the managed object list, click the name of the required NE to view its basic information and SNMP information.
Modify NE information	In the eSight, you can modify the attributes of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the name of the NE. 3. Then click **OK**.
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. - To delete an NE, click  in the **Operation** column where the NE is located. - To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

3.3 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. However, if a subnet has 10 subordinate subnets, you can move subnets to the subnet from another subnet.
- A subnet supports a maximum of 500 NEs.

Procedure

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

Step 2 In the **Resource Management** window, select the parent object for the NE to be added, and then click **Create Resource**.

Step 3 On the **Select Object Type** page, select a subnet type under **Subnets and Solutions**.

Step 4 On the **Configure Parameters** page, set **Subnet name** and **Description** for the subnet to be created.

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.

Copyright © Huawei Technologies Co., Ltd.

- 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
View subnet information	In the eSight, you can view subnet information conveniently, including the basic information and protocol information about subnets. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. Click the name of the subnet. The eSight displays all information about the subnet.
Modify subnet information	In the eSight, you can modify the attributes of a subnet, such as the subnet name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the target subnet is located. 2. On the page for modifying subnet information, modify the configuration parameters of the subnet. 3. Then click **OK**.
Delete a subnet	You can delete the subnets that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete subnets. - To delete a subnet, click  in the **Operation** column where the subnet is located. - To delete multiple subnets, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.

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**.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 In the **Resource Management** window, select the parent object for the NE to be added, and then click **Create Resource**.

Step 3 On the **Select Object Type** page, select an NE type under **Physical Devices**.

Step 4 On the **Configure Parameters** page, set the basic information and SNMP protocol for the NE.

NOTE

If you configure simple network management protocol (SNMP) parameters for an NE, click **Save Protocol Template** to save the settings as an SNMP parameter configuration template. If you need to configure SNMP parameters again, click **Select Protocol Template** to select the saved protocol template to apply.

Step 5 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

Follow-up Procedure

The following table describes the operations that you can perform after you manually create an NE in the eSight.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. Click the name of the required NE. The eSight displays all information about the NE.
Modify NE information	In the eSight, you can modify the name of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the configuration parameters of the NE. 3. Then click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. ● To delete an NE, click  in the **Operation** column where the NE is located. ● To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

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, **10.123.124.115**.
NE Name	1 to 128 characters. The NE name cannot contain the following characters #%&+/;<=>?\.
Protocol Type	Set to **SNMP**.
Protocol Version	The protocol version must be the same as the SNMP protocol version in the device. The value range is **V1** or **V2c**.

Copyright © Huawei Technologies Co., Ltd.

Field name	Description
Port	This parameter must be the same as the port number of the SNMP protocol, for example, **161**.
Read Community	This parameter must be the same as the read community of the SNMP protocol, for example, **public**.
Write Community	This parameter must be the same as the write community of the SNMP protocol, for example, **private**.

Procedure

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

Step 2 On the managed object page on the right of the **Resource Management** window, click **Batch Import**.

Step 3 On the **Select Objects to Import in Batches** page, select **Import Hosts and Network Devices**.

Step 4 In **Import Hosts and Network Devices**, click 

next to **Template to download**, and download the **.xls** template to the local computer.

Step 5 Open the template, fill in NE information, and save the template.

Step 6 Click  next to **Resource file to import** to select the .xls file that you have saved.

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

Step 7 Click  to upload the file.

Resources displays NE information in the file and the result of the check. If the **Result** column is blank, the NE check is successful.

Step 8 Select NEs under **Resources**, 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.

----End

Follow-up Procedure

The following table describes the operations that you can perform after you manually import NEs to the eSight.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. Click the name of the required NE. The eSight displays all information about the NE.
Modify NE information	In the eSight, you can modify the name of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the configuration parameters of the NE. 3. Then click **OK**.
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. ● To delete an NE, click  in the **Operation** column where the NE is located. ● To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

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**.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 In the **Resource Management** window, select an NE and click  .

Step 3 In the **Source Nodes** area in the **Move Nodes** dialog box, select an NE to be moved. In the **Target Nodes** area, select a subnet.

Step 4 Click **OK**.

In the **Resource Management** window, the adjusted NE is displayed under the required subnet.

----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.

Step 2 In the **Resource Management** window, select a subnet and click  .

Step 3 In the **Source Nodes** area in the **Move Nodes** dialog box, select an NE to be moved. In the **Target Nodes** area, select a subnet.

Step 4 Then click **OK**.

In the **Resource Management** window, the adjusted subnet is displayed under the required subnet.

----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.

Copyright © Huawei Technologies Co., Ltd.

Table 3-3 Supported operations

Resource Type	GUI Entry	Supported Operations
Device	Choose **Resource** > **Equipment Resources** from the main menu.Click **NE Resource** from the navigation tree on the left.	**Export**: You can export device information to files. **Synchronize**: You can synchronize device data to eSight. **Set SNMP Parameters**: You can set SNMP parameters of NEs on eSight in batches. **Set Telnet Parameters**: You can set Telnet parameters of NEs on eSight. **Modify Remarks**: You can click  to modify remarks and maintain information of device. Display the NE manager: You can click **Name** of a device to display the NE manager corresponding to the device.
Subrack	Choose **Resource** > **Equipment Resources** from the main menu.Click **Frame Resource** from the navigation tree on the left.	**Export**: You can export frame information to files. **Modify Remarks**: You can click  to modify frame remarks.
Board	Choose **Resource** > **Equipment Resources** from the main menu.Click **Board Resource** from the navigation tree on the left.	**Export**: You can export board information to files. **Modify Remarks**: You can click  to modify board remarks.
Subcard	Choose **Resource** > **Equipment Resources** from the main menu.Click **Subcard Resource** from the navigation tree on the left.	**Export**: You can export subcard information to files. **Modify Remarks**: You can click  to modify subcard remarks.
Port	Choose **Resource** > **Equipment Resources** from the main menu.Click **Port Resource** from the navigation tree on the left.	**Export**: You can export port information to files. **Modify Remarks**: You can click  to modify port remarks.

Copyright © Huawei Technologies Co., Ltd.

3.9 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.

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**.

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 #{readvalue} 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.

Copyright © Huawei Technologies Co., Ltd.

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 **Source NE**, **Source Port**, **Destination NE**, and **Destination Port**, and click **OK**.

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	Change the link display rules. 1. In the **Link Management** window, click **Display Rule** to set the display rule for a link. ● In **Naming Rule**, set the display fields of a link name. ● In **Tip Rule**, set the display fields of link tips. **NOTE** 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.
Delete a link	Delete a link. 1. In the **Link Management** window, select a link to be deleted and click **Delete**. 2. In the displayed dialog box, click **Yes**. **NOTE** The deleted link is a link of eSight. To re-upload the link data to eSight, you can perform the **Discover Link** operation.

Copyright © Huawei Technologies Co., Ltd.

3.10 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.

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.

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

3.11 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.

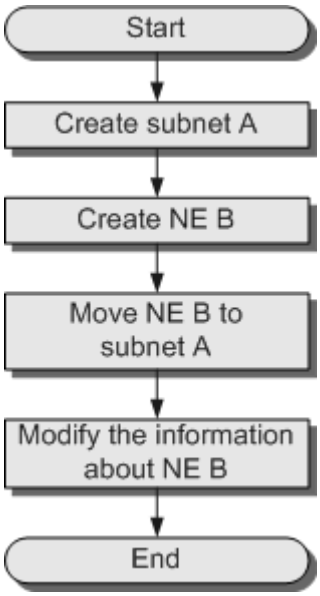
Context

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 theeSight.

Figure 3-2 shows the procedure.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 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 Nodes** 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.

Copyright © Huawei Technologies Co., Ltd.

4. Then click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

4 Topology Management

About This Chapter

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

Copyright © Huawei Technologies Co., Ltd.

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 **1.2.2 Basic Concepts About 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

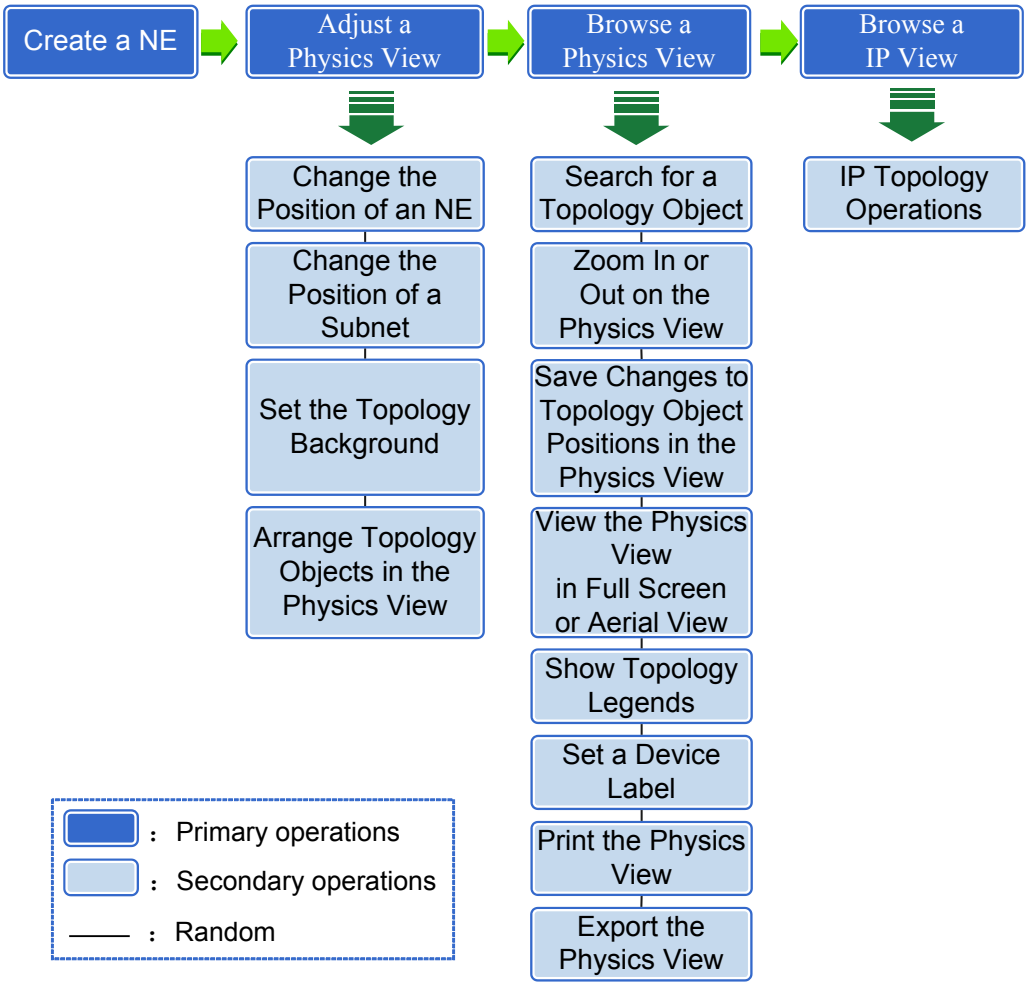


Table 4-1 describes the topology management operations.

Copyright © Huawei Technologies Co., Ltd.

Table 4-1 Topology management operations

Operation	Description	Navigation Path
Adjust the Positions of NEs	When the positions of NEs change, you need to adjust the corresponding positions in the physics view to update the relationships between NEs and other topology objects.	**Resource** > **Topology Management**
Adjust the Positions of Subnets	When the positions of subnets change, you need to adjust the corresponding positions in the physics view to update the relationships between the subnets and other topology objects.	**Resource** > **Topology Management**
Set the Topology Background	This topic describes how to set the topology background based on the layout of topology objects.	**Resource** > **Topology Management**
Arrange Topology Objects in the Physics View	This topic describes how to rearrange topology objects in a physics view if required.	**Resource** > **Topology Management**
Search Topology Objects	You can use the search function to quickly locate an object, such as an NE, a link or a subnet.	**Resource** > **Topology Management**
Zoom In or Out on the Physics View	This topic describes how to zoom in or zoom out on a physics view, restore a physics view to its initial state, and make a physics view display in a proper size or in full screen mode.	**Resource** > **Topology Management**
Save NE Positions in the Physics View	If the position of a topology object in the physics view is changed, you can save the position as required.	**Resource** > **Topology Management**
View the Physics View in Full Screen or Aerial View	This topic describes how to view a topology view in full screen or in aerial view.	**Resource** > **Topology Management**
Show Topology Legends	This topic describes how to show topology legends in the topology view. Topology legends define the meanings of topology object colors or status.	1. **Resource** > **Topology Management** 2. On the toolbar of the **Topology Management** window, choose  > **Show Legends**.

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
Set 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.	1. **Resource** > **Topology Management**. 2. On the toolbar of the **Topology Management** window, choose  > **Set Device Label**.
Print the Physics View	You can print the physics view.	**Resource** > **Topology Management**
Export the Physics View	You can export the physics view to a local PC.	**Resource** > **Topology Management**
IP Topology Operations	Describes how to perform operations on the IP topology to monitor devices and links.	**Resource** > **IP Topology Management**

4.2 Physical Topology Management

4.2.1 Designing a Physics View

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

The eSight provides the following suggestions for designing the physics 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 Physics View

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

4.2.2.1 Changing the Position of an NE

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

Prerequisites

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

Copyright © Huawei Technologies Co., Ltd.

Context

You can adjust the positions of NEs in the physics 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.

Step 2 In the **Topology management** window, adjust the position of an NE.

- Move a single NE: In the physics view, click the NE, and drag it to a specified position.
- Move multiple NEs: In the physics view, select multiple NEs while holding down **Ctrl**, and drag them to a specified position.

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

----End

4.2.2.2 Changing the Position of a subnet

When the positions of subnets change, you need to adjust the corresponding positions in the physics 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 physics 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.

Step 2 In the **Topology Management** window, 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.

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

----End

4.2.2.3 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**.

Copyright © Huawei Technologies Co., Ltd.

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.

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 topology view, select **Hide background image**.

Step 4 Click **OK**.

The image is displayed as the topology background.

----End

4.2.2.4 Rearranging Topology Objects in a Physics View

This topic describes how to rearrange topology objects in a physics 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

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

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

Step 3 Click  to save the new positions.

----End

4.2.3 Browsing a Physics View

This topic describes the methods of browsing a physics view.

4.2.3.1 Searching for a Topology Objects

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.

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.

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 physics view and navigation tree.

----End

4.2.3.2 Zooming In or Out on a Physics View

This topic describes how to zoom in or zoom out on a physics view, restore a physics view to its initial state, and make a physics 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.

Copyright © Huawei Technologies Co., Ltd.

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

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

----End

4.2.3.3 Saving Changes to Topology Object Positions in the Physics View

If the position of a topology object in the physics 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.

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

Step 3 Click  to save the physics view.

----End

4.2.3.4 Viewing the Topology View in Full Screen or Aerial View

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

Procedure

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

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

The aerial view is displayed, in which the NEs in the white rectangle are visible.

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

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

Copyright © Huawei Technologies Co., Ltd.

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

Step 5 Click to close the aerial view.

Step 6 Click to display the topology view in full screen.

NOTE

- 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 topology 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 topology 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.

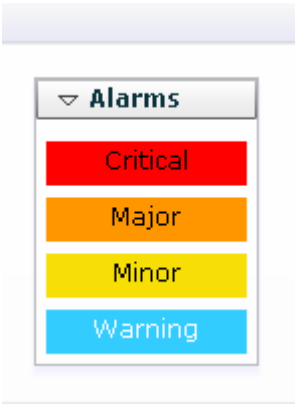
Procedure

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

Step 2 On the toolbar of the **Topology Management** window, choose > **Show Legends**

Topology legends are shown in the following figure.

Copyright © Huawei Technologies Co., Ltd.



----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.

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.

Step 4 Click **OK**.

The selected device information is displayed under the device icon.

----End

4.2.3.7 Printing the Physics View

You can print the physics view.

Procedure

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

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

Copyright © Huawei Technologies Co., Ltd.

Step 3 Set the print parameters.

Step 4 Click **Print**.

----End

4.2.3.8 Exporting the Physics View

You can export the physics view to a local PC.

Procedure

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

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

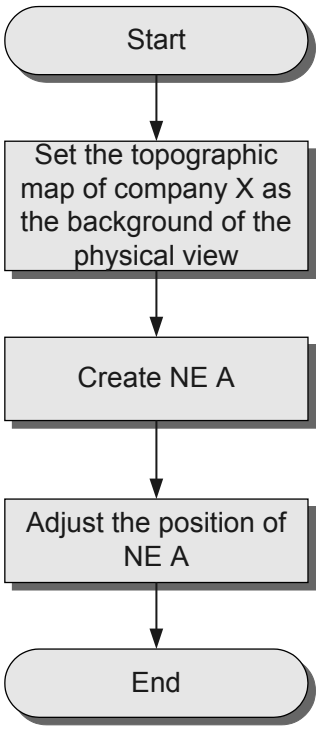
This topic describes an example about how to perform topology management operations. With this example, you can learn about the procedure for creating a topology view.

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 4-2 shows the procedure for creating a topology view.

Figure 4-2 Procedure



Copyright © Huawei Technologies Co., Ltd.

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. 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 A.
4. Then 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 Physics View** and **4.2.3 Browsing a Physics 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.

Copyright © Huawei Technologies Co., Ltd.

Table 4-2 IP topology management functions

Function		Description
IP topology monitoring	Device alarm, subnet alarm, and link alarm	● Device alarm: The color of a device icon indicates the highest severity of alarms generated on the device. ● 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. ● Subnet alarm: The color of a subnet indicates the highest severity for alarms generated on the subnet. **NOTE** Topology views display icons that indicate the real-time highest severity of alarms that occur on devices, links, and subnets.
	Link status Detailed information about links and devices	● The Layer 2 topology view displays the real-time status of LLDP links. ● The Layer 3 topology view displays the real-time status of IP links.
	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 **Current Alarms**.
	Viewing active alarms on a device	In the IP topology view, right-click a device, and choose **Alarm List**.
IP topology management	Automatic recognition of Layer 2 and Layer 3 devices	eSight recognizes routing devices based on the routing function. 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. **NOTE** When a device is added to eSight, it will be displayed in the IP topology.
	Blank subnet display and hiding	A blank subnet refers to a subnet where no device is deployed. eSight can display and hide blank subnets as required.

Copyright © Huawei Technologies Co., Ltd.

Function		Description
	IP change management	● IP Change Notification: 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. ● Remove IP Change Notifications: If an IP change notification requires no further attention, you can remove it. ● IP Changes: When an IP change notification is displayed, you can view the IP change details in the IP change list. ● IP Change Summary: IP change summary lists detailed information about all IP changes on the entire network. ● Remove All IP Change Notifications: If all the current IP change notifications require no further attention, you can remove them.

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**.

     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.

Copyright © Huawei Technologies Co., Ltd.

1. View IP change notifications: On the IP topology management page, if  is displayed on a device, the device IP address is changed.
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**.

   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**.
3. 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.
- 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**.

----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.

Copyright © Huawei Technologies Co., Ltd.

Step	Description
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

Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

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 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

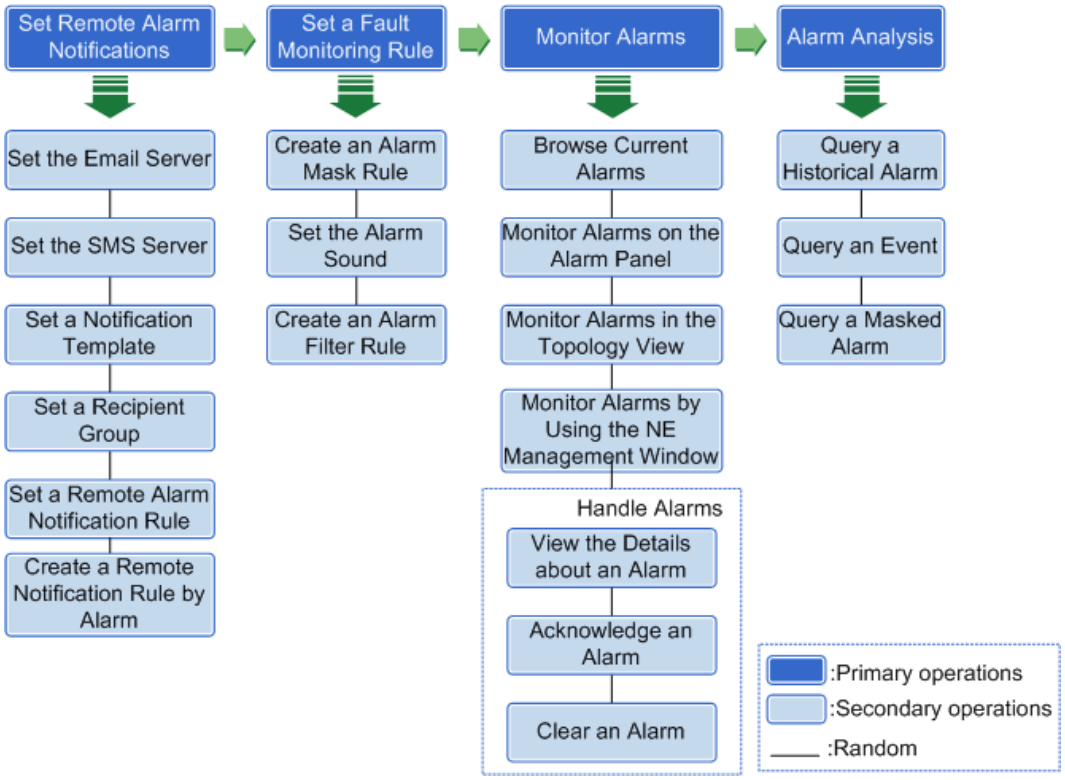


Table 5-1 describes the fault management operations.

Copyright © Huawei Technologies Co., Ltd.

Table 5-1 Fault operations

Operation	Description	Navigation Path
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 notify the device users by email.	**Fault** > **Alarm Settings** > **Remote Notification** > **Email Server**
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 notify the device users by SMS.	**Fault** > **Alarm Settings** > **Remote Notification** > **SMS Server**
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.	**Fault** > **Alarm Settings** > **Remote Notification** > **Notification Template**
5.2.5 Setting a Recipient Group	When you set the remote alarm notification, you need to set the recipient group to be notified.	**Fault** > **Alarm Settings** > **Remote Notification** > **Notification Recipient Groups**
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.	**Fault** > **Alarm Settings** > **Remote Notification** > **Remote Notification Rules**
5.2.7 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.	**Fault** > **Alarm Settings** > **Remote Notification** > **Remote Notification Rules**
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.	**Fault** > **Alarm Settings** > **Basic Settings** > **Mask Rules**
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.	**Fault** > **Alarm Settings** > **Basic Settings** > **Alarm Sound**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
5.3.3 Creating an Alarm Filter Rule	You can save the frequently used alarm filter criteria as a template for future queries by using the same filter criteria.	**Fault** > **Current Alarms** > **Filter criteria** > **Set filter criteria**
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.	**Fault** > **Current Alarms**
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.	eSight Main user interface of the client
5.4.3 Monitoring Alarms in the Topology View	The topology view allows you to monitor the alarms of NEs real time.	**Resource** > **Topology Management**
5.4.4 Monitoring Alarms in the NE Monitoring List	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.	**Resource** > **Resource Management**
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.	**Fault** > **Current Alarms**
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.	**Fault** > **Current Alarms**
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.	**Fault** > **Current Alarms**
5.5.1 Querying a Historical Alarm	You can quickly find the desired historical alarms based on specified search criteria.	**Fault** > **Historical Alarms**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
5.5.2 Querying an Event	You can query events to view the notification sent from the device to the eSight.	**Fault** > **Events**
5.5.3 Querying a Masked Alarm	This topic describes how to quickly query the desired masked alarms.	**Fault** > **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.

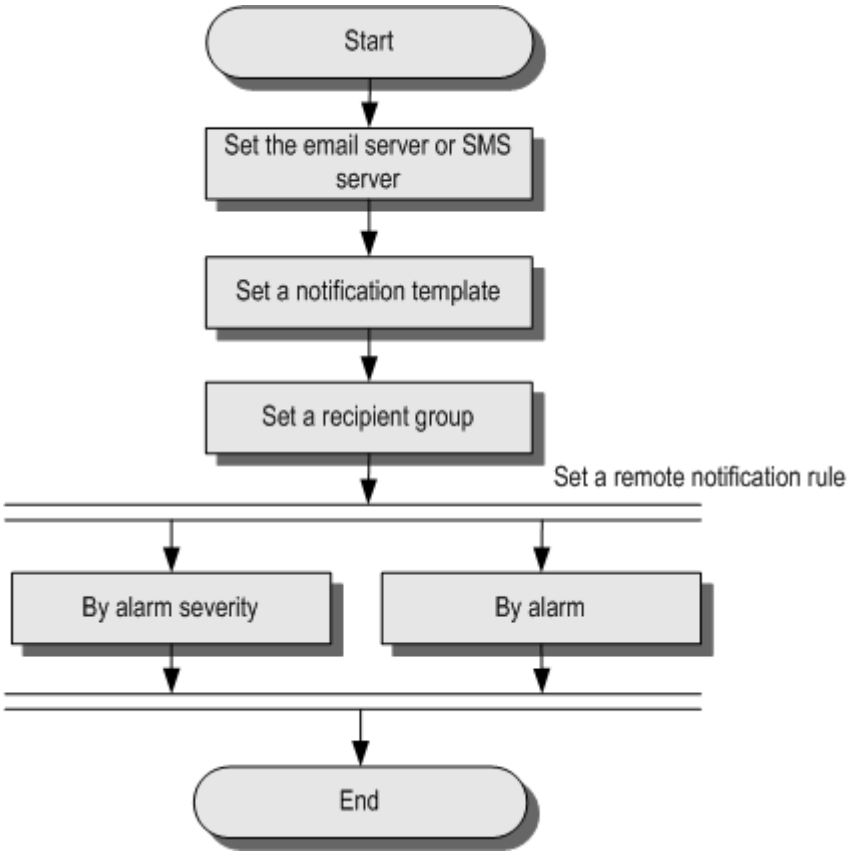
5.2.1 Procedure for Setting Remote Notification

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.

Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

Step	Operation	Description
4	Set a remote notification rule	You can add notification rules by **By Alarm Severity** and **By Alarm**. 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 notify the device users by email.

Prerequisites

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

Procedure

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

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

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

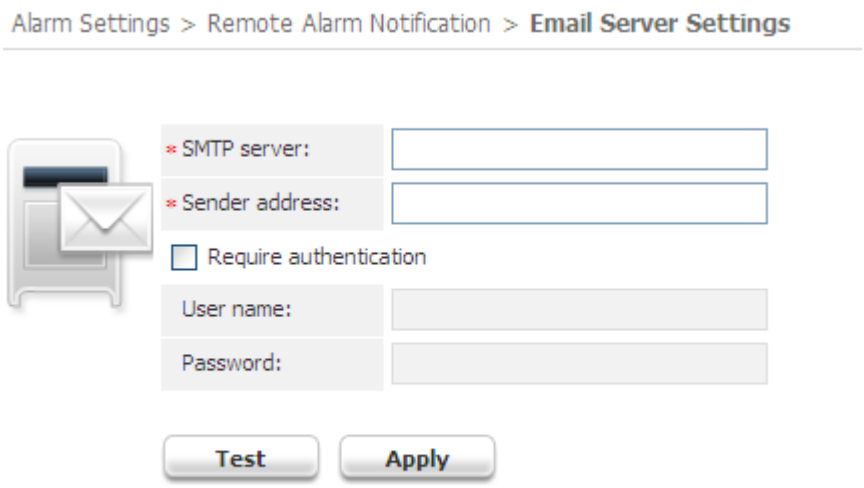
- **SMTP server**: the host name or IP address of the SMTP Email server.

  NOTE

  You are recommended to use the IP address of the Email server to avoid the connection failure due to domain name resolution failure. The default SMTP port number is **25**. Ensure that the SMTP port on the Email server is available.

- **Sender address**: the email address of the sender.
- **Require authentication**: if the SMTP server requires authentication, you need to select **Require authentication** and set the user name and password of the SMTP server. Determines whether the current user has permission to send emails.

Copyright © Huawei Technologies Co., Ltd.



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.
- After setting the parameters of the email server, you can click **Apply** to save the settings. As the email server parameters involves the user name and password, to ensure security, the eSight does not prompt you to save data when you do not click **Apply**.

----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 notify the device 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.

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.
- **Protocol**: the protocol used by the short message center.

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.

Copyright © Huawei Technologies Co., Ltd.

Table 5-3 Support long messages

Encoding Protocol	Support Long Messages
SMPP3_3/SMPP3_4 CMPP2_x/ CMPP3_x	● If you select **Yes**: The recipient can receive the entire message, no matter how many characters are contained a short message sent by the sender. ● If you select **No**: A short message contains a maximum of **70** characters. If a message contains more than **70** characters, the system splits the message and sends several short messages to the recipient.
SGIP	● If you select **Yes**: The recipient can receive the entire message, no matter how many characters are contained a short message sent by the sender. ● If you select **No**: A short message contains a maximum of **80** characters. If a message contains more than **80** characters, the system splits the message and sends several short messages to the recipient.

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.
- After setting the parameters of the SMS server, you can click **Apply** to save the settings. As the SMS server parameters involves the user name and password, to ensure security, the eSight does not prompt you to save data when you do not click **Apply**.

----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.

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** box. Click  to add the field to the **Selected Alarm Fields** list.

Copyright © Huawei Technologies Co., Ltd.

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 the **Available Event Fields** box. 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** area or the **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.

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.

Step 2 In the **Alarm Settings** window, choose **Remote Notification** > **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	1. Click **Create**. 2. On the **Create Recipient Group** page, set the name and description of the user group, and add users to the user group. Add users to the user group: a. On the **Create Recipient Group** page, click **Create**. b. In the **Create Recipient** dialog box, set the user name, mobile phone number, and email address. c. Click **OK**. On the **Create Recipient Group** page, click  or  in the **Operation** column where the required user information is located to modify or delete the user information. 3. On the **Create Recipient Group** page, click **Save**.

Copyright © Huawei Technologies Co., Ltd.

Setting Recipient Groups	Operation Method
View recipient Group	1. Click **Group Name** of the required user group. 2. On the **View User Group** page, view the user group information and user information.
Edit a recipient group and users	1. Click in the **Operation** column where the required user group information is located. 2. On the **Modify User Group** page, modify the name, description, and user information about the recipient group. Modifying user information involves adding, deleting, and modifying user information.
Delete a recipient group	1. Click in the **Operation** column where the required user group information is located. 2. In the **Confirm** dialog box, click **Yes**.

----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.

Prerequisites

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

Context

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.

Procedure

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

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

Step 3 In the **Remote Notification Rules** page, you can perform the following operations.

Copyright © Huawei Technologies Co., Ltd.

Setting Notification Rules	Operation Method
Create notification rules	If you create a remote alarm notification rule, the alarms that meet conditions are sent to the maintenance personnel. This helps the maintenance personnel learn about the alarm information about the eSight server and then take measures. The eSight allows you to create a notification rule by alarm severity or alarm. A remote notification rule is enabled by default once it is created. ● **By Alarm Severity**: 1. Choose **Create** > **By Alarm Severity**. 2. 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**. ● **By Alarm**: For details, see **5.2.7 Creating a Remote Notification Rule by Alarm**.
Enable notification rules	Enable a disabled remote notification rule. Select one or more notification rules and click **Enable** to enable the notification rules.
Disable notification rules	Disable a remote notification rule that is not used currently. Select one or more notification rules and click **Disable** to disable the notification rules.
Modify notification rules	Modify a remote notification rule to meet management requirements. 1. Click in the **Operation** column where the required remote notification rule is located. 2. On the **By Alarm Severities** or **By Alarm** 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. 1. Click in the **Operation** column where the required remote notification rule is located. 2. In the **Confirm** dialog box, click **Yes**.

----End

Copyright © Huawei Technologies Co., Ltd.

5.2.7 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

You must learn about information about the subnet, alarm source, and event related to the alarm.

Procedure

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

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**.

Step 4 Select an alarm source.

1. Under **Alarm Sources** step on the **Create by Alarm** page, set **Rule name** and click **Add Alarm Sources**.
2. Under **Subnets** in the **Add Alarm Sources** dialog box, select subnets.
   - Select the **Root** node. All the NEs are displayed in **Alarm Sources**.
   - Select a subnet. All the NEs under the subnet are displayed in the **Alarm Sources** area.
   - Select an NE under the subnet. A red asterisk (*) is displayed in the upper right corner of the subnet, which indicates that you selected an NE under the subnet.
3. Under **Alarm Sources** in the **Add Alarm Sources** dialog box, select NEs.
   - Click **Select All** or **Clear All** to select or deselect all the alarm sources under **Alarm Sources**.
   - Select the alarm sources under multiple subnets as required. The alarm sources that you selected will not be displayed under these subnets.
4. Click **OK**.
5. Click **Next**.

Step 5 Select an alarm or event.

1. Under **Alarms/Events** step on the **Create By Alarm** page, click **Add 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.
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**.

Copyright © Huawei Technologies Co., Ltd.

- 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.

Step 7 Click **Finish**.

A remote notification rule is enabled by default once it is created.

----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.

Step 2 In the **Alarm Settings** window, choose **Basic Settings** > **Mask Rules**.

Step 3 On the **Mask Rules** page, click **Create**.

Step 4 Set the basic information.

Copyright © Huawei Technologies Co., Ltd.

1. Under **Basic Information** step on the **Create an Alarm Mask Rule** page, set **Rule name**, **Date**, and **Time**.
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**.
2. Under **Subnets** in the **Add Alarm Sources** dialog box, select subnets.
   - Select the **Root** node. All the NEs are displayed in **Alarm Sources**.
   - Select a subnet. All the NEs under the subnet are displayed in the **Alarm Sources** area.
   - Select an NE under the subnet. A red asterisk (*) is displayed in the upper right corner of the subnet, which indicates that you selected an NE under the subnet.
3. Under **Alarm Sources** in the **Add Alarm Sources** dialog box, select NEs.
   - Click **Select All** or **Clear All** to select or deselect all the alarm sources under **Alarm Sources**.
   - Select the alarm sources under multiple subnets as required. The alarm sources that you selected will not be displayed under these subnets.
4. Click **OK**.
5. Click **Next**.

Step 6 Select an alarm.

1. Under **Alarms** step on the **Create an Alarm Mask Rule** page, click **Add Alarms**.
2. Under **Device Type** in the **Add Alarms** dialog box, select a device type.
   - Select a device type. All the device types under the subnet are displayed in the **Device Type** area.
   - 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.
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.

Copyright © Huawei Technologies Co., Ltd.

Setting Alarm Masking Rules	Operation Method
Enabling an Alarm Mask Rule	Enable a disabled alarm mask rule. On the **Mask Rules** page, select one or more mask rules, and click **Enable**. If the **Enabled** column for a mask rule is displayed as **Enabled**, 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. On the **Mask Rules** page, select one or more mask rules, and click **Disable**. If the **Enabled** column for a mask rule is displayed as **Disabled**, 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. 1. On the **Mask Rules** page, click  in the **Operation** column where the required mask rule is located. 2. In the **Confirm** dialog box, click **Yes**.
Modifying an Alarm Mask Rule	Modify an alarm mask rule to meet management requirements. 1. On the **Mask Rules** page, click  in the **Operation** column where the required mask rule is located. 2. On the **Modify Alarm Mask Rule** 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**

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 In the **Alarm Settings** window, choose **Basic Settings** > **Alarm Sound**.

Step 3 In the **Alarm Sound** page, you can perform the following operations.

Setting Alarm Sound	Operation Method
Disable alarm sound	Select **Severity** and click **Disable** to disable the alarm sound for the severity.
Enable alarm sound	Select **Severity** and click **Enable** to enable the alarm sound for the severity.
Play alarm sound	Click  in the **Play** column to play the alarm sound.
Change alarm sound	Click  in the **Operation** column. On the **Set Alarm Sound** page, change the values of **Alarm sound** and **Play count**, and click **Save**.
Restore the default settings	Click **Default Setting** to restore the alarm sound to the initial setting.

----End

5.3.3 Creating an Alarm Filter Rule

You can save the frequently used alarm filter criteria as a template for future queries by using the same filter criteria.

Prerequisites

You have the operation rights for **Current Alarms Management**.

Context

The default filter criteria 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 cannot be deleted or modified.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Fault** > **Current Alarms** from the main menu.

Step 2 In the **Current Alarms** window, select **Set filter criteria** from the **Filter criteria** drop-down list on the toolbar.

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	When the default filter criteria of the eSight cannot meet the current management requirements, you can create user-defined filter criteria. 1. Click **Create**. In the right area, set the name, alarm severity, acknowledgement status, clearance status, event type, and first occurrence time. 2. Click **Save**.
Delete customizing alarm filter criteria	Delete unnecessary user-defined filter criteria to ensure sufficient memory and proper running of tasks on the server. 1. In the filter criteria list, select the user-defined filter criterion and click **Delete**. 2. In the **Confirm** dialog box, click **Yes**.
Modify customizing alarm filter criteria	Modify user-defined filter criteria to meet the latest management requirements. 1. In the list of filter criteria on the left, select a user-defined filter criterion. In the right area, modify the name, alarm severity, acknowledgement status, clearance status, event type, and first occurrence time. 2. Click **Save**.
Copy customizing alarm filter criteria	Copy a user-defined filter criterion. 1. In the list of filter criteria on the left, select a user-defined filter criterion, and click **Copy**. In the right area, modify the name, alarm severity, acknowledgment status, clearance status, event type, and first occurrence time. 2. Click **Save**.

----End

5.4 Monitoring Alarms

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

Copyright © Huawei Technologies Co., Ltd.

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 the alarms have the same alarm source, location information, and alarm ID, the alarms are merged to one record.
- If the current filter criteria are modified, the system searches for alarms based on the modified filter criteria.

Procedure

Step 1 Choose **Fault** > **Current Alarms** from the main menu.

Step 2 In the **Current Alarms** window, select filter criteria from the **Filter criteria** drop-down list and perform a search. You can customize filter criteria if required. For details, see **5.3.3 Creating an Alarm Filter Rule**.

Step 3 In the **Current Alarms** window, you can perform the following steps:

Management Alarms	Operation Method	Description
Lock alarms	Click **Lock**. The alarms in the current list are locked. In addition, **Lock** is automatically changed to **Unlock**.	If the alarms in the current list are locked, note that: ● Newly reported alarms can be displayed in the current alarm list only after you click **Unlock**. ● 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. ● If you acknowledge or clear an alarm when you click **Lock**, the alarm can be updated to the historical alarm list only when you click **Unlock**.

Copyright © Huawei Technologies Co., Ltd.

Management Alarms	Operation Method	Description
Unlock alarms	Click **Unlock**. The eSight reports alarms to the alarm list automatically. In addition, **Unlock** is automatically changed to **Lock**.	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: ● Click **Search** without setting any search criteria. All alarms are displayed in the current list. ● 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 **Search**.	-
Acknowledge	Select one or more alarms and click **Acknowledge**.	● If the alarm is acknowledged, **Acknowledged By** displays the user who acknowledges the alarm. ● If the alarm is unacknowledged, **Acknowledged By** displays  .
Unacknowledge	Select one or more alarms and choose **More** > **Unacknowledge**.	After an alarm is unacknowledged, its status is changed from **Acknowledged** to **Unacknowledged**.
Clear	Select one or more uncleared alarms and click **Clear**.	● The background color of clear alarms is green. ● The background color of uncleared alarms is white.
Alarm Mask	1. Click in the **Operation** column where the required alarm is located, and select **Mask Rules**. 2. In the **Mask Rules** dialog box, set the rule name and shielding date. Click **OK**.	● The newly created alarm mask rule is in enabled status by default. ● 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. ● You cannot set a masking rule for a performance alarm or clear alarm.

Copyright © Huawei Technologies Co., Ltd.

Management Alarms	Operation Method	Description
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 **OK**.	-
Locate to Topo	Click  in the **Operation** column where the required alarm record is located.	eSight locates the NE in the managed object that generates the alarm in the topology view.
Alarm Details	Click **Alarm Name** of which you want to view details.	The **Alarm Details** dialog box displays the name, probable cause, and proposed repair actions for the selected alarm.
Alarm Logs	Click **Number of Occurrences** about which you want to view the log information.	The **Alarm Logs** dialog box displays the alarm log related to this alarm record.
Export	Select one or more alarms and choose **Export** > **Selected Records** to export the alarm information. If you want to export all alarms, choose **Export** > **All**.	-

----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.

NOTE

On the home page, you can customize the alarm bar chart to display only critical alarms, major alarms, minor alarms, and warning alarms. The display times changes with the the display times on the alarm panel.

Copyright © Huawei Technologies Co., Ltd.

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.

----End

5.4.3 Monitoring Alarms in the Topology View

The topology view allows you to monitor the alarms of NEs real time.

Prerequisites

You have the operation rights for **Current Alarms Management**.

Context

In the topology 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.

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.

Step 4 In the NE management window, view the active alarms of the NE.

----End

5.4.4 Monitoring Alarms in the NE Monitoring List

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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 **Optional:** Set search criteria to search for NEs.

1. In the **Resource Management** window, set **Search by** and **Search criteria**.
2. Click **Search**.

Step 3 **Optional:** In the **Resource Management** window, select an NE or a subnet.

Step 4 In the NE list on the right of the **Resource Management** window, click in the **Operation** column where the target NE is located.

Step 5 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.

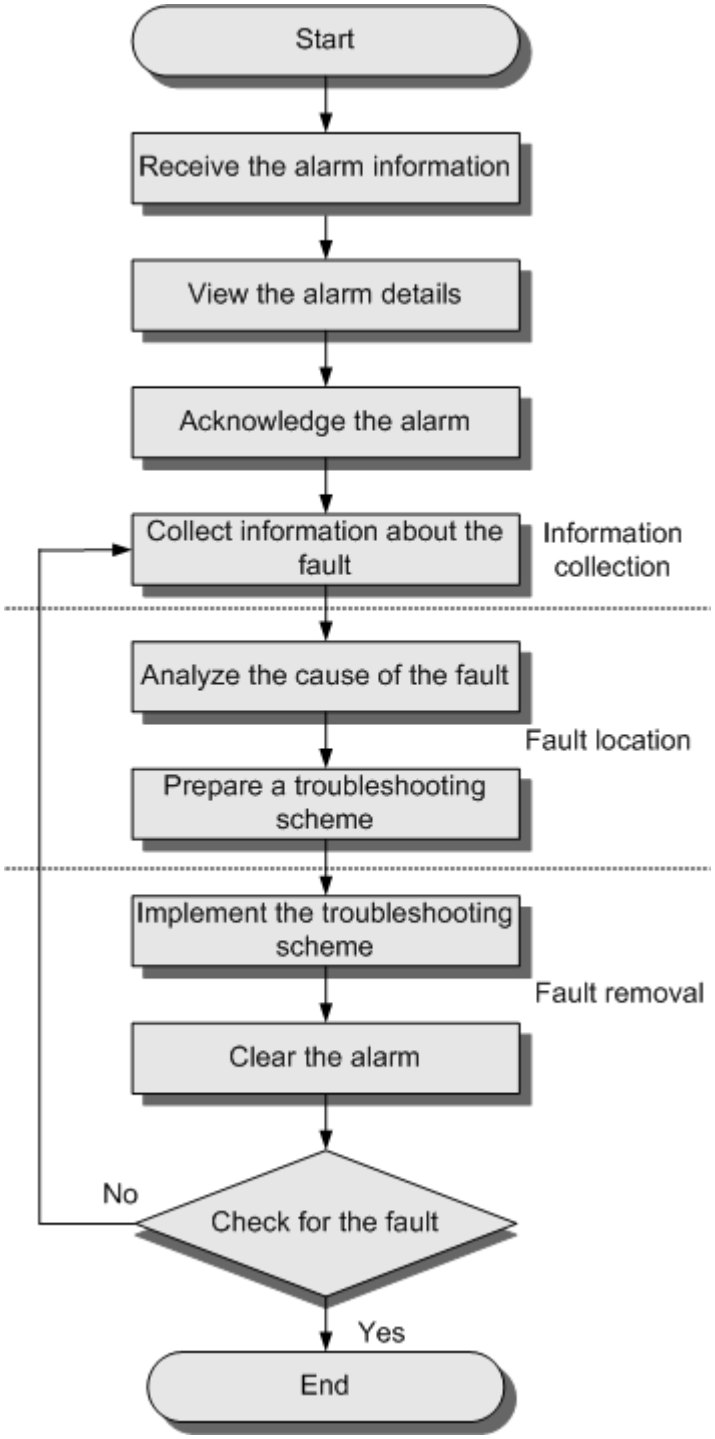
5.4.5.1 Procedure for Handling Alarms

This topic describes the procedure for handling alarms in the eSight.

Copyright © Huawei Technologies Co., Ltd.

Flow Chart of Handling Alarms

Figure 5-3 Procedure for handling alarms



Copyright © Huawei Technologies Co., Ltd.

Procedure Description

Table 5-4 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. For details about how to configure an alarm notification mode, see **5.2 Setting Remote Alarm Notifications**.
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	Analyze the symptom 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.

Copyright © Huawei Technologies Co., Ltd.

Table 5-5 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 is expired, you can learn why the alarm is generated based on the alarm name.
Object instance	Indicates the location information. The location information helps quickly find the alarm causes and analyze how to handle the alarm.
Severity	Indicates the severity of a fault. Alarm severities are classified into critical, major, minor, and warning.
Proposed repair actions	Allows you to view the fault rectification suggestion and helps you quickly locate and resolve the fault.
Number of occurrences	Indicates the number of occurrences of an alarm.
Alarm source	Indicates the NE where an alarm is generated.
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, **Uncleared** or **Cleared**.
Cleared by	Indicates the user who manually clears an alarm, for example, user **admin**. When the alarm is automatically cleared, the parameter is empty.
Acknowledge status	Indicates the acknowledgement status of an alarm, for example, **Unacknowledged** or **Acknowledged**.
Acknowledged time	Indicates the time on which the acknowledge status of an alarm changes.
Alarm serial number	Indicates the serial number of an alarm. The serial number uniquely identifies an alarm record in the eSight.
Equipment alarm serial number	Indicates the serial number of a piece of equipment. The equipment SN uniquely identifies an alarm of the equipment.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Clear method	Indicates the methods of clearing an alarm. This parameter can be set to **ADAC** or **ADMC**. ● **ADAC** ADAC indicates an ADAC fault. After an ADAC fault is rectified, the system automatically detects the rectification and reports a clear alarm. ● **ADMC** ADMC indicates an ADMC fault. After an ADMC fault is rectified, the system cannot detect the rectification and report the clear alarm. You need to clear the alarm manually.
Clear type	Indicates the clearing type of an alarm.
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.
NE name	Indicates the name of the NE that generates an alarm.
NE type	Indicates the type of an NE. Each NE has a unique type.
Event type	Indicates the type of an alarm 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 the alarm that the threshold is exceeded. **NOTE** You can set thresholds for performance alarm counters and SLA alarm counters.
Notification ID	Indicates the notification ID of an alarm. The notification ID is included in the reported alarm information (including alarm generation, alarm clear, acknowledgement 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**.

Copyright © Huawei Technologies Co., Ltd.

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.

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.

----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.

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.

----End

Copyright © Huawei Technologies Co., Ltd.

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.

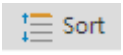
5.5.1 Querying a Historical Alarm

You can quickly find the desired historical alarms based on specified search criteria.

Prerequisites

You have the operation rights for **Browse Historical Alarms**.

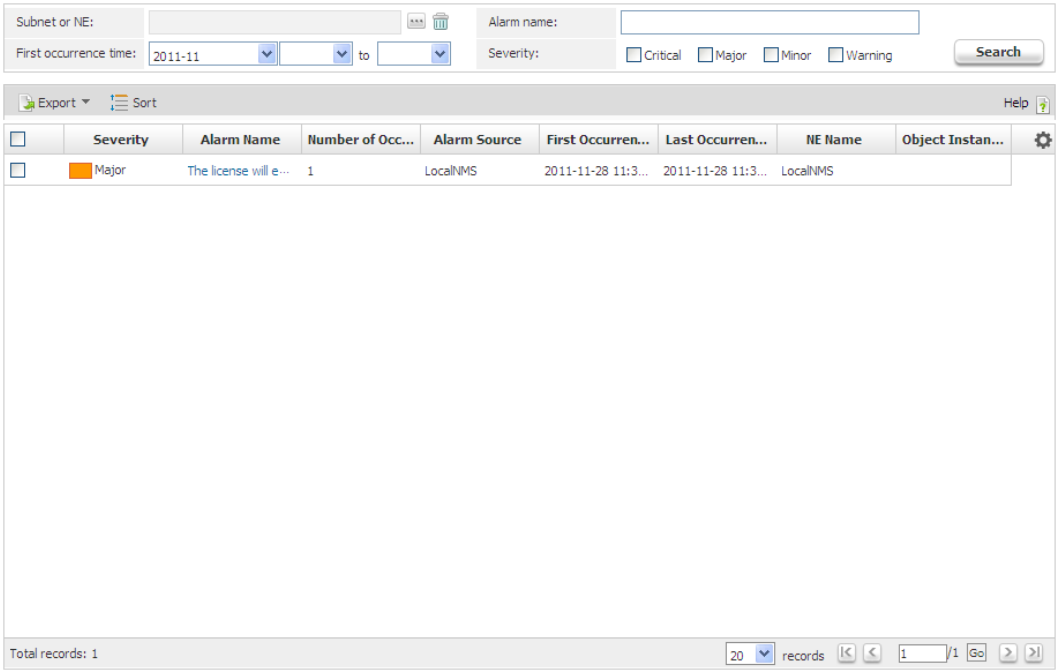
Context

- 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.

Step 2 **Optional:** In the **Historical Alarms** window, set the search information in the search bar and click **Search**.



Copyright © Huawei Technologies Co., Ltd.

- **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.

Step 3 In the **Historical Alarms** window, you can perform the following operations.

Querying Historical Alarms	Operation Method
Alarm Details	1. Click **Alarm Name**. 2. In the **Alarm Details** dialog box, view the alarm severity, possible causes, and rectification suggestion.
Export	Select one or more alarms and choose **Export** > **Selected Records** to export the alarm information. **NOTE** If you want to export all alarms, choose **Export** > **All**. 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 view the notification sent from the 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.

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.

Copyright © Huawei Technologies Co., Ltd.

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.

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 Sort to sort alarms in the **Sort** dialog box.

Procedure

Step 1 Choose **Fault** > **Masked Alarms** from the main menu.

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**: set the first time of masking the alarm.
- **Severity**: select the severity of a masked alarm.

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.

Copyright © Huawei Technologies Co., Ltd.

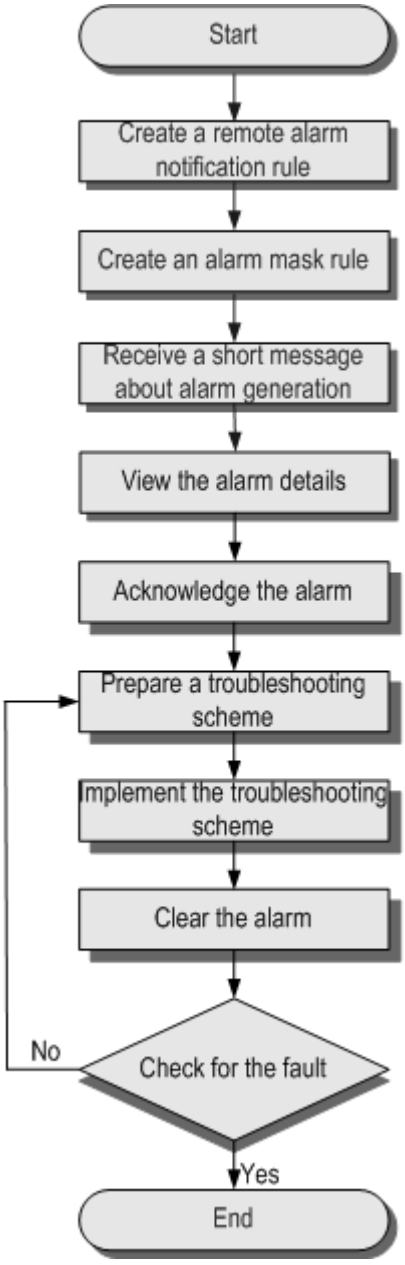
Context

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 5-4**.

Figure 5-4 Procedure



Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

- Time: all time

4. Click **Next**. Under **Alarm Sources** step, click **Add Alarm Sources**.
5. Under **Subnets** in the **Add Alarm Sources** dialog box, select the subnet to which NE B belongs. Under **Alarm Sources**, 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

Copyright © Huawei Technologies Co., Ltd.

6 Performance Management

About This Chapter

Performance management enables network maintenance personnel to monitor the network or service running status periodically. By performance management, network maintenance personnel can enhance network performance in a timely manner to ensure proper running of the entire network.

Copyright © Huawei Technologies Co., Ltd.

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 Performance Management Concepts**. 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

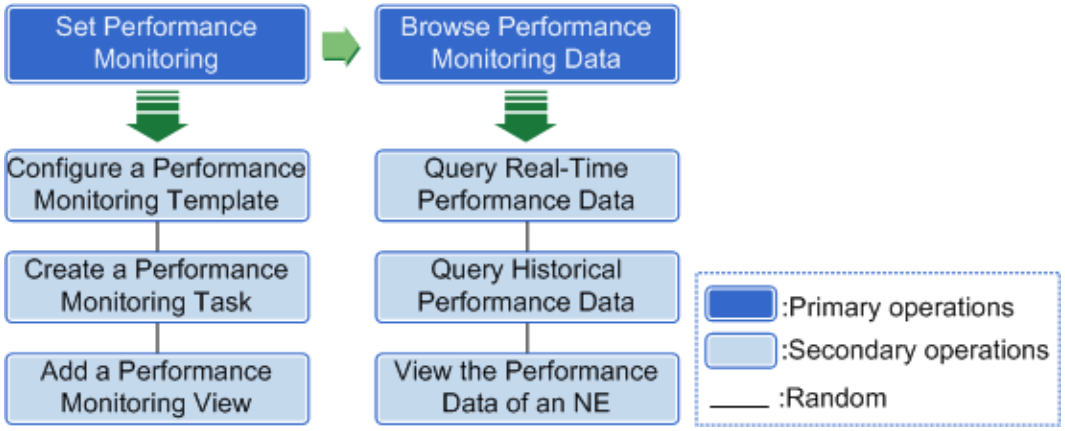


Table 6-1 describes the performance management operations.

Table 6-1 Performance management operations

Operation	Description	Navigation Path
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.	**Performance** > **Template Configuration**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
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.	**Performance** > **Monitoring Configuration**
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.	**Performance** > **Monitoring View**
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.	**Performance** > **Monitoring View**
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.	**Performance** > **Historical Data**
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.	**Resource** > **Resource Management**

6.2 Performance Monitoring Process

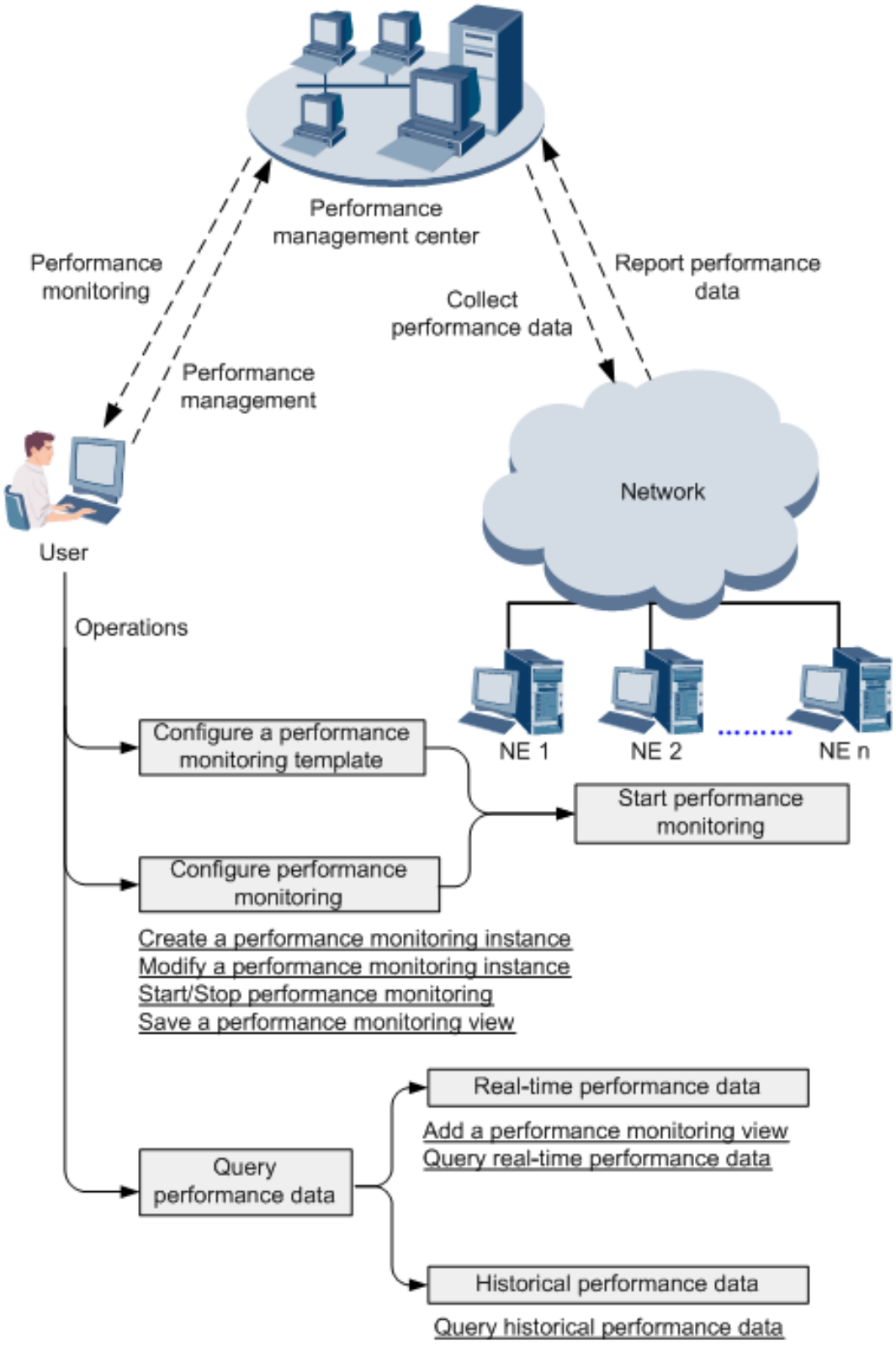
The eSight collects performance data on managed NEs, and displays the collection result for users to analyze. This topic describes the performance monitoring process.

Performance Monitoring Process

Figure 6-2 shows the performance monitoring process. The two sides connected to the eSight are users and NEs. After users enable performance monitoring, the eSight collects performance data of NEs and presents the data for viewing.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Performance monitoring process



Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

Step 2 In the navigation tree on the left of the **Template Configuration** window, select an NE type. All performance indicators of this NE type are displayed in collapsed mode on the right pane.

Step 3 Click  to expand the performance counters.

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.

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 setting the indicator attributes, you can set to enable the template for referencing the settings of the performance monitoring template.

Step 7 Click **Apply** to deliver the performance monitoring template (including the performance monitoring task) to NEs.

----End

Result

If the alarm threshold is set, when the condition of generating an alarm is met, the system 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.

Copyright © Huawei Technologies Co., Ltd.

Step 2 In the **Monitoring Configuration** window, click **Create**.

Step 3 Select a managed object.

1. On the **Create a performance monitoring task** page, click **Select Managed Objects**.
2. In the **Select Managed Objects** dialog box, select a subnet from **Subnets**.
3. Select an object in **Managed Objects**, and 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**.
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.

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.
2. In the **Select Measurement Objects** dialog box, select measurement objects.
   - Select measurement indicators for a measurement object:
     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**.

Copyright © Huawei Technologies Co., Ltd.

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 indicators for a measurement object:

a. In the **Select Measurement Objects** dialog box, select measurement objects from the measurement objects provided by the eSight by default.

b. Click  . In the displayed text box, enter the measurement object information such as the phone number.

Click  to delete the measurement object. You cannot delete the measurement objects provided by the eSight by default.

c. Click **OK**.

NOTE

You can manually enter measurement counters only for performance monitoring tasks in which the measurement object type is **Unspecified measuring objects**. To set the measurement object type, choose **Customize Device** > **NE Management Capability** > **Performance Indicator**, and set **Measurement Object Type** to **Unspecified measuring objects**.

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 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 creating a performance monitoring task, 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. 1. In the **Monitoring Configuration** window, select one or more tasks, and click **Modify**. 2. In the **Modify Properties** dialog box, modify the indicator attributes, such as, the threshold of generating an alarm. **CAUTION** After the thresholds are changed, all previous alarms are cleared.
Deleting a Performance Monitoring Task	You can delete unnecessary tasks to ensure sufficient memory and proper running of tasks on the server. In the **Monitoring Configuration** window, select one or more tasks, and click **Delete**.

Copyright © Huawei Technologies Co., Ltd.

Setting Performance Monitoring Task	Operation Method
Starting a Performance Monitoring Task	You can start a performance monitoring task to enable the eSight to monitor performance indicators and collect data, and report alarms. In the **Monitoring Configuration** window, select one or more tasks whose **Collection Status** is **Stopped**, and click **Start**.
Stopping a Performance Monitoring Task	You can stop the tasks that do not require attention to ensure sufficient memory and proper running of tasks on the server. In the **Monitoring Configuration** window, select one or more tasks, and click **Stop**.

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.

Procedure

- Create a performance monitoring view on the main page.
  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, and select a managed object in **Managed Object**.
  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.
  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**.

Copyright © Huawei Technologies Co., Ltd.

4. In the **Add Monitoring View** window, set the view name, and click **OK**.
5. 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	You can modify the performance monitoring view to meet management requirements. 1. In the **Monitoring View** window, click  of the monitoring view. 2. In the **Modify Monitoring View** window, modify the view name, and add or delete indicator instances in the view.
Deleting a Performance Monitoring View	You can delete unnecessary performance monitoring views to release resources for creating more views. In the **Monitoring View** window, click  of the monitoring view.

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.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Click to display the proper 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.

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.

Step 4 In the **Select Object Type** dialog box, click **OK**.

The managed object list in the **Select Managed Object** dialog box dynamically displays all managed objects of this type.

Step 5 Select a subnet in **Subnets** and select one or more managed objects of the subnet in **Managed Objects**. 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.

Step 7 **Optional:** Set the curve diagram to show the performance monitoring data.

1. On the **Data Graph** tab page, click **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.

   You can select a maximum of six object instances. In the diagram, performance indicators of object instances are represented by curves in different colors.

----End

Follow-up Procedure

On the **Data Table** tab page, click **Export All Data** to save the collected measurement data in a local .csv file.

Copyright © Huawei Technologies Co., Ltd.

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.
  2. In the **Resource Management** window, select an NE.
  3. Click in the **Operation** column of the NE to access the NE management window.
- Access the NE management window through the **Performance Management** entry.
  1. Choose **Performance** > **Monitoring Configuration** from the main menu.
  2. In the performance monitoring list of the **Monitoring Configuration** window, click the name of the target monitoring task in the **Managed Object** column.

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.

   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.

Copyright © Huawei Technologies Co., Ltd.

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.

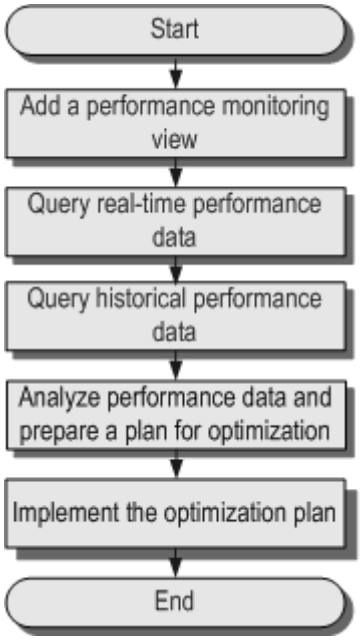
Context

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 6-3**.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 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

Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

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

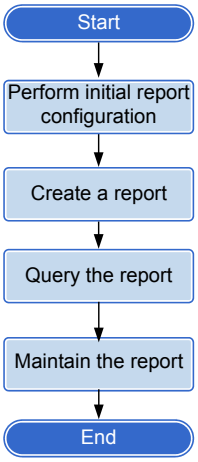


Table 7-1 describes the report management operations.

Table 7-1 Operation description

Operation	Description
1. **Perform initial report configuration**	eSight configures the report system by default. Customers can customize configuration items such as the report storage area, logo, and data sources as required. ● Configure the report storage area. ● Customize the logo of report customers. ● Configure data sources of monitored reports.
2. **Create a report**	eSight generates reports based on report tasks, automatically stores periodical reports to the report storage area, and sends reports to customers by email.
3. **Query the report**	You can view report content.

Copyright © Huawei Technologies Co., Ltd.

Operation	Description
4. **Maintain the report**	You can maintain report tasks as follows: ● Modifying a report task ● Configuring the report storage area ● Exporting reports ● Managing report task status

7.2 Setting the Report System Parameters

Customers can customize configuration items such as the report storage area, logo, and data sources as required.

7.2.1 Setting a Data Source

When the data source monitored and eSight server are not on the same device, you can set the data source from which eSight obtains data to generate a report.

Context

When the upper-layer eSight is to monitor the lower-layer eSight, you must set the report data source on the upper-layer eSight as the database of the lower-layer eSight.

Procedure

Step 1 Choose **Reports** > **Report System Configuration** from the main menu.

Step 2 Select **Data Sources** and click **Create**. In the window that is displayed, set parameters related to the data source.

Step 3 Click **Test Connection**. After the test, click **OK**.

----End

Follow-up Procedure

To specify the data source to a design file, do as follows:

1. Choose **Reports** > **Report Task Manager** from main menu.
2. Click **Create**, select a design file, and click  . Set the data source of the design file and click **OK**.

7.2.2 Configuring the Report System

Configure the space of the report storage area and customer information by means of report system configuration.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Reports** > **Report System Configuration** from the main menu.

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**.

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.

Step 2 Click **Create** and select a design file.

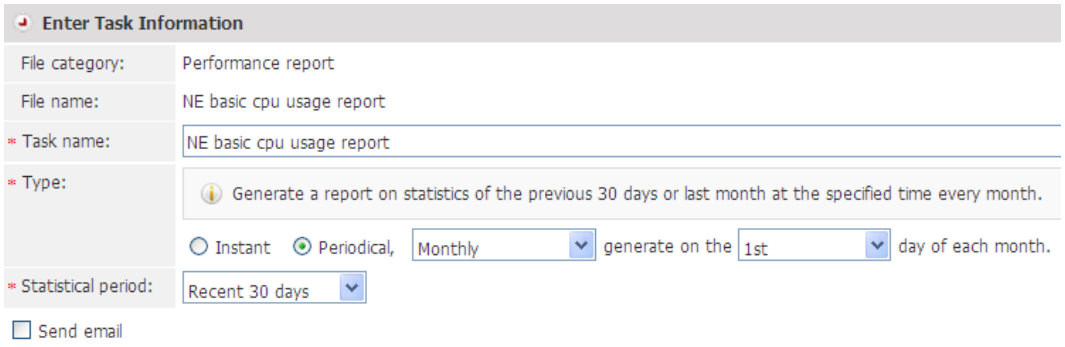
TIP

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.

Step 3 **Optional:** Click as required to set the data source of the design file and click **OK**.

Step 4 Click **Next** and set the following parameters as required.



Copyright © Huawei Technologies Co., Ltd.

Table 7-2 Parameter Description

Parameter	Description
Type	● Instant: Create an instant report. An instant report is generated when an instant task is created and executed manually. ● Periodical: Create a periodical report. A periodical report is generated according to the period set in the task created. **NOTE** By default, eSight generates reports at 04:00 every day. You can change the time for generating periodical reports in the ***eSight server installation directory*\AppBase\bin\runtime.center\config\report\report_conf.xml** file. Then you must restart eSight for the change to take effect.
Statistical period	You can set the statistical period of the periodical report in either of the following ways: Take a monthly report as an example. The report is created on May 11, 2011. If the statistical period is set to **Recent 30 days**, data from April 11, 2011 to May 10, 2011 is collected. If the statistical period is set to **Last month**, data from April 1, 2011 to April 30, 2011 is collected.

Step 5 **Optional:** Select **Send email** to set parameters related to email forward. A report is sent to a user.

Step 6 Set the task parameters and click **Finish**.

The values of the parameters vary with the design file.

----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.

Step 2 View reports.

1. For a periodical report, click  after the report. In the window that is displayed, you can view the report information.
2. For an instant report, click  after the report. In the window that is displayed, you can view the report information.

----End

7.5 Maintaining the Report System

Periodically maintain the report system as required.

Copyright © Huawei Technologies Co., Ltd.

7.5.1 Modifying a Report Task

Modify a report task as required.

Procedure

Step 1 Choose **Reports** > **Report Task Manager** from main menu.

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**, click .

Step 4 In the **Modify Task** window, modify parameters of the report tasks and click **Save**.

----End

7.5.2 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.

Step 2 Select **Reports Disk Usage**, modify **Max.capacity(MB)**, and click **Save**.

Step 3 Choose **Reports** > **Report Task Manager** from main menu.

Step 4 For a periodical report task, click , select the reports to be cleared, click **Export**, and select the file format of the reports to be exported. 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.

Step 5 Click **Delete** as required to delete the reports in the storage area.

----End

7.5.3 Managing Report Task Status

Periodically maintain the report system as required.

Procedure

Step 1 Choose **Reports** > **Report Task Manager** from main menu.

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.

Copyright © Huawei Technologies Co., Ltd.

- For a periodical report task, click  to disable the task.
- For an instant report task, click  to execute the task immediately.

----End

Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

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

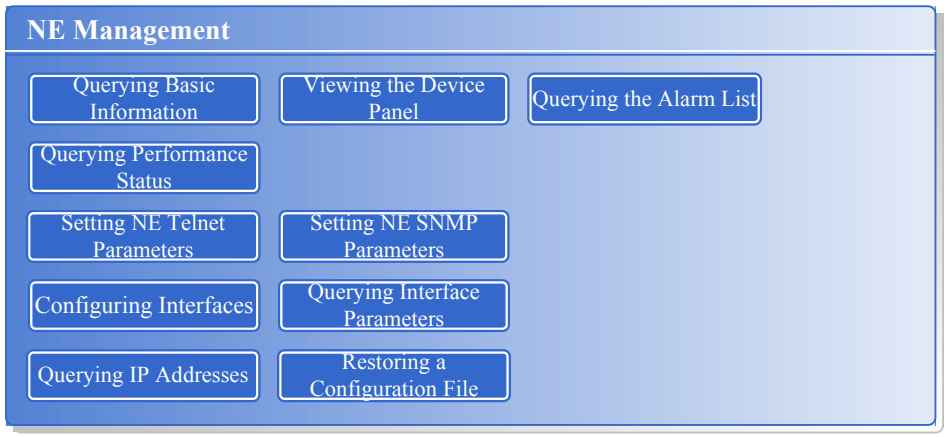


Table 8-1 describes the NE management operations.

Table 8-1 Operation description

Operation	Description	Access
Querying Basic Information	Queries basic NE information.	**Resource** > **Resource Management**
Viewing the Device Panel	Views slot, board, sub-board, and port parameters on the device panel.	**Resource** > **Resource Management**
Querying the Alarm List	Queries the current alarm information.	**Resource** > **Resource Management**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Access
Querying Performance Status	Queries performance data.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
Configuring Interfaces	Activates and deactivates interfaces and changes interface aliases.	**Resource** > **Resource Management**
Querying Interface Parameters	Queries interface information including the interface index, description, IP address, type, status, rate, and alias.	**Resource** > **Resource Management**
Querying IP Addresses	Queries NE and interface IP addresses during service configuration and network planning.	**Resource** > **Resource Management**
Restoring a Configuration File	Restores an NE configuration file that is corrupted.	**Resource** > **Resource Management**

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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 Query the basic information of the NE in the **Basic Information** pane on the right.

Copyright © Huawei Technologies Co., Ltd.

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.

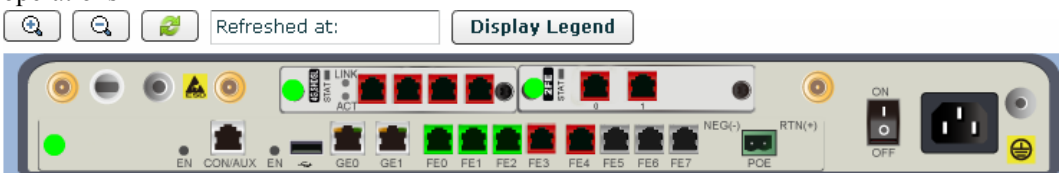
Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **View** > **Device Panel**.

Step 3 Move the cursor to a board, subcard, or port. eSight displays the parameter information of the board, subcard, or port.

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:

- **Browse Alarm**: View alarms on an NE to understand the NE operating status. For details, see **5.4.4 Monitoring Alarms in the NE Monitoring List**.

Copyright © Huawei Technologies Co., Ltd.

- **Create New Style**: Draw a picture to customize a device panel. For details, see **12.6.4 Customizing the Device Panel**.
- **Bind Style**: Bind a created device panel with an NE.

----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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **View** > **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	Click **Lock**. The alarms in the current list are locked. If the alarms in the current list are locked, note that: ● Newly reported alarms can be displayed in the current alarm list only after you click **Unlock**. ● 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. **NOTE** ● If you acknowledge or clear an alarm when you click **Lock**, the alarm can be updated to the historical alarm list only when you click **Unlock**. ● If an alarm is available, you can select the alarm. ● If an alarm is unavailable, you cannot select the alarm because the check box is dimmed.
Unlock	Click **Unlock**. The eSight reports alarms to the alarm list automatically.
Search	You can perform a search by using either of the following methods: ● Click **Refresh** without setting any search criteria. All alarms are displayed in the current list. ● Select a search scope from **Search in** when the window is locked, and click **Search**.

Copyright © Huawei Technologies Co., Ltd.

Operation Name	Operation Method
Acknowledge	Select one or more alarms and click **Acknowledge**. **NOTE** ● If the alarm is acknowledged, **Acknowledge User** displays the user who acknowledges the alarm. ● If the alarm is unacknowledged, **Acknowledge User** displays  .
Unacknowledge	Select one or more alarms and choose **More** > **Unacknowledge**. **NOTE** After an alarm is unacknowledged, its status is changed from Acknowledged to Unacknowledged.
Clear	Select one or more uncleared alarms and click **Clear**. **NOTE** ● The background color of cleared alarms is green. ● The background color of uncleared alarms is white.
Alarm Mask	1. Select an alarm. Then click in the **Operation** column and choose Shield Alarms**.** 2. In the **Alarm Mask** dialog box, set the rule name, shielding time, masking time, and location information. Click **OK**. **NOTE** ● In the current alarm window, the newly created alarm mask rule is in enabled status by default. ● 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. ● You cannot set a mask rule for a performance alarm or cleared alarm.
Locate to Topo	Select an alarm and click  . **NOTE** eSight locates the NE in the managed object that generates the alarm in the topology view.
Alarm Details	Select an alarm and click **Alarm Name**. The **Alarm Details** dialog box displays the name, cause, and solution for the selected alarm.
Alarm Logs	Select an alarm and click **Number of Repetitions**. The **Alarm Logs** dialog box displays the alarm log related to this alarm record.
Export	Select one or more alarms and choose **Export** > **Selected Records** to export the alarm information. If you want to export all alarms, choose **Export** > **All**.

Copyright © Huawei Technologies Co., Ltd.

----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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **View** > **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 Configuring Web NMS of NE

eSight integrates NE Web NMS to enable NE configuration.

Prerequisites

The NE support web NMS.

Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Config** > **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.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The Telnet parameters on eSight and NE are the same.

A device is added to eSight.

Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

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

Step 3 On the right of the window, set the Telnet parameters, and then click **Test**. 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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

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

Copyright © Huawei Technologies Co., Ltd.

- **Timeout interva(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**. 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 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.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

SNMP write permission is set.

Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **Interface Manager**.

Step 3 Click **Synchronize**. The **Progress** dialog box is displayed. After the synchronization task is complete, click **OK**.

Step 4 Click  to set parameters related to an interface.

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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **IP Address**.

Copyright © Huawei Technologies Co., Ltd.

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.

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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **Configuration File**.

Step 3 Perform **restoration** in **Operation**.

----End

Follow-up Procedure

Backing Up NE Configuration Files, refer to **11.3.2 Backing Up NE Configuration Files Manually**.

Copyright © Huawei Technologies Co., Ltd.

9 Service Management

About This Chapter

eSight provides the function of managing Wireless Local Area Network (WLAN), the IP Security (IPSec) Virtual Private Network (VPN), Service Level Agreement(SLA)and BGP/MPLS VPN services.

Copyright © Huawei Technologies Co., Ltd.

9.1 IPSec VPN Service Monitoring and Management

eSight monitors and manages the IPSec VPN 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.

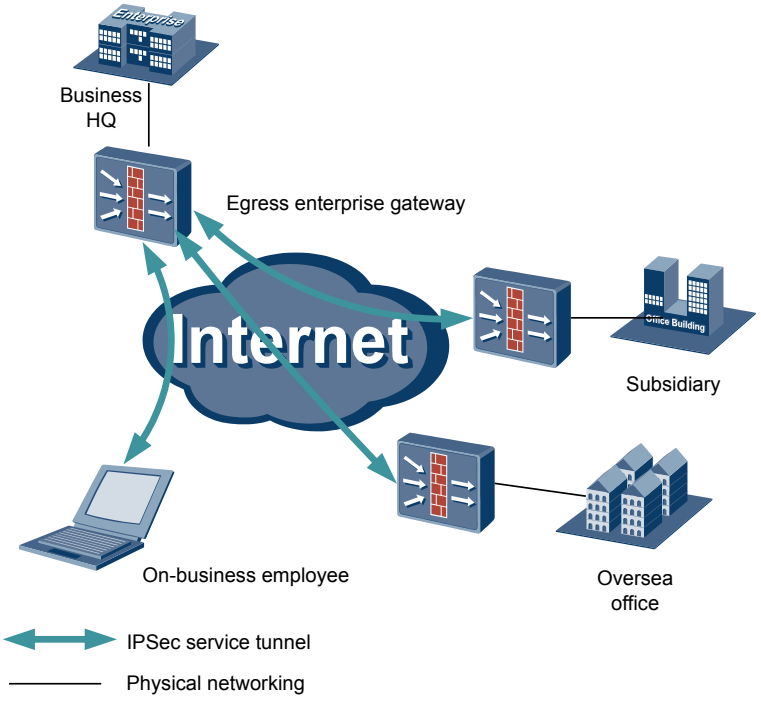
9.1.1 IPSec VPN Application

IPSec VPN establishes secure communication tunnels for enterprises and users in different geographic areas. This helps prevent data from being illegally viewed or tempered 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 9-1**. 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 9-1 Typical application scenario of IPSec VPN



Copyright © Huawei Technologies Co., Ltd.

9.1.2 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 9-2 shows the overview of IPSec VPN management operations. For details, click operations in the overview.

Figure 9-2 Overview of IPSec VPN Management Operations

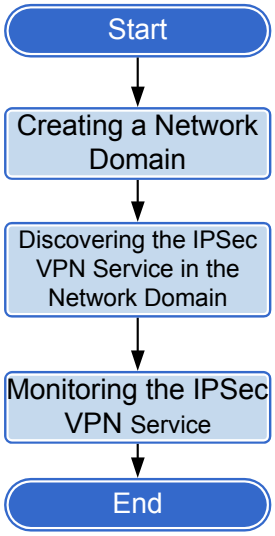


Table 9-1 describes the IPSec VPN management operations.

Table 9-1 Operation description

Operation		Description
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.
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.
Monitoring the IPSec VPN Service	**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.

Copyright © Huawei Technologies Co., Ltd.

Operation		Description
	Querying the Running State of the IPSec VPN Service	When maintaining the IPSec service, you must query the running status periodically.

9.1.3 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.

Step 2 In the basic information pane, click **Create**.

Step 3 In the window that is displayed, set **Network Domain** and **Description**.

Step 4 Click **Add**, select an NE or multiple NEs from the NE list, and click **OK**.

----End

9.1.4 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.

Step 2 In the navigation tree on the left, choose **IPSec VPN Resource Management** > **Network Domains**. On the right, click **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.

----End

9.1.5 Monitoring the IPSec Service

This topic describes how to monitor the performance of the IPSec network domain.

9.1.5.1 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **IPSec VPN Management** from the main menu.

Step 2 In the navigation tree on the left, choose **IPSec VPN Resource Management** > **Network Domains**. On the right, click **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.

Tunnel status in the topology view:

- Green: up
- Red: down

----End

9.1.5.2 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.

Step 2 In the navigation tree on the left, choose **IPSec VPN Resource Management** > **Network Domains**. On the right, click **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**.

----End

9.2 WLAN Management

This topic describes the basic concepts and configuration methods of the WLAN.

9.2.1 Basic Concepts of WLAN

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.

Copyright © Huawei Technologies Co., Ltd.

Related Concepts of the WLAN

- AP: 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: controls and manages all APs on a WLAN, and provides authentication services for WLAN users by interacting with an authentication server.
- Control And Provisioning of Wireless Access Points (CAPWAP): transmits management packets and data packets between APs and ACs.
- Service Set Identifier (SSID): The wireless terminal can scan all the networks and then selects a specified SSID to access a specified wireless network.
- Virtual Access Point (VAP): 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.

9.2.2 WLAN 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.

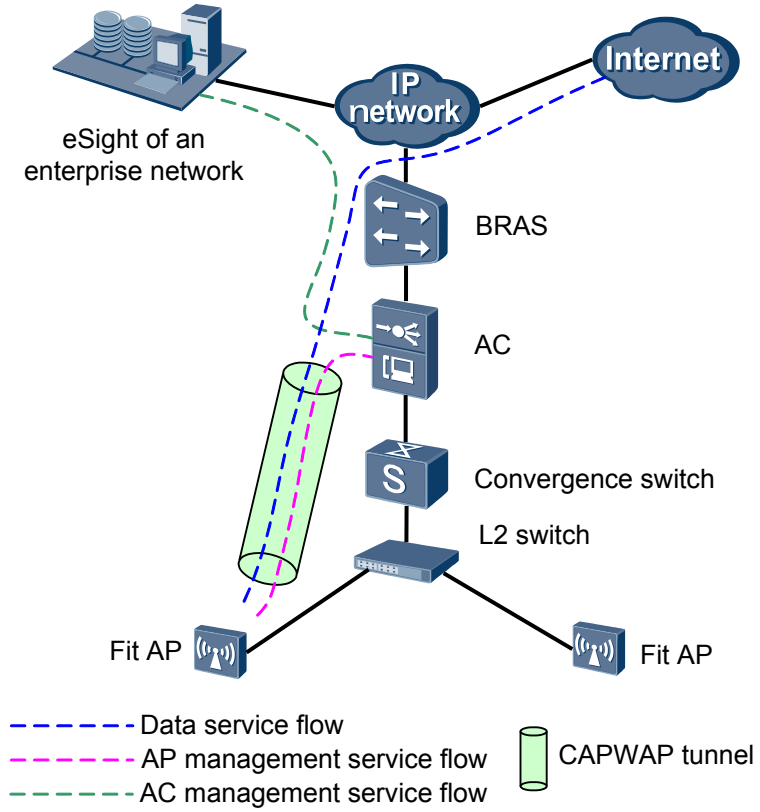
Two configuration scenarios exist based on whether data services are encapsulated in CAPWAP tunnels.

- 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 9-3**. All the data services and AP management services are encapsulated in CAPWAP tunnels. Different Virtual Local Area Networks (VLANs) distinguish different services.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-3 Data services encapsulated in CAPWAP tunnels



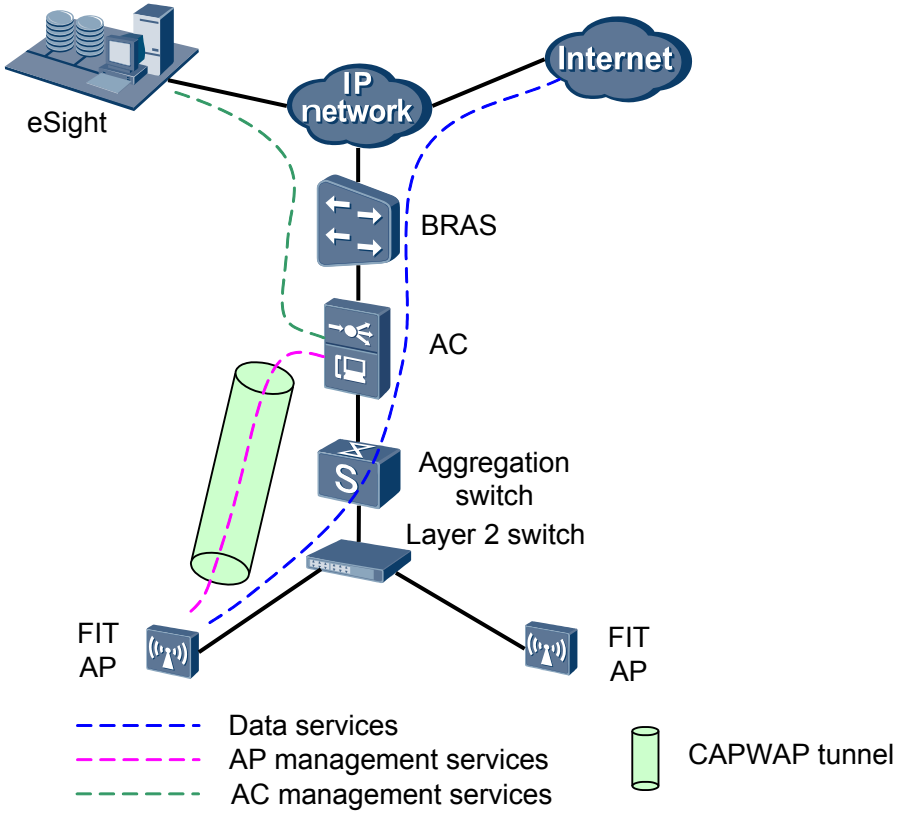
In this mode, you only need to configure management VLANs on switches in advance. You do not need to configure data VLANs. The AP management VLANs connect APs to ACs.

- 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 9-4**. 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.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-4 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.

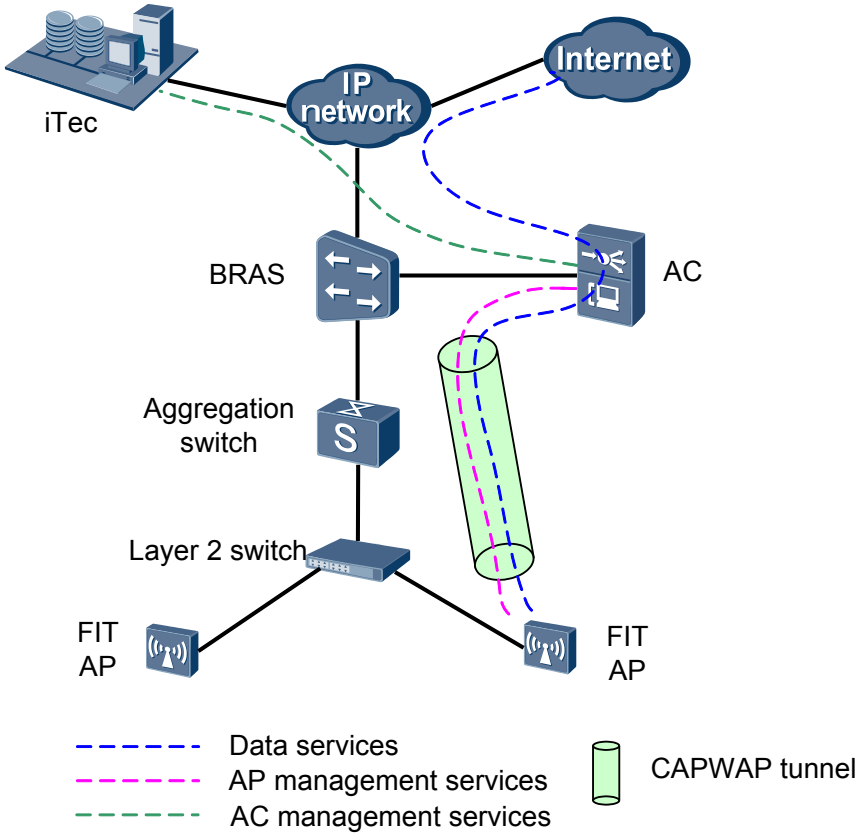
Two configuration scenarios exist based on whether data services are encapsulated in CAPWAP tunnels.

- 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 9-5**. All the data services and AP management services are encapsulated in CAPWAP tunnels. Different VLANs distinguish different services.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-5 Data services encapsulated in CAPWAP tunnels



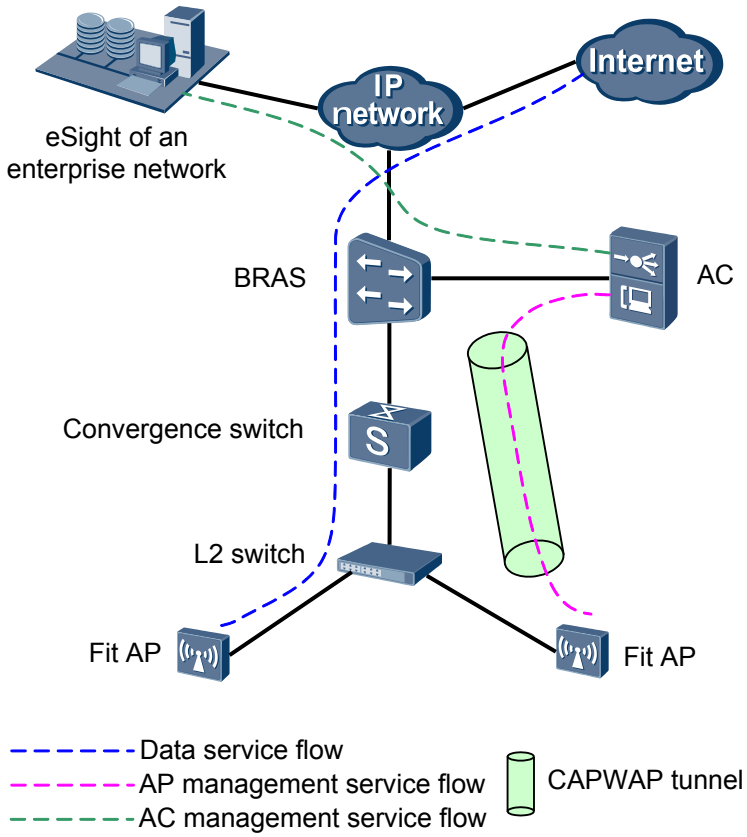
In this mode, you only need to configure management VLANs on switches in advance. You do not need to configure data VLANs. The AP management VLANs connect APs to ACs.

- 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 9-6** shows the networking diagram.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-6 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 9-2** compares the direct connection network with the hung beside network.

Copyright © Huawei Technologies Co., Ltd.

Table 9-2 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.

9.2.3 Overview of WLAN Configuration Operations

This topic describes the WLAN configuration operations.

Figure 9-7 shows the overview of WLAN configuration operations.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-7 Overview of WLAN configuration operations

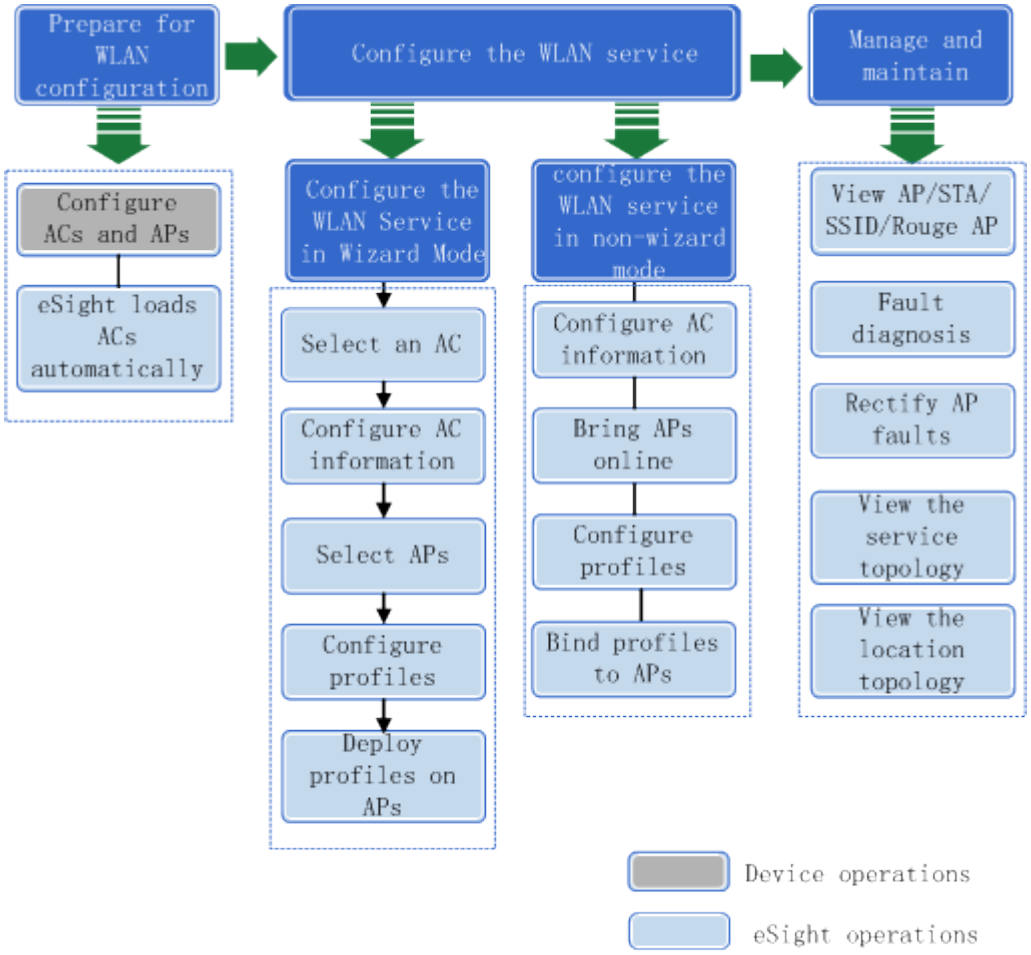


Table 9-3 lists the WLAN configuration operations.

Table 9-3 WLAN configuration procedure

Stage	Operation Description
Prepare for WLAN configuration	Prepare for WLAN configuration and management. ● Configure ACs and APs, and verify that the management channels and service channels between ACs and APs function properly. ● eSight loads ACs automatically.

Copyright © Huawei Technologies Co., Ltd.

Stage	Operation Description
Configure the WLAN service	**9.2.4.1 Configuring the WLAN Service in Wizard Mode** describes the detailed procedure for configuring the WLAN service. To configure the WLAN service in non-wizard mode, proceed as follows: 1. Configure AC basic information: Create an AC, and set the AC source interface, authentication mode, and forwarding type. 2. Bring APs online. 3. Configure profiles: Configure the AP profile, radio profile, and ESS profile. 4. Bind profiles to APs: Bind profiles to APs to complete the service configuration for APs.
Manage and maintain the WLAN service	● View AP/STA/SSID/Rouge AP: eSight allows you to browse the detailed information about APs, stations (STAs), SSIDs, and rogue APs on the entire network. ● Fault diagnosis: eSight provides the fault diagnosis function for you to locate service faults. ● 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. ● View the service topology: You can view ACs, APs, rogue APs, STAs, and the logical relationship between them in the service topology. ● 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.

9.2.4 WLAN Operation

This topic describes how to manage the WLAN service.

9.2.4.1 Configuring the WLAN Service in Wizard Mode

This topic describes how to configure the WLAN service in wizard mode.

Copyright © Huawei Technologies Co., Ltd.

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**.

Step 2 In the navigation tree, choose **Service Management** > **Configuration Wizard**.

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**, and **Forwarding type**.

- 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.

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**.

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**.

NOTE

You can bind multiple ESS profiles to an AP.

Step 7 **Optional:** Select **Add to whitelist**, and click **Deploy**.

Step 8 When the service is deployed, click **Finish**.

----End

9.2.4.2 Setting Basic AC Information

Set the basic AC information to prepare for eSight to load APs.

Prerequisites

SNMP write permission is set.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **WLAN Management**.

Step 2 In the navigation tree on the left, choose **Resource Service** > **AC**.

Step 3 In the pane on the right, click **Add**. In the displayed **Create AC** window, click **Select**. In the window that is displayed, select an AC and click **OK** to create an AC.

NOTE

To create an AC of the SPU type, ensure that the AC runs WLAN services.

Step 4 In the **Create AC** window, click **OK**. An AC is successfully created.

Step 5 Click  to set the basic parameters of the AC.

Step 6 After **Interface name**, click **Select**, select an interface, and click **OK**.

Step 7 Set **AP authentication mode** and **Forwarding type**.

NOTE

When **AP authentication mode** is set to **No authentication**, the AP is automatically connected to the WLAN.

When **AP authentication mode** is set to **MAC** or **SN**, a user must manually import the AP, create the AP in offline mode, add the AP MAC or SN to the whitelist, and determine the rogue AP in online mode.

When **Forward type** is set to **ESS**, the AP forwards user data in the mode specified by using the ESS profile bound with the AP.

When **Forward type** is set to **AP**, the AP forwards user data in the mode set by the AP.

----End

Follow-up Procedure

After the AC is configured, click **Name** and view the AC information in the **AC Information** window that is displayed.

9.2.4.3 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.

Copyright © Huawei Technologies Co., Ltd.

- 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **AC**. In the pane on the right, click **Name**.

Step 3 Add an AP in offline mode.

1. In the navigation tree on the left, choose **WLAN Management** > **AP** and click **Add**.
2. Set AP parameters.
   - After **AP region** or **AP profile**, click **Select** and set the parameters.
   - After **Radio profile** and **ESS profile**, click **Bind** to bind corresponding profiles.
   - Click **OK**.

Step 4 Add an AP to the whitelist.

1. In the navigation tree on the left, choose **WLAN** > **AP Whitelist** and click **Create**.
2. Under **AP Whitelist**, set **MAC** or **SN**.

Step 5 Add a unauthorized AP.

1. In the navigation tree on the left, choose **WLAN Management** > **Unauthorized AP** and click **Synchronize**.
2. Click a unauthorized AP and click **Confirm AP identities**.

----End

9.2.4.4 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **AC**. In the pane on the right, click **Name**.

Step 3 In the navigation tree on the left, choose **Manage Template** > **AP Profile**.

Step 4 Click **Create**. In the window that is displayed, set AP profile parameters.

Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK**. The new AP profile is displayed in the list.

NOTE

Click to modify AP profile parameters.

----End

9.2.4.5 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **AC**. In the pane on the right, click **Name**.

Step 3 In the navigation tree on the left, choose **Manage Template** > **RF Profile**.

Step 4 Click **Create**. In the window that is displayed, set RF profile parameters.

- When is set to, 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 is set to, 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.
- Bit 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.

NOTE

Click to modify RF profile parameters.

----End

9.2.4.6 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **WLAN Management**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **AC**. In the pane on the right, click **Name**.

Step 3 In the navigation tree on the left, choose **Manage Template** > **ESS Profile**.

Step 4 Click **Add**. In the window that is displayed, set ESS profile parameters.

- **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.

NOTE

Click  to modify ESS profile parameters.

----End

9.2.4.7 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **AC**. In the pane on the right, click **Name**.

Step 3 In the navigation tree on the left, choose **Wlan Management** > **AP Region**.

Step 4 Click **Create**. In the window that is displayed, set AP region parameters.

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

Copyright © Huawei Technologies Co., Ltd.

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 5 Click **OK**. The new AP region is displayed in the list.

NOTE

Click  to modify AP region parameters.

Click  to set an AP region as a default AP region.

----End

9.2.4.8 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **AC**. In the pane on the right, click **Name**.

Step 3 In the navigation tree on the left, choose **Wlan Management** > **AP**.

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**.

Step 5 On the **Bind Profile** page, set the profile bound to the AP as required.

TIP

Some APs may support multiple radios. You can bind the radio profile and ESS profile to APs at multiple radios.

----End

9.2.5 WLAN Maintenance Tasks

This topic describes tasks involved in WLAN maintenance and management.

9.2.5.1 Viewing AC Information

After configuring the WLAN service, you can view basic information about all ACs, AP information, region information, AP and AC alarms, and online user statistics.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **WLAN Management**.

Step 2 In the navigation tree, choose **Resource Management** > **AC**.

Step 3 Click the name of an AC on the page that is displayed to view basic information about the AC, AP information, region information, AP and AC alarms, and online user statistics.

----End

Follow-up Procedure

The system provides statistics within one hour by default and refreshes statistics every 30 minutes. You can set the time range and refresh interval.

1. Click  in the upper right corner of **Online Users Statistics**.
2. Click **Setting**.
3. Select **Time range** and **Refresh Interval**.
4. Click **OK** to save the setting.
   The system displays the result based on the configured values.

9.2.5.2 Viewing AP Information

After an AP is connected to a WLAN, you can query all AP information managed by eSight.

Procedure

Step 1 Choose **Network Application** > **WLAN Management**.

Step 2 In the navigation tree, choose **Resource Management** > **Fit AP**.

Step 3 In the pane on the right, click **Synchronize** to synchronize the AP information to eSight.

Step 4 On the **Fit AP** tab page, click **Name** to view the AP parameter setting.

Table 9-4 Important parameters

Parameter	Description
Data forwarding mode	● Direct forwarding: The AP sends the original packets directly. ● Tunnel forwarding: The AP encapsulates packets to the CAPWAP tunnel and forwards the packets to an upper-layer network to ensure packet forwarding security.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
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. When the channel frequency is 20 MHz, the transmission rate is low but you can select many channels, effectively reducing the interference. When the channel frequency is approximately 40 MHz, the transmission rate is high but you can select only a few channels. Bandwidths **40-MHz** and **40+MHz** have the same transmission rate but different available channels.
Channel Value	Number of managed channels. Setting principle: 2.4 GHz frequency band ● 20 MHz: 1-13 ● 40 MHz-minus: 5-11 ● 40 MHz-plus: 1-7 5 GHz frequency band ● 20 MHz: 149, 153, 157, 161, 165 ● 40 MHz-minus: 153, 161 ● 40 MHz-plus: 149, 157
Operating Channel Value	Number of current operating channels. **NOTE** In a radio profile bound to an AP, if **Channel Mode** is set to **Manual**, set **Operating Channel Value** to the same value as that of **Channel Value**. If **Channel Value** is set to **Automatic**, the parameter value is allocated by eSight.
Operating power	Current operating power. **NOTE** The operating power determines the signal coverage scope displayed in the location topology.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Transmit Power Level	Value range: 0-15 Value **0** 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. To save power consumption, you can shut down excess antennas.

----End

9.2.5.3 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **STA**.

Step 3 Click **Synchronize** to browse information on all radio users on the live network.

----End

9.2.5.4 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **SSID**.

Step 3 Click **Synchronize** to browse all SSID information on the live network.

----End

Copyright © Huawei Technologies Co., Ltd.

9.2.5.5 Managing 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**.

Step 2 In the navigation tree on the left, choose **Resource Management** > **Rogue AP**.

Step 3 Click **Synchronize** to browse all rogue APs on the live network.

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.
RSSI	RSSI is short for Received Signal Strength Indicator.

----End

9.2.5.6 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**.

Step 2 In the navigation tree, choose **WLAN topology** > **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.

Copyright © Huawei Technologies Co., Ltd.

- 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

9.2.5.7 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**.

Step 2 In the navigation tree, choose **WLAN topology** > **Location topology**.

Step 3 Double-click  to access the WLAN service topology.

Step 4 Select a proper diagnosis method based on the site scenario.

Copyright © Huawei Technologies Co., Ltd.

Diagnosis Method	Application Scenario	Operation
Perform the ping operation on an AP	● Check the connectivity by pinging a network device on an AP. ● Check the connectivity between an AP and the FTP server during an upgrade.	1. Select an AP, click  , and select **Ping**. 2. In the **AP Ping** window, enter the target device IP address, and click **ping**. The ping result is displayed.
Perform the ping or tracert operation on the tunnel between an AP and an AC	● 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. ● Ping is used to check whether a fault occurs on the tunnel between an AP and AC or test the network quality. ● Tracert is used to locate a network fault after it is detected by the ping function.	1. Select the tunnel between an AP and AC, click  , and select **Ping** or **Tracert**. 2. In the window where the ping or tracert result is displayed, click **OK**.

----End

9.2.5.8 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**.

Step 2 In the navigation tree, choose **Resource Management** > **AC**. Then click 

in the **Operation** column on the right of the window.

Copyright © Huawei Technologies Co., Ltd.

Restart the AP, restore the AP to factory settings, or replace the AP based on the site scenario.

Step 3 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**.

Step 4 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**.

Step 5 Replace an AP.

1. Select an AP, and click  .
2. Set **SN** and **MAC** for the new AP, and click **OK**.

----End

9.2.5.9 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**.

Step 2 In the navigation tree, choose **WLAN topology** > **Location topology**.

Step 3 Right-click in the location topology, and choose **Add Location**. In the dialog box that is displayed, set Layer 1 **subnet name**, and click **OK**.

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 Double-click the new location icon, and click **Set Background** on the shortcut icon bar. In the dialog box that is displayed, select **select image**, and select a proper image of the physical network environment based on the site scenario.

NOTE

An image can be in GIF, JPG, JPEG, or PNG format. The image size cannot exceed 2 MB.

Step 5 Right-click in the location topology, and choose **Add AP**. In the dialog box that is displayed, select the required APs, and click **OK**.

NOTE

You can add APs only in the lowest-layer location topology.

Step 6 Right-click in the location topology, and choose **Set scale**. Then set the start point, end point, actual distance between the two points, and click **OK**. After the setting is complete, check the

Copyright © Huawei Technologies Co., Ltd.

scale in the upper left corner of the topology background. It is recommended that the scale be smaller than the minimum value in **Table 9-5**.

The minimum value of the scale is provided based on the AP quantity and signal coverage, in meters. **Table 9-5** lists the minimum value of the scale.

Table 9-5 Minimum value of the scale

AP Quantity	Signal Strength	Signal Strength (Blocks)	Rate	Rate (Blocks)	Channel (Collision Domains)	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***.

Step 8 Click **Save the Position** on the shortcut icon bar.

----End

Follow-up Procedure

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 **Add Location**. **NOTE** After APs are added to a location topology view, no more locations can be added in it.

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Setting
Set Channel Color	Set colors for channels as required.	Right-click in the location topology, and choose **Set Channel Color**. **NOTE** All channels are displayed when **Display only operating channels** 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. **NOTE** 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. **TIP** You can view channel collisions by channel.	Right-click in the location topology, and choose **Display Signal Coverage**.
Hide Signal Coverage	Hide the signal coverage scope.	Right-click in the location topology, and choose **Hide Signal Coverage**.
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 **Set scale**. **NOTE** 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: ● Ensuring that the location topology view is consistent with the real network layout. ● Controlling signal attenuation.	Right-click in the location topology, and choose **Add Block**. **NOTE** 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.

9.2.6 Example: Typical WLAN Management Operations

This topic uses a configuration example to describe how to configure the WLAN service.

Copyright © Huawei Technologies Co., Ltd.

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

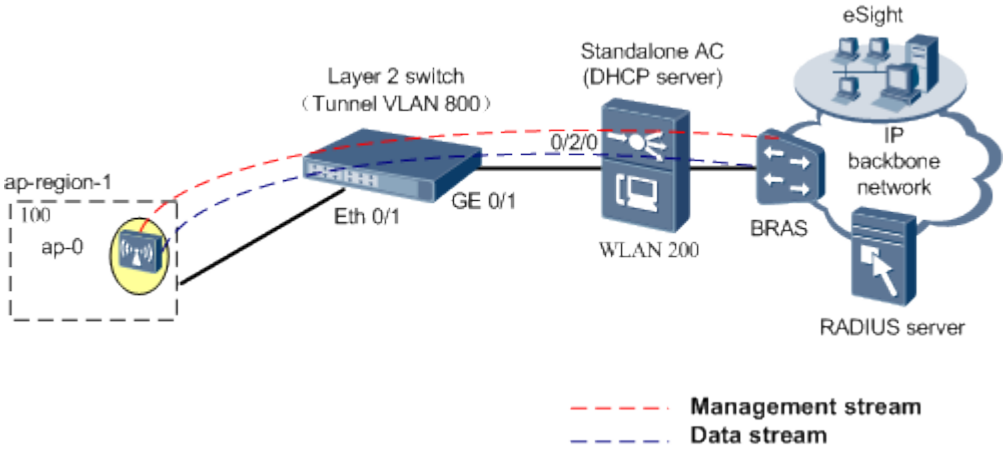
A network provider provides the WLAN service for the small region ap-region-1 through the AP ap-0.

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 9-8 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

Copyright © Huawei Technologies Co., Ltd.

- 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

- Radio 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

Copyright © Huawei Technologies Co., Ltd.

Configuration Procedure

NO.	Step	Description
1	Select an AC	Select a proper AC based on the data plan. **NOTE** 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

Copyright © Huawei Technologies Co., Ltd.

9.3 BGP/MPLS VPN Management

This topic describes terms, functions, and typical configuration examples of BGP/MPLS VPN management provided by eSight.

9.3.1 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.

9.3.1.1 Terms

This topic describes BGP/MPLS VPN terms to help you better monitor and manage the BGP/MPLS VPN service on eSight.

Table 9-6 lists the basic concepts.

Table 9-6 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. 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.

Copyright © Huawei Technologies Co., Ltd.

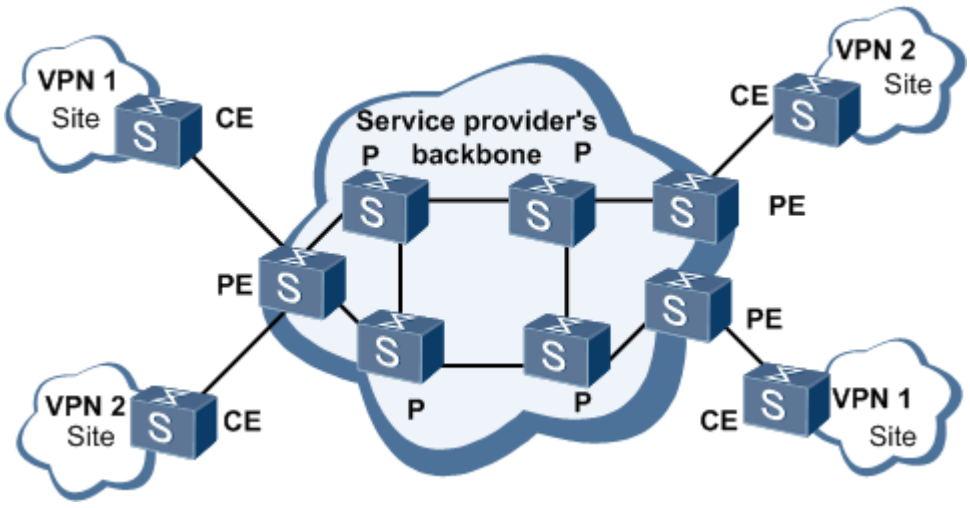
Concept	Description
VPN Target	VPN targets are used by VPN instances to control VPN member relationship and routing principles of directly connected sites and remote sites. Each VPN instance is associated with one or more VPN targets (a site can belong to different VPNs), which are of the following types: ● Export target: A local PE learns IPv4 routes from the directly connected site, 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. ● 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. VPN target attributes define the sites that can receive a VPN route, and the sites from which the PE can receive routes. 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.

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 9-9 shows the BGP/MPLS VPN basic model.

Figure 9-9 BGP/MPLS VPN basic model



Copyright © Huawei Technologies Co., Ltd.

9.3.1.2 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.

9.3.1.3 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

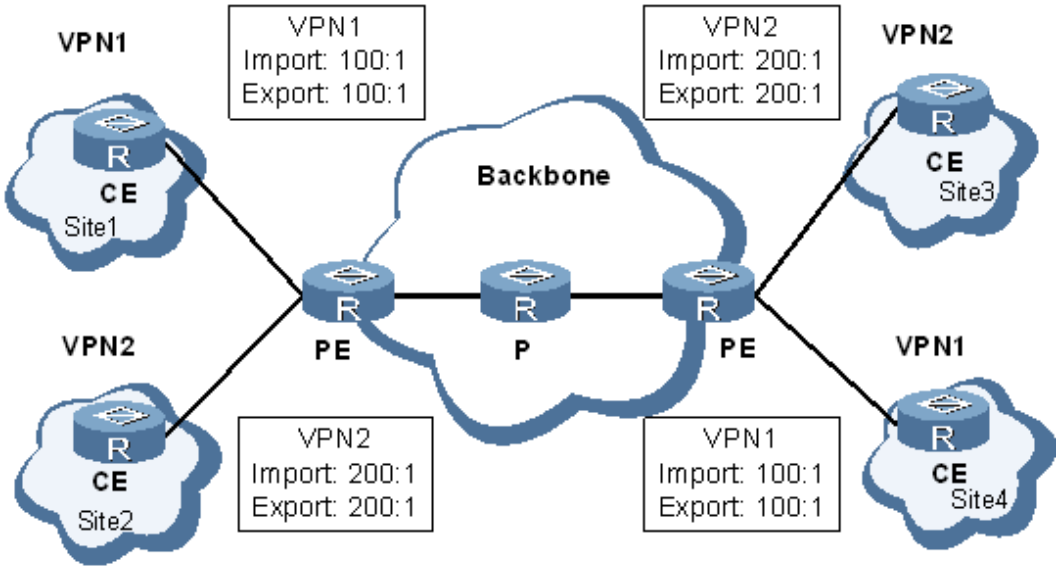
Full-Mesh Network

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 9-10 shows the Full-Mesh network.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-10 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.

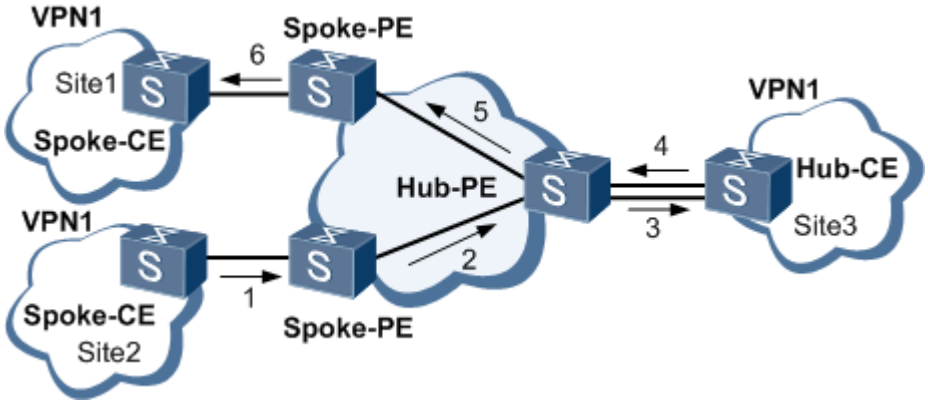
The configuration of a VPN target on a PE must comply with the following rules:

- 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 9-11 shows the Hub-Spoke network.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-11 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:

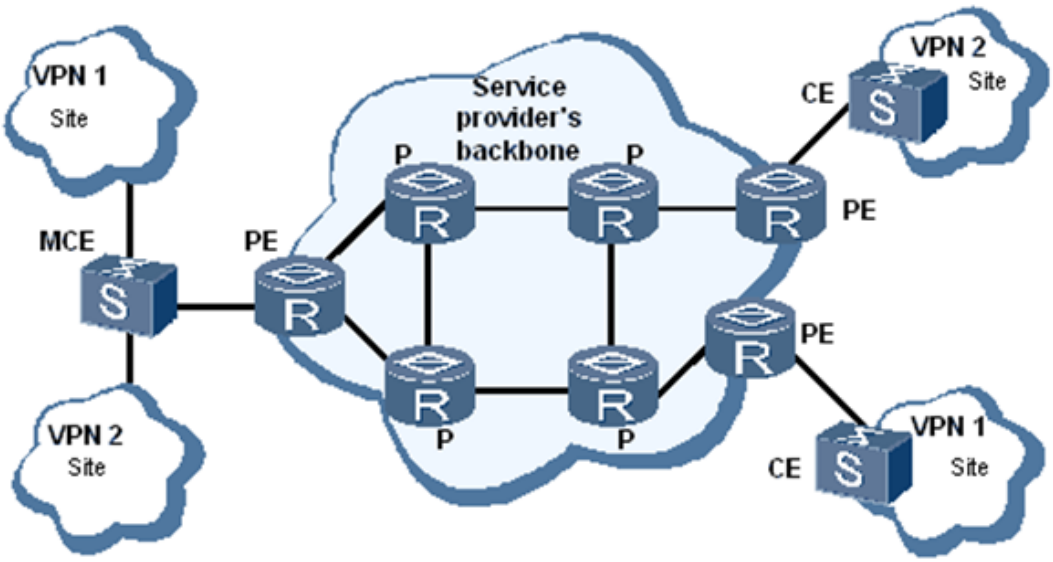
- Create and maintain an independent multi-VRF table for each VPN.
- Process all VPN services.

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 9-12 shows the MCE network.

Figure 9-12 MCE network



Copyright © Huawei Technologies Co., Ltd.

HoVPN Network

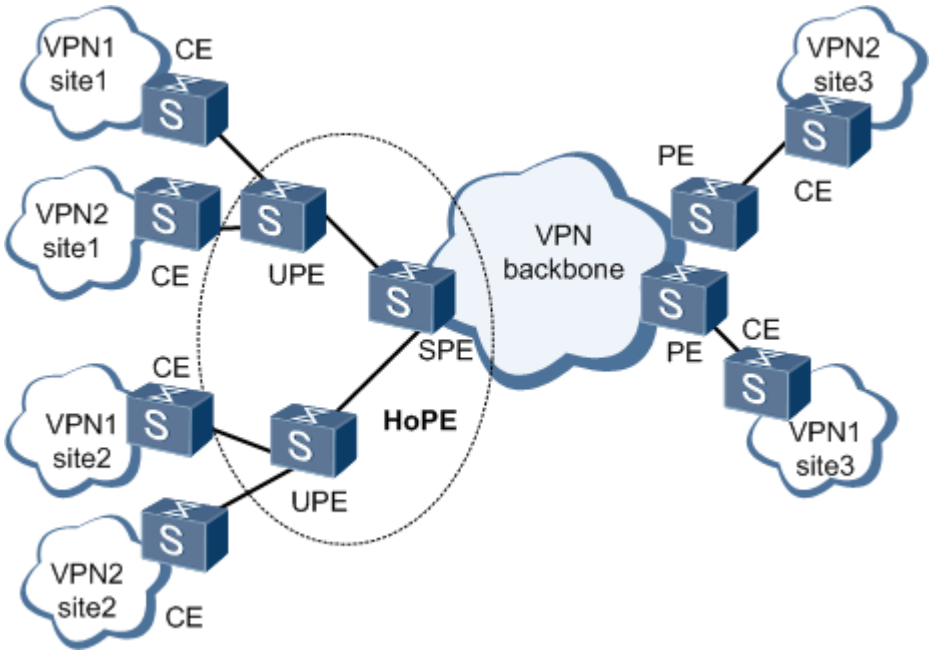
On a Hierarchy of VPN (HoVPN), the functions of a PE are distributed among multiple PEs. Playing different roles, the PEs form a hierarchical architecture and fulfill the functions of a centralized PE. An HoVPN is also called a Hierarchy of PE (HoPE).

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 9-13 shows the HoVPN network.

Figure 9-13 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

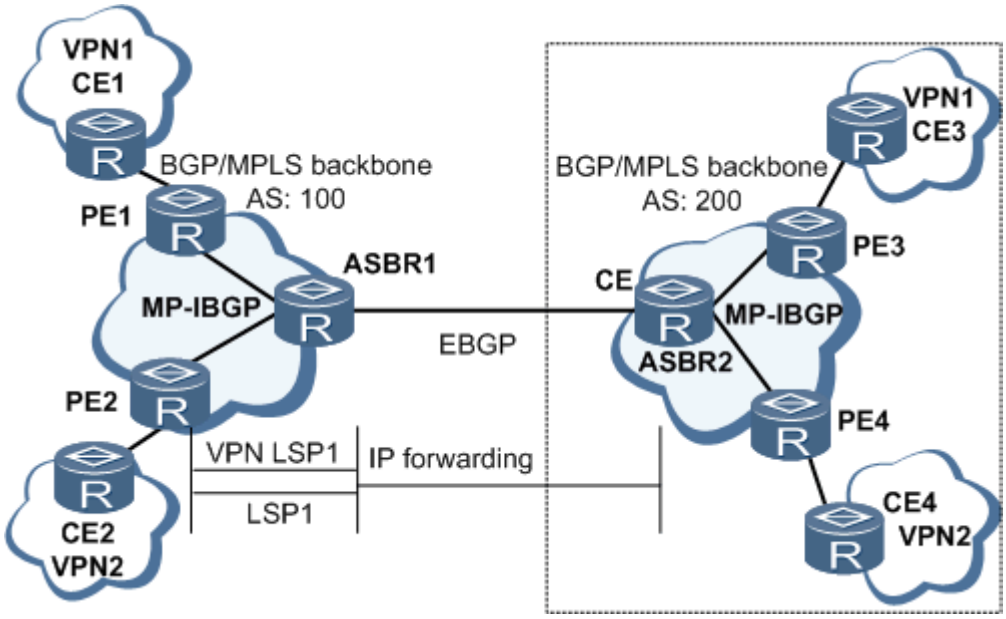
Copyright © Huawei Technologies Co., Ltd.

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 9-14 shows the Inter-AS VPN Option A network.

Figure 9-14 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.

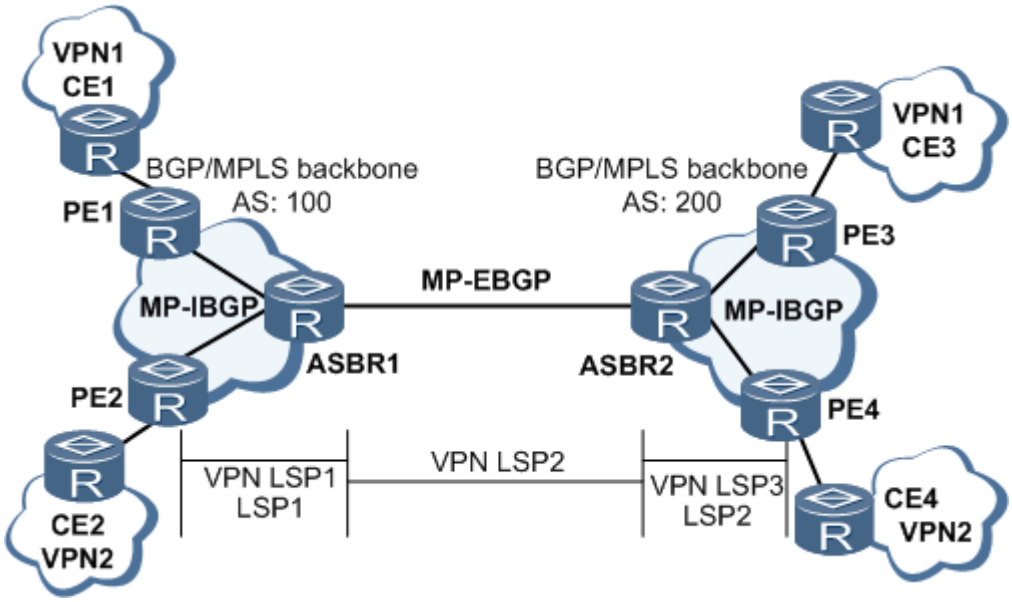
Inter-AS VPN Option B Network

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 9-15 shows the Inter-AS VPN Option B network.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-15 Inter-AS VPN Option B network



Comparison Between Options A and B

Table 9-7 lists the Comparison Between Options A and B.

Table 9-7 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.

Copyright © Huawei Technologies Co., Ltd.

9.3.2 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 9-16 shows the BGP/MPLS VPN management process.

Figure 9-16 BGP/MPLS VPN management process

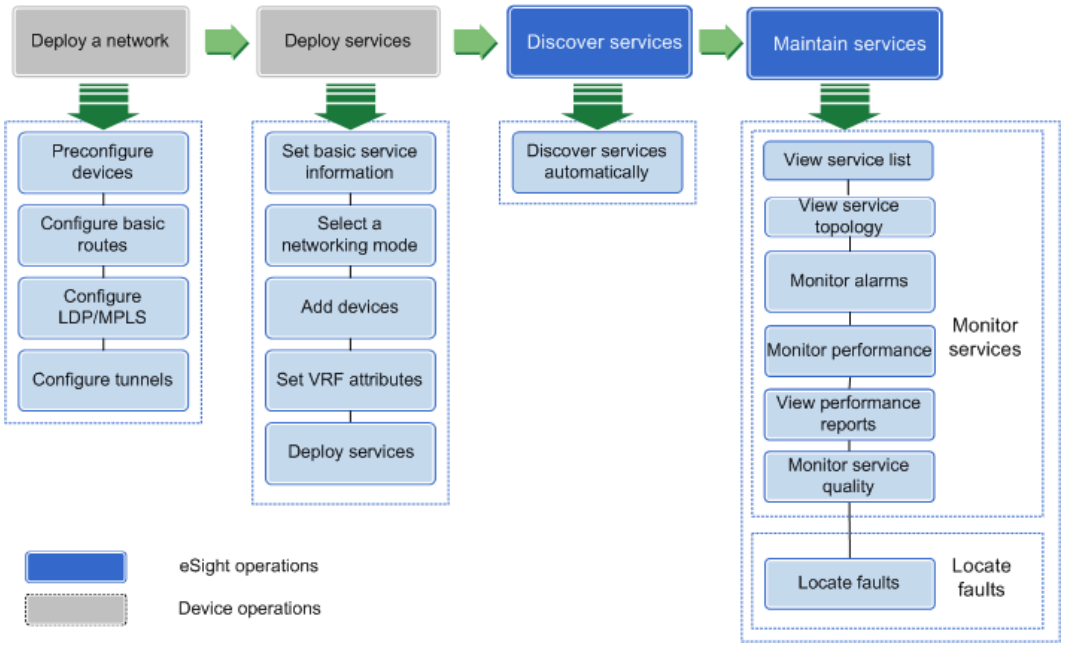


Table 9-8 lists the management process in detail.

Table 9-8 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	Monitor services	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.

Copyright © Huawei Technologies Co., Ltd.

Operation		Description
	Locate faults	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.

9.3.3 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.

9.3.3.1 Automatic Discovery Process

This topic describes the BGP/MPLS VPN automatic discovery process.

Figure 9-17 shows the automatic discovery flowchart.

Figure 9-17 Automatic discovery flowchart

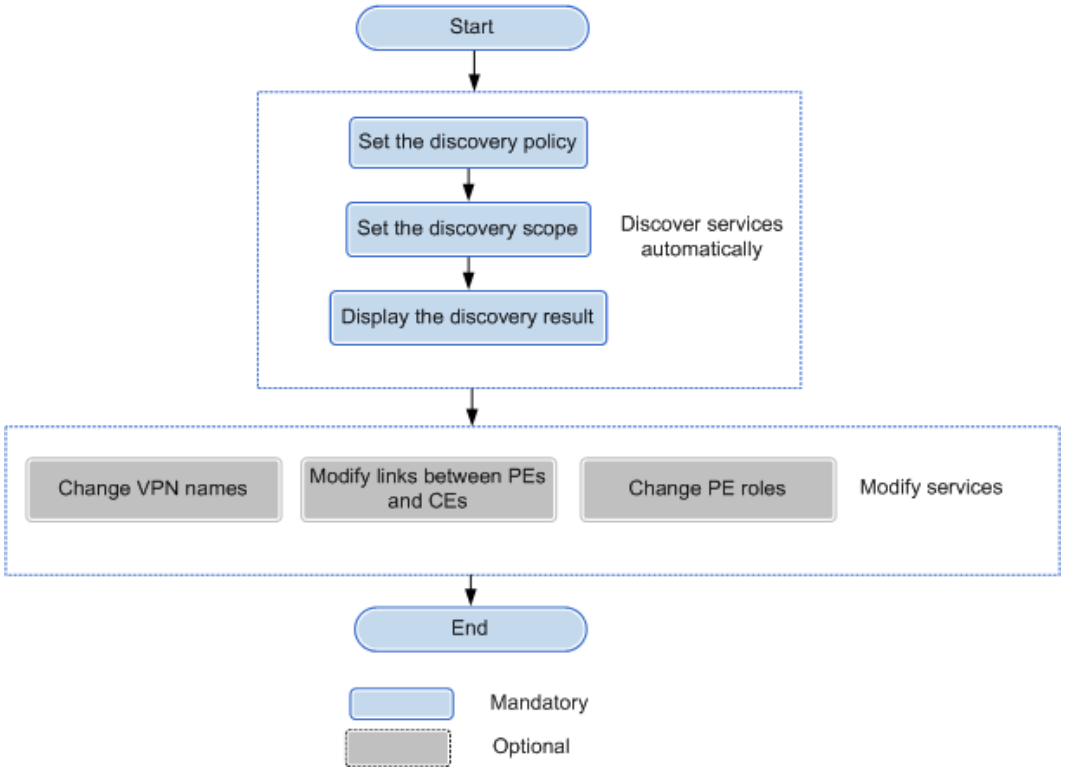


Table 9-9 lists the automatic discovery process in detail.

Copyright © Huawei Technologies Co., Ltd.

Table 9-9 Automatic discovery process

Operation	Description
Discover services automatically	Set the discovery policy and discovery scope to discover L3VPN services on devices that have completed network deployment and service deployment to eSight. Discover services automatically including: Set the discovery policy, Set the discovery scope, and Display the discovery result. 1. Set the discovery policy The discovery policy can be discovery by Discover by VRF connection or discovery by VRF name. You can use the policy of discovery by VRF name when VRF names are the same on VPN. 2. Set the discovery scope The discovery scope can be selected devices or global PEs/CEs. 3. Display the discovery result The discovery result includes the following information: L3VPN name, discovery status, and actual operation.
Modify services	Modify the following information about discovered services: L3VPN name, device role, and service link. Modify services including: Change the L3VPN name, Modify links between PEs and CEs, and Change the PE role. 1. Change the L3VPN name Change names of discovered L3VPNs. 2. Modify links between PEs and CEs 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. 3. Change the PE role You can change the PE role based on the site scenario. The values are **PE**, **UPE**, and **SPE**.

9.3.3.2 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.

Copyright © Huawei Technologies Co., Ltd.

- 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**.

Step 2 In the navigation tree, choose **Service Management** > **Service List**, and click **Auto Discover**.

Step 3 Select the discovery policy and discovery scope.

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.

Copyright © Huawei Technologies Co., Ltd.

- **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.

9.3.3.3 Modifying Services

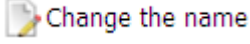
This topic describes how to change names, device roles, and service links for discovered L3VPN services.

Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

Procedure

Step 1 Choose **Network Application** > **BGP/MPLS VPN Management**.

Step 2 In the navigation tree, choose **Service Management** > **Service List**, click  choose 

, 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.

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**.

----End

Copyright © Huawei Technologies Co., Ltd.

9.3.4 Monitoring Services

This topic describes how to monitor the operating status of BGP/MPLS VPN services that are automatically discovered by eSight.

9.3.4.1 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**.

Step 2 In the navigation tree, choose **Service Management** > **Service List**.

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**.

----End

Follow-up Procedure

In the L3VPN service list, you can perform the following operations.

Operation	Operation Method
Enable an L3VPN service	Click Enable. The L3VPN service changes to the **Enabled** state.
Disable an L3VPN service	Click Disable. The L3VPN service changes to the **Disabled** state. **NOTE** An L3VPN service is interrupted after being disabled.
Delete an L3VPN service	Click Delete.

Copyright © Huawei Technologies Co., Ltd.

9.3.4.2 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.

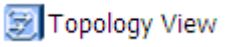
Prerequisites

L3VPN services have been discovered to eSight using the automatic discovery function.

Procedure

Step 1 Choose **Network Application** > **BGP/MPLS VPN Management**.

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, choose  and click 

.

  The **Topology View** page is displayed.
- In the navigation tree, choose **Service Management** > **Topology View**.

  The **Topology View** page is displayed.

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 9-18**.

  Figure 9-18 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 9-19**.

  Figure 9-19 Highest L3VPN alarm severity

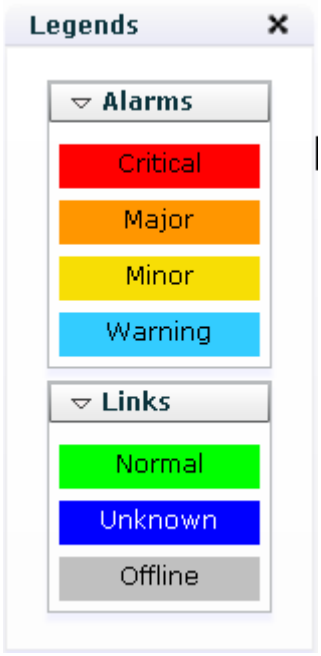
  NOTE

  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 9-20**. This helps you understand the alarm status and operating status of topology objects.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-20 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.

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.

Copyright © Huawei Technologies Co., Ltd.

- 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 9-21**.

Figure 9-21 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 9-22**. If an L3VPN alarm is generated in a region, the region is enclosed in a box.

Figure 9-22 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

9.3.4.3 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **BGP/MPLS VPN Management**.

Step 2 In the navigation tree, choose **Service Management** > **Region Management**.

Perform the following operations in the region management list as required:

1. Create a region: Click Create.
2. Modify a region: Click  in the **Operation** column.
3. Import a physical topology view. When subnets created in a physical topology view are imported to the region management page, devices on the subnets are also imported. To import a physical topology view, click Import Physical Topology.
4. Delete a region: Select a region, and click Delete.
5. View region information: Select a record in the **Subregion/Device** 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 Add Subregion. **NOTE** ● A subregion can be added only to an existing region or subregion. ● A region can contain a maximum of nine layers of subregions.
Switch regions for a device	Select a device in a region, and click Switch Region. **NOTE** Subregions cannot be switched to other regions.
Import a device	Click Import PE Device.
Delete a subregion or device	Select a subregion or device, and click Delete.
View region information	Select a record in the **Sub Region/PE Name** column, and view subregion details.

- Perform the following operations on the subregion details page as required.

Copyright © Huawei Technologies Co., Ltd.

Operation	Operation Method
Add a subregion	Click Add Subregion. **NOTE** ● A subregion can be added only to an existing region or subregion. ● A region can contain a maximum of nine layers of subregions.
Switch regions for a device	Select a device in a region, and click Switch Region. **NOTE** Subregions cannot be switched to other regions.
Import a device	Click Import PE Device.
Delete a subregion or device	Select a subregion or device, and click Delete.
View region information	Select a record in the **Sub Region/PE Name** column, and view subregion details.

9.3.4.4 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**.

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 View alarms. Current L3VPN alarms are displayed on the **VPN Alarm** page.

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.

Copyright © Huawei Technologies Co., Ltd.

- 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 9-23**.

  Figure 9-23 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

9.3.4.5 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**.

Step 2 Open the **Performance counter** page in either of the following ways:

1. In the navigation tree, choose **Service Management** > **Service List**. In the L3VPN service list, select an L3VPN service, and click  in the **Operation** column.

Copyright © Huawei Technologies Co., Ltd.

2. In the navigation tree, choose **Service Management** > **Topology View**. In the L3VPN service topology of the entire network, select an L3VPN service, click , and choose 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 9-10 lists measurement objects and counter groups that L3VPN services support.

Table 9-10 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.
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

9.3.4.6 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

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **BGP/MPLS VPN Management**.

Step 2 In the navigation tree, choose **Report Management** > **Report Management**.

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

9.3.4.7 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **BGP/MPLS VPN Management**.

Step 2 In the navigation tree, choose **Service Management** > **Service List**. Select an L3VPN service, and click 

.

Step 3 On the **SLA** page that is displayed, view **TOP Service Quality Compliance** and **SLA service list**.

----End

9.3.5 Dianosing 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 9-11** lists the scenarios for using different L3VPN diagnosis options or tools.

  Table 9-11 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 9-12**, **Y** indicates that a link supports a diagnosis option or tool.

Copyright © Huawei Technologies Co., Ltd.

Table 9-12 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	-	-	-
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**.

Step 2 In the navigation tree, choose **Service Management** > **Service List**. Select an L3VPN record, and click  .

The **Quick Diagnosis** window is displayed.

Step 3 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.

Step 4 Select a link that you want to diagnose.

Step 5 Select diagnosis options or tools in the **Diagnosis option/tool** area.

Click **Advanced**, and set diagnosis option parameters.

Copyright © Huawei Technologies Co., Ltd.

Step 6 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

9.3.6 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.

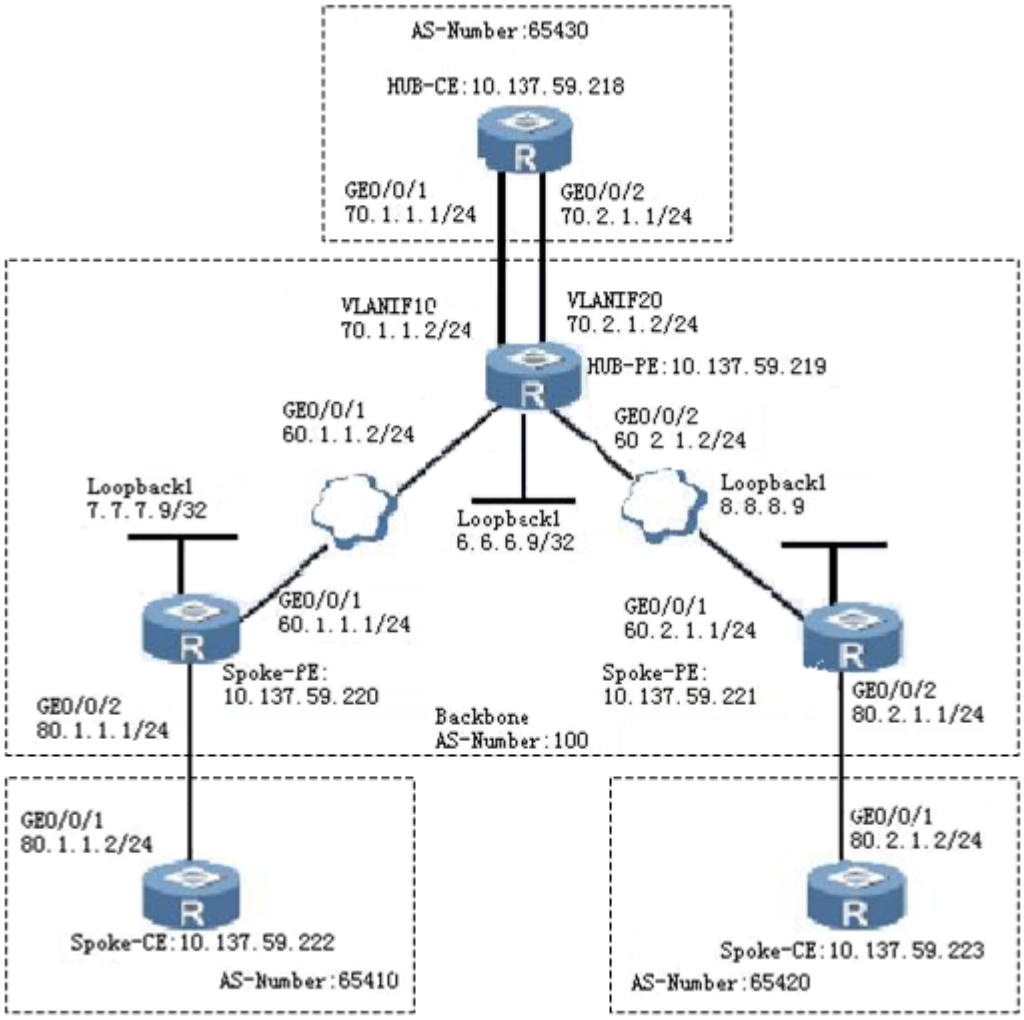
Network

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 9-24 shows Configuration network.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-24 Configuration network



Data Plan

Table 9-13 lists the Data Plan in detail.

Table 9-13 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

Copyright © Huawei Technologies Co., Ltd.

NE Name	NE Type	IP Address	Role	Location
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.

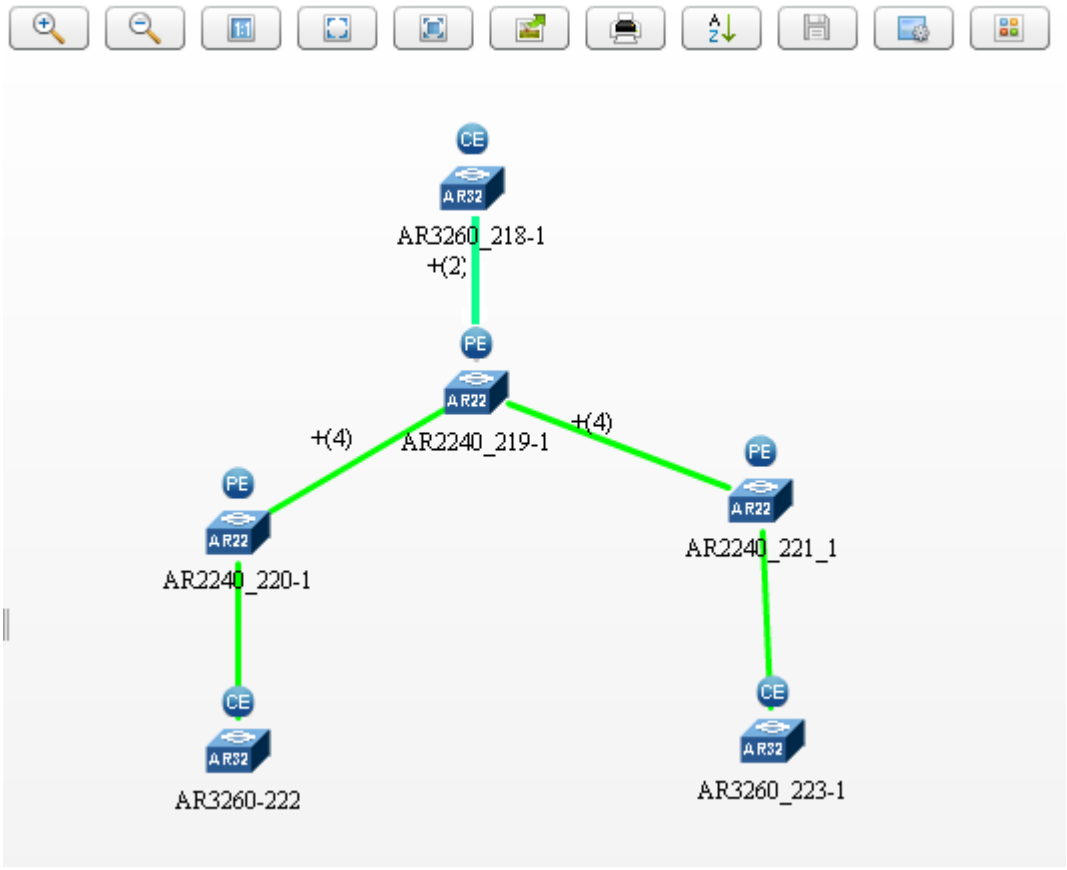
1. Choose **Network Application** > **BGP/MPLS VPN Management**.
2. In the navigation tree, choose **Service Management** > **Service List**, and click **Auto Discover**.
3. Set **Discovery policy** to **Discover by VRF connection**.
4. Click **Select Device** next to **Discovery range**. In the **Select 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 CE and PE.
   - 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 9-25** shows a VPN service topology view.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-25 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

9.4 SLA Management

eSight provides the service level agreement (SLA) monitoring and management functions, including SLA services, SLA tasks, and quick diagnosis.

9.4.1 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.

9.4.1.1 SLA Terms

This topic describes SLA terms.

Copyright © Huawei Technologies Co., Ltd.

Table 9-14 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.

9.4.1.2 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.

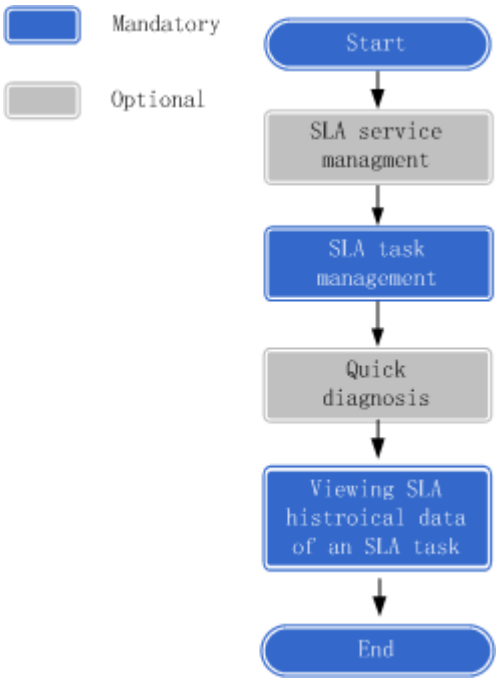
The SLA has the following functions:

- 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:

Copyright © Huawei Technologies Co., Ltd.

Figure 9-26 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.
- Viewing historical task data: Users can view a task's compliance curve and the graph of the comparison between a counter's threshold and actual values in a specified period.

9.4.1.3 SLA Terms and Default Settings

Before using the SLA component, you must master the SLA terms and default settings to ensure smooth operations.

Terms

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 instances.

SLA task: An SLA task is a test instance for monitoring network links and the service quality on these network links.

Service rating: A higher service rating indicates higher requirements on service counters such as the packet loss rate, latency, and jitter.

Compliance: The conformity indicates the ratio of the actual network quality to the expected quality, in percentage.

Copyright © Huawei Technologies Co., Ltd.

Default Settings

eSightprovides default services and service ratings for users to select.

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
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

- Jitter: interval for receiving a packets minus the interval for sending the packet.
- Lantency: 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

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

Copyright © Huawei Technologies Co., Ltd.

Counter	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
Number of timeouts	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Max. unidirectional delay from source to destination (ms)	N	Y	N	Y	N	N	N	N	N	N
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

Copyright © Huawei Technologies Co., Ltd.

Counter	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
Number of initialization or resource application failures	N	N	N	N	N	N	Y	N	N	Y
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
Number of DNS resolution failures	N	N	N	N	N	N	N	N	Y	N

Copyright © Huawei Technologies Co., Ltd.

The Test Instances That The Device Version Supports

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
S2300	V100R005C00, V100R005C01, V100R006C00, V100R006C01, V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
	V100R003C00, V100R003C01	Y	N	Y	Y	Y	Y	Y	N	Y	N
S2700	V100R005C01, V100R006C00, V100R006C01, V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
S3300	V100R003C00, V100R003C01, V100R005C00, V100R005C01, V100R006C00, V100R006C01, V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
S3700	V100R005C01, V100R006C00, V100R006C01, V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
S5300	V100R003C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
	V100R003C01, V100R005C00, V100R005C01, V100R006C00, V100R006C01	Y	N	Y	Y	Y	Y	Y	N	Y	Y
	V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
S5700	V100R005C01, V100R006C00, V100R006C01, V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
S6300	V100R006C00, V100R006C01, V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
S6700	V100R006C00, V100R006C01, V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
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

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
NE20E-8	V200R003C00, V200R003C01, V200R005C00, V200R005C01, V200R005C02, V200R005C03, V200R005C05	Y	N	Y	Y	Y	Y	Y	Y	Y	N
NE20E-X6	V600R003C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
NE40	V300R002C00, V300R002C01, V300R003C00, V300R003C01, V300R003C02, V300R005C00, V300R005C01	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
NE40E	V300R001C00	N	N	N	N	N	N	N	N	N	N
	V300R002C00, V300R003C00, V300R003C01, V300R003C02	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
	V300R006C00, V300R006C01, V600R001C00, V600R001C01, V600R003C00, V600R003C01, V600R003C02, V600R003C03, V600R003C05	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
NE40E-4	V300R003C00, V300R003C01, V300R003C02	N	N	N	N	N	N	N	N	N	N
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

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
	V300R003C00, V300R003C01, V300R003C02	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
	V300R006C00, V300R006C01, V600R001C00, V600R001C01	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
AR1200	V200R001C00, V200R001C01, V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AR2200	V200R001C00, V200R001C01, V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Device Type	Device Version	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
AR3200	V200R001C00, V200R001C01, V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AR150	V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AR200	V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

NOTE

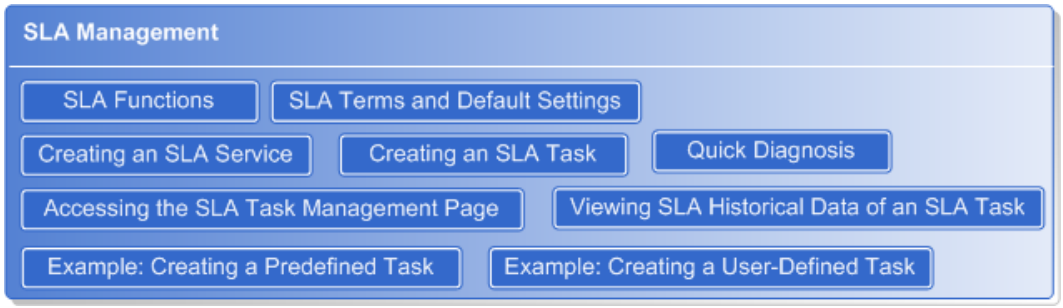
- For the UDP Echo and UDP Jitter test instances, you must enable UDP on the destination device.
  Enable UDP.
  <Huawei> **system-view**
  [Huawei] **nqa-server udpecho** *10.137.61.39 33434*
  10.137.61.39 is the destination device IP address and **33434** is the UDP port number.
- For the TCP Connect test instance, you must enable TCP on the destination device.
  Enable TCP.
  <Huawei> **system-view**
  [Huawei] **nqa-server tcpconnect** *10.137.61.39 33433*
  10.137.61.39 is the destination device IP address and **33433** is the TCP port number.

9.4.2 Overview of SLA Management Operations

This topic describes the SLA management operations.

Figure 9-27 shows the overview of SLA management operations. For more details, click the operation in the overview.

Figure 9-27 Overview of SLA management operations



Copyright © Huawei Technologies Co., Ltd.

Table 9-15 describes the SLA management operations.

Table 9-15 SLA management operations

Operation	Description	Navigation Path
9.4.1.2 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.	**Network Application** > **SLA Management** > **SLA Overview**
9.4.1.3 SLA Terms and Default Settings	Before using the SLA component, you must master the SLA terms and default settings to ensure smooth operations.	**Network Application** > **SLA Management** > **SLA Overview**
9.4.3.1 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.	**Network Application** > **SLA Management** > **SLA Service Management**
9.4.3.2 Creating an SLA Task	An SLA task is a test instance used to check the network link quality.	**Network Application** > **SLA Management** > **SLA Task Management**
9.4.3.3 Quick Diagnosis	The quick diagnosis function is used to check links monitored by SLA tasks.	**Network Application** > **SLA Management** > **Quick Diagnosis**
9.4.4.1 Accessing the SLA Task Management Page	This topic describes how to access the SLA Task Management page to monitor SLA tasks.	**Network Application** > **SLA Management** > **SLA Task Management**
9.4.4.2 Viewing SLA Historical Data of an SLA Task	The SLA task details page displays the counter value graph in a specified period.	**Network Application** > **SLA Management** > **SLA Task Management**
9.4.5.1 Example: Creating a Predefined Task	This topic describes how to create a predefined task.	**Network Application** > **SLA Management** > **SLA Task Management**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
9.4.5.2 Example: Creating a User-Defined Task	This topic describes how to create a user-defined task.	**Network Application** > **SLA Management** > **SLA Task Management**

9.4.3 Configuring SLA Tasks

This topic describes how to configure SLA tasks.

9.4.3.1 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**.

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**.

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.

9.4.3.2 Creating an SLA Task

An SLA task is a test instance used to check the network link quality.

Context

An SLA service has been created.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **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.

Step 4 Set the task execution policy.

1. Set the task execution start date and end date.
2. Set **Execution period** and **Execution days**.

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.

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.

Step 7 (Optional) Click **Test** and verify that the new SLA task can be executed properly.

Step 8 Click **OK**.

----End

9.4.3.3 Quick Diagnosis

The quick diagnosis function is used to check links monitored by SLA tasks.

Context

An SLA task has been created.

Procedure

Step 1 Choose **Network Application** > **SLA Management**.

Step 2 In the navigation tree, click **Quick Diagnosis**.

Copyright © Huawei Technologies Co., Ltd.

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.

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.

----End

9.4.4 Monitoring SLA Tasks

This topic describes how to monitor SLA tasks.

9.4.4.1 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**.

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**, **Service name**, **Source device**, 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**, **Daily Compliance**, and **Alarm Count** values are updated in real time.

Step 6 The **Historical data**, **Copy**, and **Diagnosis** buttons are provided in the table operation area.

- **Historical data**: For details, see **9.4.4.2 Viewing SLA Historical Data of an SLA Task**.
- **Copy**: Click this button to copy SLA task data. An SLA task with a new name is created.
- **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.

----End

9.4.4.2 Viewing SLA Historical Data of an SLA Task

The SLA task details page displays the counter value graph in a specified period.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Network Application** > **SLA Management**.

Step 2 In the navigation tree, choose **SLA Management** > **SLA Task Management**.

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 on 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.

----End

9.4.5 Typical SLA Applications

This topic describes two typical SLA applications.

9.4.5.1 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**.

Copyright © Huawei Technologies Co., Ltd.

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

9.4.5.2 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**.

Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

10 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.

Copyright © Huawei Technologies Co., Ltd.

10.1 Overview of Smart Configuration Tool Operations

This topic describes the Smart Configuration Tool operations.

Figure 10-1 shows the overview of Smart Configuration Tool operations. For details, click operations in the overview.

Overview of Smart Configuration Tool Operations

Figure 10-1 Overview of Smart Configuration Tool Operations

Table 10-1 describes the smart configuration tool operations.

Table 10-1 Smart Configuration Tool Operations

Operation	Description	Navigation Path
10.3.1 Delivery by Profile	The delivery by profile function allows you to set parameters for a common or user-defined command line in a profile and send the profile to multiple devices.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Profile**
10.3.2 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.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Plan Sheet**
10.3.3 Delivery Record Management	This topic describes delivery record management operations.	**Maintenance** > **Smart Configuration Tool** > **Delivery Record Management**
10.4.1 Profile Management and Delivery	This topic describes how to create a profile.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Profile**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
10.4.1.1 Creating a Profile	This topic describes how to deliver a profile to devices.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Profile**
10.4.1.2 Delivering a Profile	This topic describes how to export a verified profile. You can modify an exported profile, import the new profile, and deliver the new profile containing different parameter settings to multiple network devices.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Profile**
10.4.2 Plan Sheet Management and Delivery	You can use the plan sheet to deliver a profile containing different parameter settings to multiple network devices.	**Maintenance** > **Smart Configuration Tool** > **Delivery Record Management**
10.5.1 Example: Delivery by Profile	This topic describes a typical application to help network administrators better understand how to delivery by profile.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Profile**
10.5.2 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.	**Maintenance** > **Smart Configuration Tool** > **Delivery by Plan Sheet**

10.2 Functions

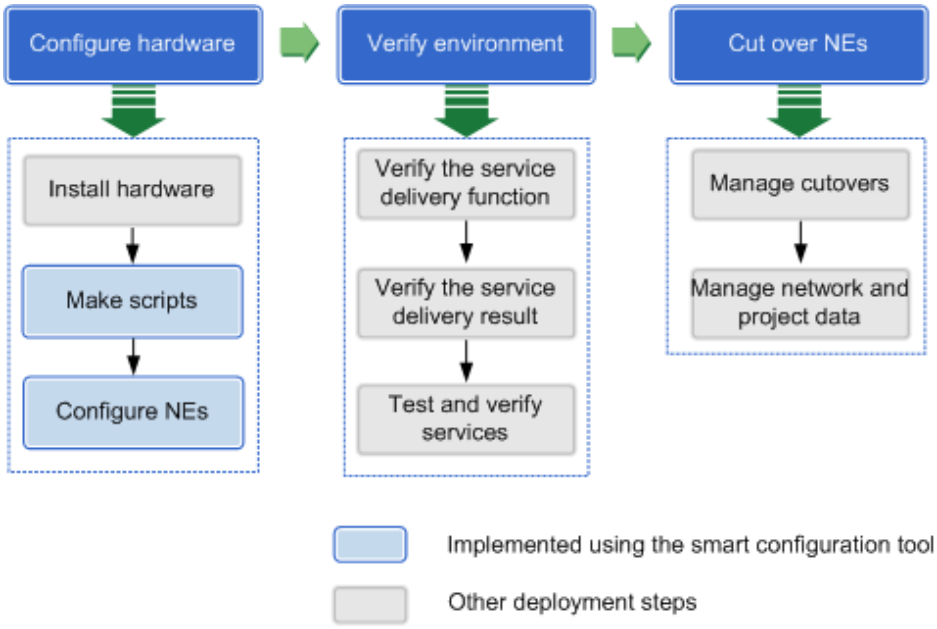
When establishing network environment, you must configure a large number of network elements (NEs). Generating scripts manually based on a network plan is time-consuming and may contain errors. With the smart configuration tool, you can configure a profile and plan sheet, and send the same parameter settings to multiple NEs, greatly improving NE configuration efficiency.

- The smart configuration tool provides the profile management function to quickly generate profiles. In a profile, 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 10-2 shows the application scenario of the smart configuration tool.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-2 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.

10.3 Function Panorama

This topic describes the delivery by profile and delivery by plan sheet functions of the smart configuration tool.

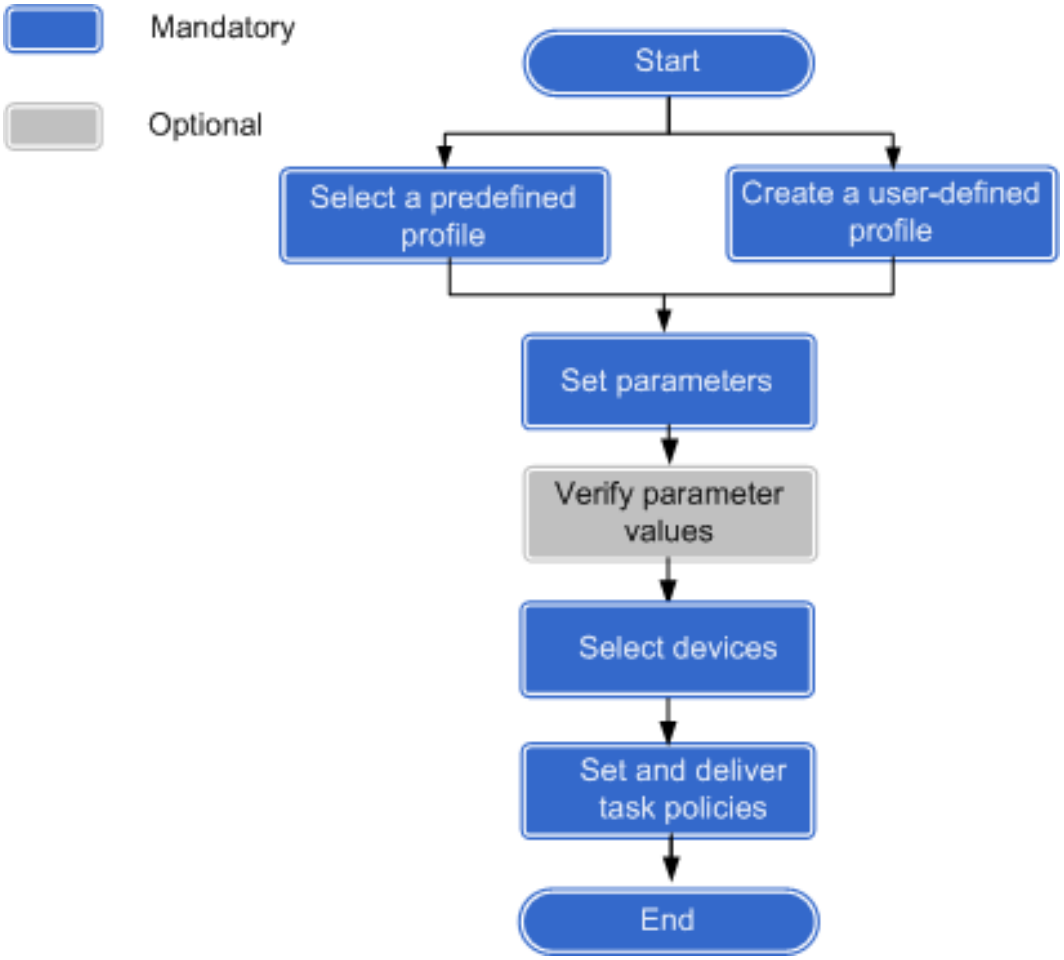
10.3.1 Delivery by Profile

The delivery by profile function allows you to set parameters for a common or user-defined command line in a profile and send the profile to multiple devices.

Copyright © Huawei Technologies Co., Ltd.

Process Description

Figure 10-3 Process of delivery by profile



Function Description

1. Profile base
   - Predefined profile: Displays predefined common profiles.
   - User-defined profile: Displays user-defined profiles in the **User-defined** folder, and allows you to create, copy, move, modify, and delete profiles, and create folders to classify profiles to make the finding and management easy.
2. Delivery by profile
   - **Deploy**: Select an existing profile in the profile base, set parameters, and send the profile to multiple devices.
   - To deliver a profile, perform the following steps: select a profile, set parameters, select devices, and configure tasks.

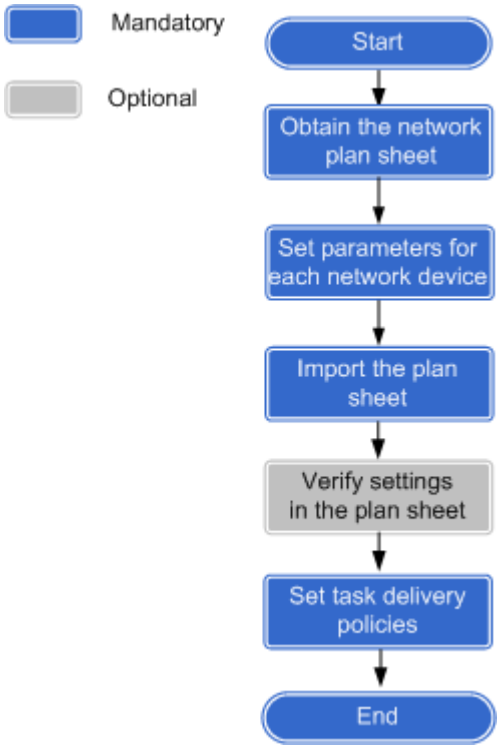
10.3.2 Delivery by Plan Sheet

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.

Copyright © Huawei Technologies Co., Ltd.

Process Description

Figure 10-4 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.

10.3.3 Delivery Record Management

This topic describes delivery record management operations.

Copyright © Huawei Technologies Co., Ltd.

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**.

10.4 Configuring Tasks

This topic describes how to configure tasks using the smart configuration tool.

10.4.1 Profile Management and Delivery

The delivery by profile function allows you to set mandatory parameters for common or user-defined command lines and send the command lines to multiple devices.

10.4.1.1 Creating a Profile

This topic describes how to create a profile.

Context

The smart configuration tool provides multiple predefined profiles. If the predefined profiles cannot meet your requirements, you can create profiles as required.

Procedure

Step 1 Choose **Maintenance** > **Smart Configuration Tool** from the main menu.

Step 2 In the navigation tree, click **Template Deploy**. Then expand the **User-defined** folder.

Step 3 Click **New Template**. The page for creating a profile is displayed.

Step 4 Set **Directory**, **Template name**, **Description**, and **Template Content**.

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.

Copyright © Huawei Technologies Co., Ltd.

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 profile is displayed in the **User-defined** folder.

NOTE

If you want to generate a profile, select a device to verify. If the profile is verified, a table profile is generated.

----End

10.4.1.2 Delivering a Profile

This topic describes how to deliver a profile to devices.

Procedure

Step 1 Choose **Maintenance** > **Smart Configuration Tool** from the main menu.

Step 2 In the navigation tree, click **Template Deploy**, and select the profile to be delivered.

Step 3 Click **Deploy**. The page for delivering a profile is displayed.

Step 4 Set parameters in the command table, and click **Next**.

Step 5 Click **Add**, select devices to which the profile is delivered in the **Select Device** dialog box that is displayed, and click **OK**. Then click **Next**.

Step 6 Set **Task Name**, **Description** (optional), **Execute** and **Restore policy**(optional), and click **Deploy/OK**. In the **Confirm** dialog box, click **YES**.

----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.

10.4.1.3 Exporting a Plan Sheet

This topic describes how to export a verified profile. You can modify an exported profile, import the new profile, and deliver the new profile containing different parameter settings to multiple network devices.

Prerequisites

Profiles have been verified.

Procedure

Step 1 Choose **Maintenance** > **Smart Configuration Tool** from the main menu.

Step 2 In the navigation tree, click **Template Deploy**, and search for a profile to be exported.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Select the profile, and click **Export Plan Sheet**. The **Export Plan Sheet** dialog box is displayed.

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 Select the devices you want to export.

Step 6 Click **OK**. Then click **Save** to save the plan sheet to the local host in the **File Download** dialog box that is displayed.

Step 7 Close the **Export Plan Sheet** dialog box.

----End

10.4.2 Plan Sheet Management and Delivery

You can use the plan sheet to deliver a profile containing different parameter settings 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, **00:00**, 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.

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 **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 name**, **Description**, **Execute** and **Restore policy**, and click **Deploy**.

Step 9 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.

----End

Copyright © Huawei Technologies Co., Ltd.

10.5 Configuration Examples

This topic describes two typical applications to help network administrators better understand the smart configuration tool.

10.5.1 Example: Delivery by Profile

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 profile **Create Multiple VLANs**.

Step 3 Click **Deploy**. The profile 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 profile 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

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.

Copyright © Huawei Technologies Co., Ltd.

10.5.2 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 profiles can be directly exported as plan sheets, and self-defined profiles 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.

Copyright © Huawei Technologies Co., Ltd.

11 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.

Copyright © Huawei Technologies Co., Ltd.

11.1 Overview of Device Configuration File Management Operations

This topic describes the device configuration file management operations.

Figure 11-1 shows the overview of device configuration file management operations. For more details, click the operation in the overview.

Figure 11-1 Overview of device configuration file management operations

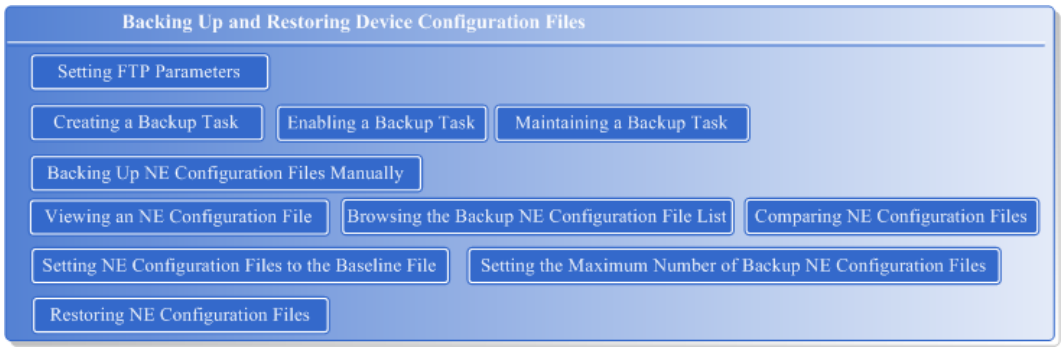


Table 11-1 lists the device configuration file management operations.

Table 11-1 Operation description

Operation	Description	Access
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.	**Maintenance** > **Configuration File Management**
Creating a Backup Task	You can create a backup task for a type of NEs.	**Maintenance** > **Configuration File Management**
Enabling a Backup Task	When a configuration file backup task is disabled, you must enable the backup task for execution.	**Maintenance** > **Configuration File Management**
Maintaining a Backup Task	You can browse and maintain a backup task as required.	**Maintenance** > **Configuration File Management**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Access
Backing Up NE Configuration Files Manually	You can back up NE configuration files manually for instant backup.	**Maintenance** > **Configuration File Management**
Viewing an NE Configuration File	This topic describes how to view a backup NE configuration file and a configuration file that is in use.	**Maintenance** > **Configuration File Management**
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.	**Maintenance** > **Configuration File Management**
Comparing NE Configuration Files	You can know differences between NE configuration files by comparing them.	**Maintenance** > **Configuration File Management**
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.	**Maintenance** > **Configuration File Management**
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.	**Maintenance** > **Configuration File Management**
Restoring NE Configuration Files	When an NE is faulty, you can upload an NE configuration file to the NE to restore NE configuration data.	**Maintenance** > **Configuration File Management**

11.2 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.

Copyright © Huawei Technologies Co., Ltd.

Context

NOTE

The FTP service port number must be 21.

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**.

Procedure

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

Step 2 In the navigation tree on the left, choose **Set System Parameters** > **FTP Parameters**.

Step 3 Set the FTP parameters and click **Apply**.

----End

11.3 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.

11.3.1 Backing Up NE Configuration Files Automatically

eSight can automatically and periodically back up NE configuration files using backup tasks.

11.3.1.1 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 **11.2 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**.

Step 2 Choose **Manage Configuration Files** > **Backup Tasks** from the navigation tree on the left.

Step 3 Click **Create** to set backup task parameters.

Step 4 Click **Add Device** next to **Apply to Device**, select a device, and click **OK** to apply the backup task to the device.

Copyright © Huawei Technologies Co., Ltd.

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

11.3.1.2 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**.

Step 2 Choose **Manage Configuration Files** > **Backup Tasks** from the navigation tree on the left.

Step 3 Set **Status** to **Disable** and click **Search**.

Step 4 Select a backup task and click **Enable**.

----End

11.3.1.3 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**.

Step 2 Choose **Manage Configuration Files** > **Backup Tasks** from the navigation tree on the left.

Step 3 Set filter parameters at the top of the pane and click **Search**.

Step 4 **Optional:** If **Latest Backup Result** is **Flailure** or **Partially successful**, click **Flailure** 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

Copyright © Huawei Technologies Co., Ltd.

11.3.2 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 **11.2 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**.

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

11.4 Managing NE Configuration Files

This topic describes common operations for managing NE configuration files.

11.4.1 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**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **Manage Configuration Files** > **Configuration Backup Files** from the navigation tree on the left.

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.
2. Click  next to a configuration file to view details.

----End

11.4.2 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**.

Step 2 Choose **Manage Configuration Files** > **Configuration Backup Files** from the navigation tree on the left.

Step 3 Click  on the right and view backup NE configuration files on the file management page.

----End

11.4.3 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**.

Step 2 Choose **Manage Configuration Files** > **Configuration Backup Files** from the navigation tree on the left.

Step 3 Click  on the right to access the NE configuration file management page.

Step 4 Select two configuration files and click **Compare** to view the comparing result.

- 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.

Copyright © Huawei Technologies Co., Ltd.

- Click **Previous Difference** or **Next Difference** to highlight the previous or next difference.

----End

11.4.4 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**.

Step 2 Choose **Manage Configuration Files** > **Configuration Backup Files** from the navigation tree on the left.

Step 3 Set an NE configuration file to the baseline file.

1. Click  on the right to access the NE configuration file management page.
2. 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.

1. Select multiple NEs and click **Set File as Baseline**.
2. If the operation fails or partially fails, you can click **Details** in the **Prompt** dialog box that is displayed to view the cause.
3. In the **Prompt** dialog box that is displayed, click **OK**.

----End

11.4.5 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 In the navigation tree on the left, choose **Set System Parameters** > **Max. Backup Files**.

Step 3 Set **Max. backup files**.

Step 4 Enable or disable **Alarm burst mode**.

NOTE

1. When **Alarm burst mode** is enabled, the configuration file module automatically backs up device configuration files when eSight receives configuration update alarms from devices.
2. 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

11.5 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**.

Step 2 Choose **Manage Configuration Files** > **Configuration Backup Files** from the navigation tree on the left.

Step 3 Restore an NE configuration file.

1. Click on the right to access the NE configuration file management page.
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**.
2. Click **Yes** in the **Prompt** dialog box that is displayed.

Copyright © Huawei Technologies Co., Ltd.

3. In the **Prompt** dialog box that is displayed, click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

12 User-Defined Devices Management

About This Chapter

When managing a network containing devices from multiple manufacturers, eSight allows you to user-defined devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types to reduce operation and maintenance costs.

Copyright © Huawei Technologies Co., Ltd.

12.1 Overview of User-Defined Devices Management

This topic describes the user-defined devices management operations.

Figure 12-1 shows the overview of user-defined devices management operations. For more details, click the operation in the overview.

Figure 12-1 overview of user-defined devices management operations

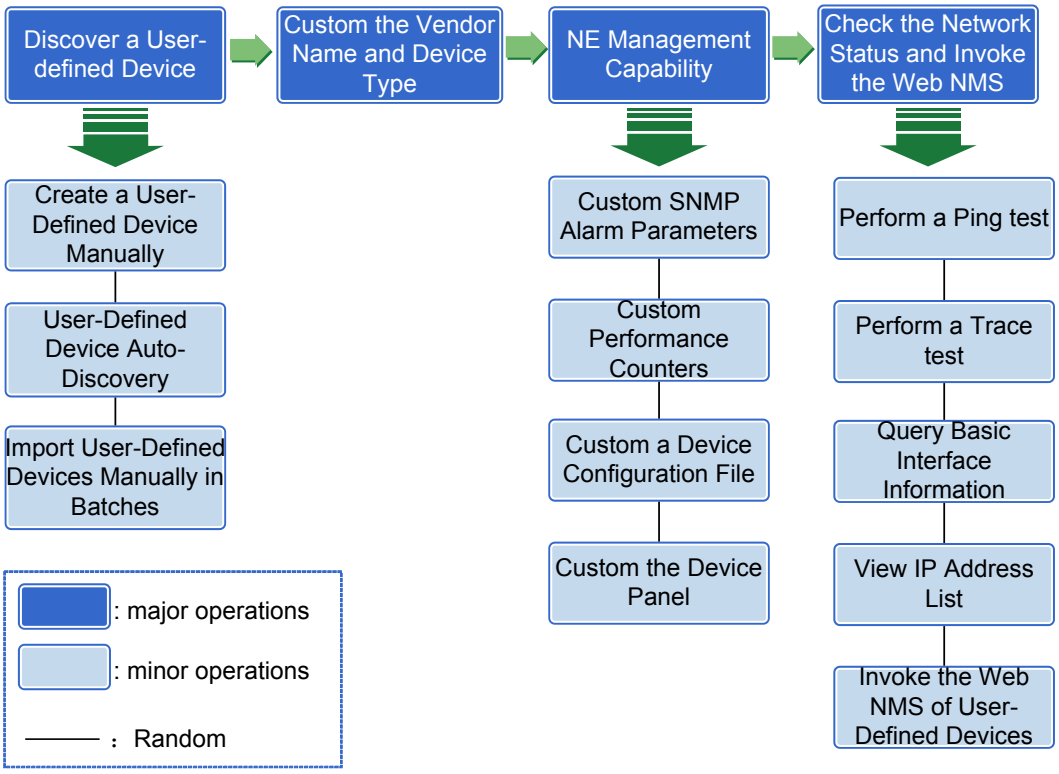


Table 12-1 describes the user-defined devices management operations.

Table 12-1 user-defined devices management operations

Operation	Description	Navigation Path
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.	**Resource** > **Resource Management**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
Customizing the Vendor Name and Device Type	eSight cannot recognize vendor names and device types of some third-party devices. You must customize the vendor name and device type as required in eSight.	**System** > **Customize Device**
Customizing SNMP Alarm Parameters	You can customize SNMP alarm parameters in eSight so that non-Huawei devices can report SNMP alarms to eSight.	**System** > **Customize Device**
Customizing Performance Counters	This topic describes how to customize performance counters, including device temperature, interface packet error rate, and CPU usage.	**System** > **Customize Device**
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.	**System** > **Customize Device**
Customizing the Device Panel	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.	**System** > **Customize Device**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Navigation Path
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
Query Basic Interface Information	eSight supports query of information on an interface.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**
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.	**Resource** > **Resource Management**

12.2 User-defined Devices' 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.

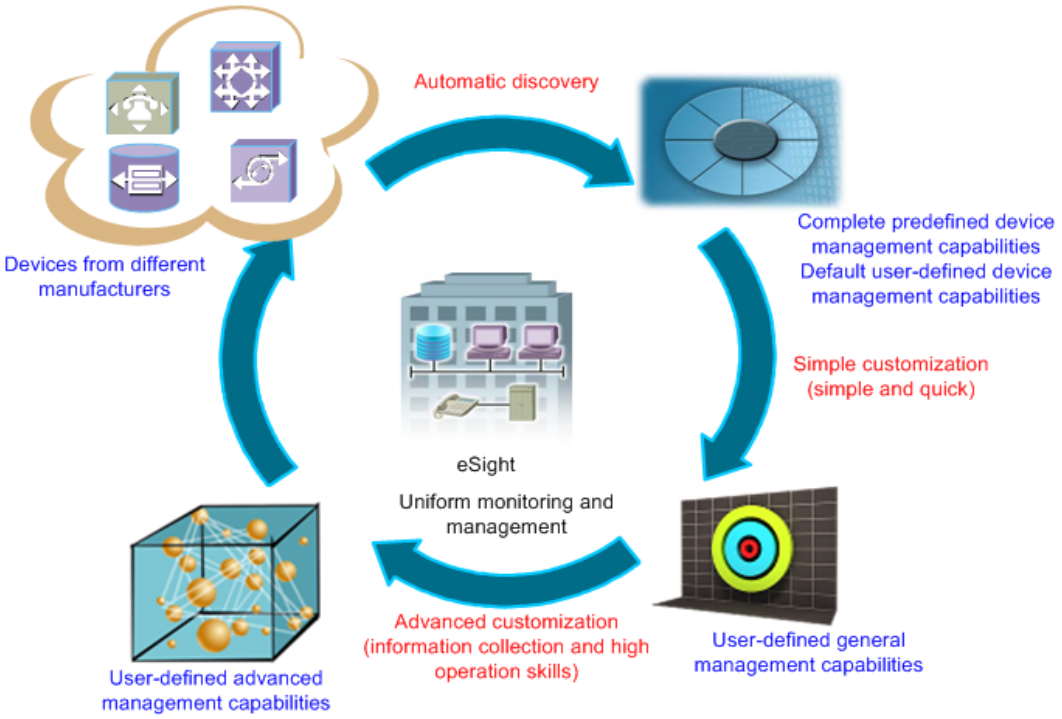
Application Scenario

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.

Copyright © Huawei Technologies Co., Ltd.

Customize other devices from different manufacturers flexibly on eSight for different management capabilities. Then you can manage devices from all manufacturers on eSight.



Default and Customizable Functions

Device	Default Functions After Discovery	New Functions After Customization
Huawei Device, H3C Device, and Cisco Device	● Basic information ● Device panel ● SNMP parameters ● Public alarm (alarm menu and NE manager) ● IP address ● Interface manager ● Telnet parameters ● Performance indicator ● Configuration file backup and restore	● Private alarm ● Performance indicator ● Panel ● Topology icon

Copyright © Huawei Technologies Co., Ltd.

Device	Default Functions After Discovery	New Functions After Customization
Unknown	● Basic information ● Device panel ● SNMP parameters	● IP address ● Interface manager ● Telnet parameters ● Alarm ● Performance indicator ● Topology icon ● Configuration file backup and restore 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.

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. Workload: 0.2 person/day For details, see **12.5 Customizing the Vendor Name and Device Type**.	● Manufacturer name (Only **Unknown** is available.) ● NE type ● NE category	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 Workload: 1 item/ hour For details, see **12.6.1 Customizing SNMP Alarm Parameters**.	● Trap OID of the alarm to add ● VB (MIB node information) **NOTE** Obtain the preceding information from the manufacturer.	Huawei Device, H3C Device, Cisco Device, and Unknown

Copyright © Huawei Technologies Co., Ltd.

Customization Item	Description	Information to Collect	Application Scope
Performance Indicator	Performance indicators supported by devices of the **Huawei Device**, **H3C Device**, and **Cisco Device** types are the same as those of predefined devices from Huawei, H3C, and Cisco respectively. By default, devices of the **Unknown** type do not support performance indicators. Therefore, you must customize performance indicators for them. Workload: 0.5 item/hour For details, see **12.6.2 Customizing Performance Counters**.	● Performance indicator OID ● Formula ● Measurement object index **NOTE** Obtain the preceding information from the manufacturer.	● Huawei Device, H3C Device, and Cisco Device: support customization but do not need customization unless otherwise specified. ● Unknown: needs customization.
Configuration backup files	Devices only of the **Unknown** 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.) Workload: 0.2 person/day For details, see **12.6.3 Customizing a Device Configuration File**.	● Backup command ● Restore command ● Restart command **NOTE** Obtain the preceding information from the manufacturer.	Unknown

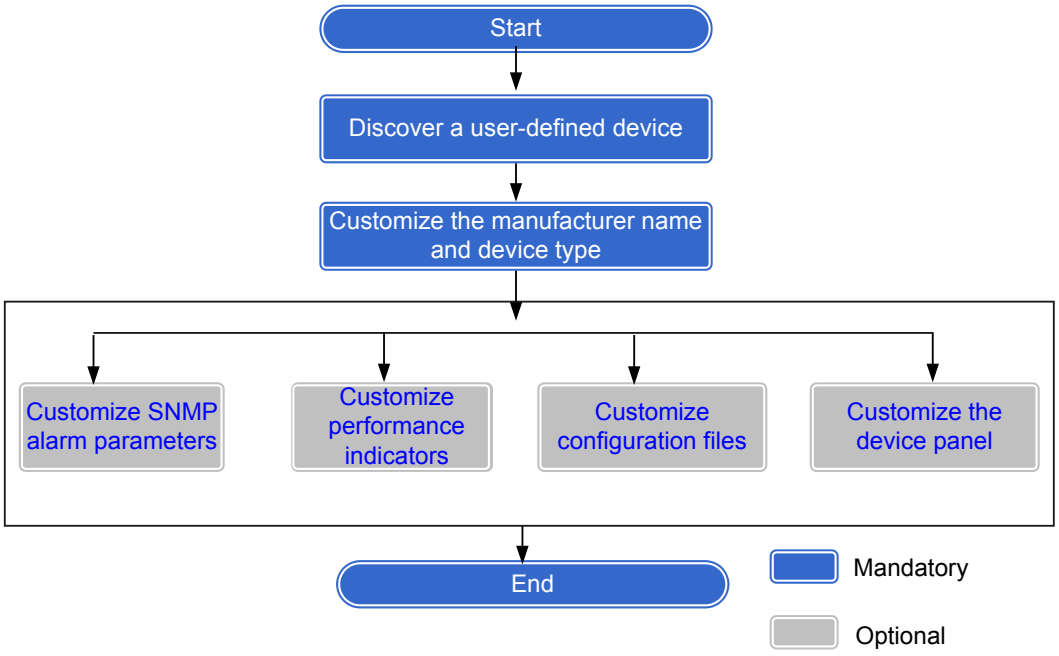
Copyright © Huawei Technologies Co., Ltd.

Customization Item	Description	Information to Collect	Application Scope
NE panel	Devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types can be displayed on the NE panel. (The displayed device panel may differ from the actual situation.) Workload: 1 person/day For details, see **12.6.4 Customizing the Device Panel**.	● Actual appearance ● Device hierarchy ● Device's **vendortype**, which is unique identifier of each device ● Start index	Huawei Device H3C Device Cisco Device

12.3 Customization Process

To customize a user-defined device, you can perform the following steps for quicker and accurate configuration.

Customization Flowchart



Copyright © Huawei Technologies Co., Ltd.

12.4 Discovering a User-defined Device

eSight allows you to add a user-defined device to eSight using three methods and manage it on eSight.

12.4.1 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** > **Resource Management** from the main menu.

Step 2 In the **Resource Management** window, select the parent object for the NE to be added, and then click **Create Resource**.

Step 3 On the **Select Object Type** page, select an NE type under **Physical Devices**.

Step 4 On the **Configure Parameters** page, set the basic information and SNMP protocol for the NE.

NOTE

If you configure simple network management protocol (SNMP) parameters for an NE, click **Save Protocol Template** to save the settings as an SNMP parameter configuration template. If you need to configure SNMP parameters again, click **Select Protocol Template** to select the saved protocol template to apply.

Step 5 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

Follow-up Procedure

The following table describes the operations that you can perform after you manually create an NE in the eSight.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. Click the name of the required NE. The eSight displays all information about the NE.
Modify NE information	In the eSight, you can modify the name of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the configuration parameters of the NE. 3. Then click **OK**.
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. ● To delete an NE, click  in the **Operation** column where the NE is located. ● To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

12.4.2 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**.

Copyright © Huawei Technologies Co., Ltd.

- NEs support the SNMP version specified by the eSight.

Procedure

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

Step 2 On the managed objects page on the right of the **Resource Management** window, click **Auto Discovery**.

Step 3 On the auto-discovery page, click **Network Segment Discovery**.

Step 4 On the **Network Segment Discovery** page, set network segment discovery parameters and SNMP parameters.

For convenience, you can click **Select Protocol Template** to use the parameters in the saved SNMP template. For details, see **Save Protocal Template**.

Step 5 **Optional:** Select **Add the discovered objects automatically to the NMS**.

NOTE

- If **Add the discovered objects automatically to the NMS** is selected, the discovered NEs are automatically added. The **Step 7** is skipped.
- If **Add the discovered objects automatically to the NMS** is not selected, you need to execute the **Step 7** to add the discovered NEs.

Step 6 Click **Discover**.

The discovered NEs are displayed in the list.

NOTE

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

Step 7 Select NEs in the list and click **Create**.

If **Add the discovered objects automatically to the 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.

Step 8 Click **Finish**.

The system returns to the **Resource Management** page, and the added NEs are displayed in the managed object list on the rights.

----End

Follow-up Procedure

The following table describes the operations that you can perform after you add the automatically discovered NEs to the eSight.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. In the managed object list, click the name of the required NE to view its basic information and SNMP information.
Modify NE information	In the eSight, you can modify the attributes of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the name of the NE. 3. Then click **OK**.
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. ● To delete an NE, click  in the **Operation** column where the NE is located. ● To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

12.4.3 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**.

Copyright © Huawei Technologies Co., Ltd.

Context

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

Table 12-2 describes every fields in Excel template.

Table 12-2 Excel template

Field name	Description
IP Address	For example, **10.123.124.115**.
NE Name	1 to 128 characters. The NE name cannot contain the following characters #%&+/;<=>?\.
Protocol Type	Set to **SNMP**.
Protocol Version	The protocol version must be the same as the SNMP protocol version in the device. The value range is **V1** or **V2c**.
Port	This parameter must be the same as the port number of the SNMP protocol, for example, **161**.
Read Community	This parameter must be the same as the read community of the SNMP protocol, for example, **public**.
Write Community	This parameter must be the same as the write community of the SNMP protocol, for example, **private**.

Procedure

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

Step 2 On the managed object page on the right of the **Resource Management** window, click **Batch Import**.

Step 3 On the **Select Objects to Import in Batches** page, select **Import Hosts and Network Devices**.

Step 4 In **Import Hosts and Network Devices**, click Template.xls next to **Template to download**, and download the **.xls** template to the local computer.

Step 5 Open the template, fill in NE information, and save the template.

Step 6 Click next to **Resource file to import** to select the .xls file that you have saved.

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

Step 7 Click to upload the file.

Resources displays NE information in the file and the result of the check. If the **Result** column is blank, the NE check is successful.

Step 8 Select NEs under **Resources**, and click **Create**.

The system starts to import the NEs.

Copyright © Huawei Technologies Co., Ltd.

- 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.

----End

Follow-up Procedure

The following table describes the operations that you can perform after you manually import NEs to the eSight.

Maintaining NEs	Operation Method
View NE information	In the eSight, you can view NE information conveniently, including the basic information and protocol information about NEs. 1. On the managed object page on the right of the **Resource Management** window, set search criteria and click **Search**. 1. In the **Search by** drop-down list, select a search type. 2. In the **Search Criteria** text box, enter search criteria. 2. Click the name of the required NE. The eSight displays all information about the NE.
Modify NE information	In the eSight, you can modify the name of an NE, such as the NE name. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. On the page for modifying NE information, modify the configuration parameters of the NE. 3. Then click **OK**.
Delete an NE	You can delete the NEs that do not need to be managed by the eSight. 1. In the managed object list on the right of the **Resource Management** window, delete NEs. - To delete an NE, click  in the **Operation** column where the NE is located. - To delete multiple NEs, select them and click **Batch Delete**. 2. In the **Confirm** dialog box, click **Yes**.

Copyright © Huawei Technologies Co., Ltd.

Maintaining NEs	Operation Method
Manage an NE	In the eSight, you can open the NE management window in the resource management window. 1. In the managed object list on the right of the **Resource Management** window, click  in the **Operation** column where the required NE is located. 2. In the NE management window, perform management operations on the NE. For details, see **Monitory Alarms in the NE Monitoring List** and **View NE Performance Overview**.

12.5 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**. The device list is displayed.
2. Click **Manage** next to an NE. The NE manager is displayed.
3. On the **Basic Information** tab page, click **User-defined device type** next to **Model**. The **Vendor Information** page is displayed.

Step 2 Click **Create**, and customize vendor information in the window that is displayed.

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**.

Step 6 In the dialog box indicating operation success, click **OK**.

----End

Follow-up Procedure

1. Choose **Resource** > **Resource Management**. The device list is displayed.
2. Click a user-defined device in the device list. The page for configuring the basic device information is displayed.
3. Click **Manage**, and verify that the device type is customized successfully in the NE manager.

12.6 NE Management Capability

Copyright © Huawei Technologies Co., Ltd.

12.6.1 Customizing SNMP Alarm Parameters

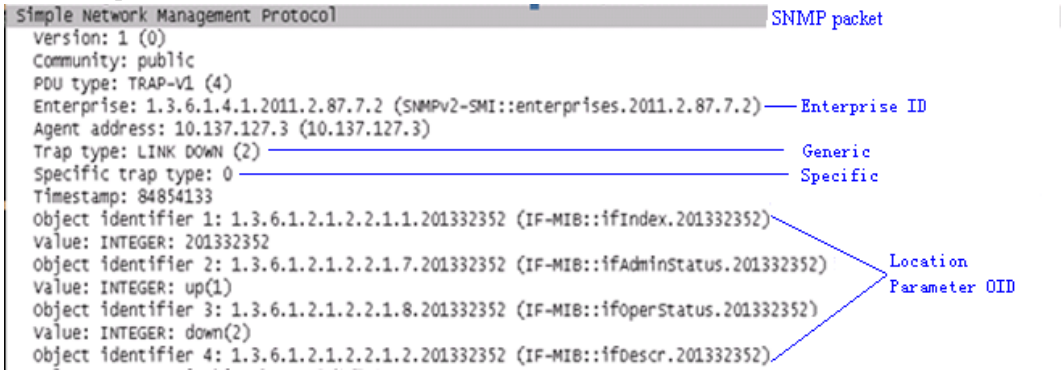
You can customize SNMP alarm parameters in eSight so that non-Huawei devices can report SNMP alarms to eSight.

Context

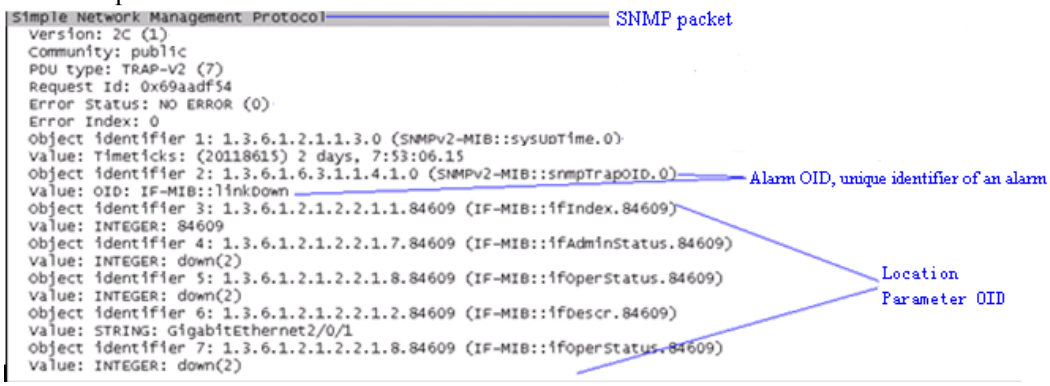
You must obtain alarms' trap IDs and MIB node information for locating alarm parameters from the manufacturer.

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:



SNMPv2 packet structure:



Procedure

Step 1 Choose **System** > **Customize Device** from the main menu.

Step 2 In the navigation tree on the left, choose **NE Management Capability** > **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**.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
SNMP Version		SNMP versions supported by eSight, including SNMPv1, SNMPv2c, and SNMPv3. ● Set the alarm OID for devices supporting SNMPv2c or SNMPv3. ● For devices supporting SNMPv1, set **Generic**, **Specific**, and **Enterprise ID**.
Generic		The combination of **Generic**, **Specific**, and **Enterprise ID** is the unique identifier of an SNMPv1 alarm.
Specific		
Enterprise ID		
Alarm OID		Trap OID supporting SNMPv2c, which is the unique identifier of an alarm.
New Parameter	Location Parameter Name	Name of an alarm location parameter. For example, **Port index** 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.

12.6.2 Customizing Performance Counters

This topic describes how to customize performance counters, including device temperature, interface packet error rate, and CPU usage.

Copyright © Huawei Technologies Co., Ltd.

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.

Step 2 In the navigation tree on the left, choose **NE Management Capability** > **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**.

   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**.
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**.

Step 4 Create a performance monitoring instance.

1. On the main menu, choose **Performance** > **Monitoring Configuration**, and click **Create**.
2. Click **Select Managed Objects**. In the **Select Managed Objects** window that is displayed, select a subnet in the topology tree on the left, and select a user-defined device in the managed object list on the right.
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**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You must manually specify monitoring objects for the performance counters without specified monitoring objects.

5. 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.

12.6.3 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.

Step 2 In the navigation tree on the left, choose **NE Management Capability** > **Configuration File**.

Step 3 Click **Create**, click **Select** next to **NE Type**, and select a desired device type.

Step 4 Set **Backup command**, **Restore command**, and **Restart command**, and click **OK**.

Step 5 Create a backup task for the configuration file.

1. Choose **Maintenance** > **Configuration File Management**.
2. Choose **Manage Configuration Files** > **Backup Tasks** from the navigation tree on the left.
3. Click **Create** and set parameters related to the 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.

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

12.6.4 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.

Copyright © Huawei Technologies Co., Ltd.

- Devices of the **Unknown** type have default device panels and do not support customization.

Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **View** > **Device Panel**. In the right pane, the default device panel provided for non-Huawei devices is displayed.

Step 3 Customize a subrack.

1. Right-click a subrack, and choose **Create 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.
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.
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.

   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**.

Copyright © Huawei Technologies Co., Ltd.

4. (Optional) Click  , upload a port image from the local host, and select the port image in the **Extended Attributes** area.
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.

12.7 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.

12.7.1 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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **View** > **Basic Information**. In the pane on the right, click **Ping**.

Step 3 In the displayed **Ping** window, set the Ping test parameters and click **Ping**.

Step 4 In the **Ping** window, view the Ping test result and click **Close**.

----End

12.7.2 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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **View** > **Basic Information**. In the pane on the right, click **Trace**.

Step 3 In the displayed **Trace** window, view the Trace test result.

Step 4 Click **Close**.

----End

Copyright © Huawei Technologies Co., Ltd.

12.7.3 Query Basic Interface Information

eSight allows users to query interface information.

Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **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

12.7.4 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 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **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.

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

12.8 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

Step 2 In the navigation tree on the left, choose **Device Config** > **Web NMS**.

----End

Copyright © Huawei Technologies Co., Ltd.

13 System Management

About This Chapter

Copyright © Huawei Technologies Co., Ltd.

13.1 Overview of System Management Operations

This topic describes the system management operations.

Figure 13-1 shows the overview of system management operations. For more details, click the operation in the overview.

Figure 13-1 Overview of system management operations

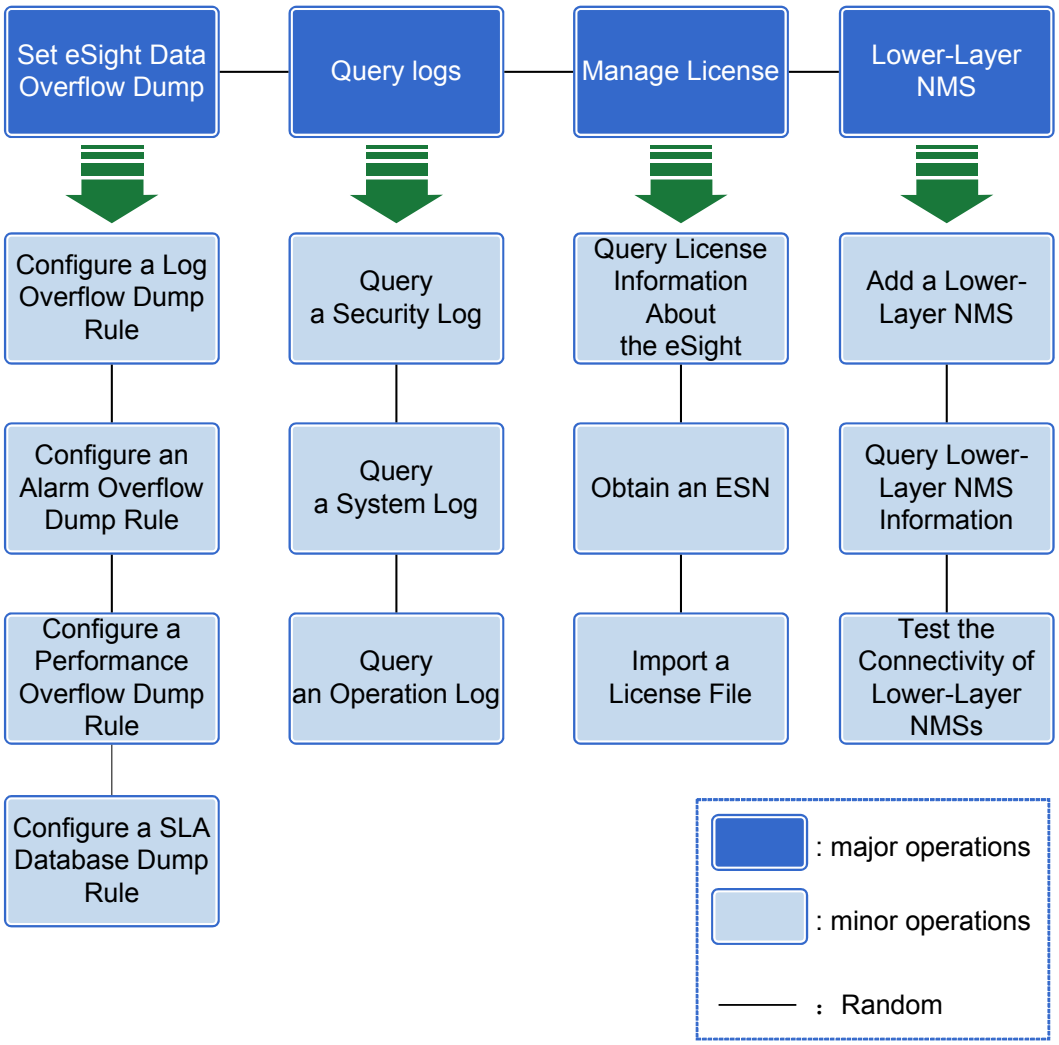


Table 13-1 describes the system management operations.

Copyright © Huawei Technologies Co., Ltd.

Table 13-1 Operation description

Operation	Description	Access
13.2.1 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.	**System** > **System Configuration** > **Database Overflow Dump** > **Log Database Dump**
13.2.2 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.	**System** > **System Configuration** > **Database Overflow Dump** > **Alarm Database Dump**
13.2.3 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.	**System** > **System Configuration** > **Database Overflow Dump** > **Performance Database Dump**
13.2.4 Configuring SLA Database Dump	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.	**System** > **System Configuration** > **Database Overflow Dump** > **SLA Database Dump**

Copyright © Huawei Technologies Co., Ltd.

Operation	Description	Access
13.3.2 Querying a Security Log	You can query security logs to understand the information about eSight related security operations.	**System** > **Log Management** > **Query Logs** > **Security Logs**
13.3.3 Querying a System Log	You can query system logs to understand the information about eSight operations.	**System** > **Log Management** > **Query Logs** > **System Logs**
13.3.4 Querying an Operation Log	You can query operation logs to understand the information about eSight user operations.	**System** > **Log Management** > **Query Logs** > **Operation Logs**
13.5.1 Querying License Information About the eSight	You can query the information about the current license.	**System** > **License Management**
13.5.2 Obtaining an ESN	When the license is going to expire, you need to obtain the ESN of the computer. The ESN is used to apply for a license.	**System** > **License Management**
13.5.3 Importing a License File	If the original license of the eSight expires, you need to import a license file to the eSight.	**System** > **License Management**
13.4.2.1 Adding a Lower-Layer NMS	You can add a lower-layer NMS to enable eSight to manage it.	**System** > **Lower-layer NMSs**
13.4.2.2 Querying Lower-Layer NMS Information	You can periodically query the lower-layer NMS status.	**System** > **Lower-layer NMSs**
13.4.2.3 Testing the Connectivity of Lower-Layer NMSs	You can periodically test the connectivity of lower-layer NMSs.	**System** > **Lower-layer NMSs**

13.2 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.

13.2.1 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.

Copyright © Huawei Technologies Co., Ltd.

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.

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 13-2**.

Table 13-2 Maximum log management tablespace size

Edition	MySQL Database	SQL Server Database	Oracle Database
Express	2 GB	-	-
Compact	2 GB	-	-
Standard	2 GB	1 GB	-
Professional (Windows)	2 GB	1 GB	-
Professional (SUSE Linux)	-	-	1 GB

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/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

13.2.2 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.

Copyright © Huawei Technologies Co., Ltd.

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.

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 13-3**.

Table 13-3 Maximum alarm management tablespace size

Edition	MySQL Database	SQL Server Database	Oracle Database
Express	8 GB	-	-
Compact	8 GB	-	-
Standard	8 GB	2 GB	-
Professional (Windows)	8 GB	2 GB	-
Professional (SUSE Linux)	-	-	4 GB

NOTE

The **Database dump threshold (%)** parameter indicates the percentage of the maximum alarm 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

13.2.3 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.

Copyright © Huawei Technologies Co., Ltd.

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.

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 13-4**.

Table 13-4 Maximum performance management tablespace size

Edition	MySQL Database	SQL Server Database	Oracle Database
Express	8 GB	-	-
Compact	8 GB	-	-
Standard	8 GB	4 GB	-
Professional (Windows)	8 GB	8 GB	-
Professional (SUSE Linux)	-	-	30 GB

NOTE

The **Database dump threshold (%)** parameter indicates the percentage of the maximum performance 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

13.2.4 Configuring SLA Database Dump

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.

Copyright © Huawei Technologies Co., Ltd.

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.

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.

The maximum SLA management tablespace size varies according to eSight edition and database type. For details, see **Table 13-5**.

Table 13-5 Maximum SLA management tablespace size

Edition	MySQL Database	SQL Server Database	Oracle Database
Express	-	-	-
Compact	-	-	-
Standard	20 GB	20 GB	-
Professional (Windows)	20 GB	20 GB	-
Professional (SUSE Linux)	-	-	20 GB

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

13.3 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.

Copyright © Huawei Technologies Co., Ltd.

13.3.1 Logs Types

Logs of the eSight include 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.

13.3.2 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.

Step 2 In the **Log Management** window, select **Query Logs** > **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**.

----End

13.3.3 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**.

Copyright © Huawei Technologies Co., Ltd.

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.

Step 2 In the **Log Management** window, select **Query Logs** > **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**.

----End

13.3.4 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.

Step 2 In the **Log Management** window, select **Query Logs** > **Operation Logs**.

Step 3 Directly view the logs or set search criteria to search for the specified logs.

NOTE

- 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.
  - Click the value in the **Details** column of the target log.
  - In the **Operation Log Details** dialog box, click **Operation Log Details** to view the result of each operation.

----End

Copyright © Huawei Technologies Co., Ltd.

13.4 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.

13.4.1 Lower-Layer NMS Management

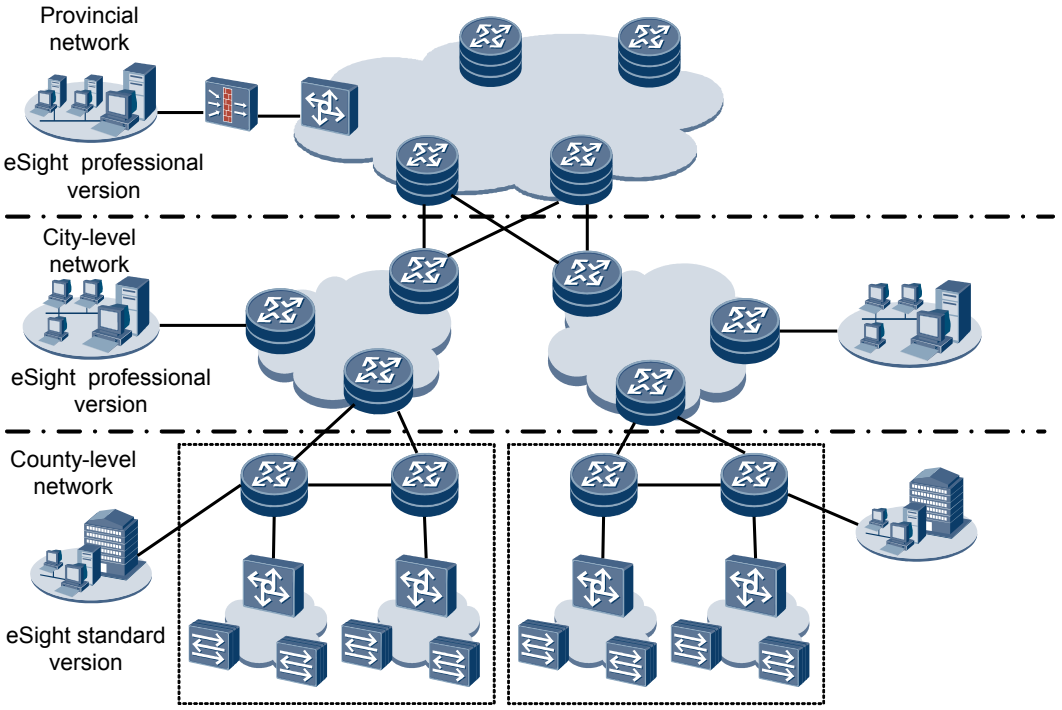
The hierarchical network management mechanism of eSight enables users to divide management areas and construct a layer-based management system based on the geographical area and organization structure. Upper-layer NMSs have higher rights than lower-layer NMSs. Upper-layer NMSs have rights to manage lower-layer NMSs; however, lower-layer NMSs have no right to manage upper-layer NMSs.

13.4.1.1 Lower-Layer NMS Application

The hierarchical network management mechanism enables multiple NMSs to share the management responsibilities and reduces the management pressure.

See **Figure 13-2**. 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 13-2 Lower-Layer NMS application



13.4.1.2 Lower-Layer NMS Function

This topic describes the basic functions of the hierarchical network management.

Copyright © Huawei Technologies Co., Ltd.

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.

13.4.2 Managing a Lower-Layer NMS

This topic describes how to manage a lower-layer NMS.

13.4.2.1 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.

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

Step 3 Click **OK**.

----End

13.4.2.2 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.

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

Copyright © Huawei Technologies Co., Ltd.

Step 3 Query the 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

13.4.2.3 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.

Step 2 Click **Check Status**. eSight tests the connectivity of lower-layer NMSs.

NOTE

If you do not specify a lower-layer NMS, by default, eSight tests the connectivity of all lower-layer NMSs.

----End

13.5 Managing Licenses

You have permission for the eSight only after obtaining a license. The license file controls the resources and functions of the eSight.

13.5.1 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 13-6 describes the license information.

Table 13-6 License information

Item	Attribute	Description	Example
Basic License Information	Validity period	Date when the license file expires	2011-04-14

Copyright © Huawei Technologies Co., Ltd.

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 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	Fault management
	Supported or Not	Whether the function is supported by the license file	Supported

Procedure

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

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 **13.5.3 Importing a License File**.

----End

13.5.2 Obtaining an ESN

When the license is going to expire, you need to obtain the ESN of the computer. The ESN is used to apply for a license.

Prerequisites

The current user knows the network adapter number or MAC address of the eSight server.

Copyright © Huawei Technologies Co., Ltd.

Context

You can obtain an ESN by selecting the network adapter or entering the MAC address.

Procedure

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

Step 2 In the **License Management** window, click **Obtain ESN**.

Step 3 On the **Obtain ESN** page, obtain the 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

13.5.3 Importing a License File

If the original license of the eSight expires, you need to import a license file to 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.

Step 2 In the **License Management** window, click **Import License**.

Step 3 On the **Import License** page, click next to the **License file** text box and select a license file.

Step 4 Click **Import**.
The information about the imported license file is displayed.

Step 5 Click **Apply**.

----End

13.6 Backing Up and Restoring the Database

To ensure eSight database security, you must back up and restore the database in time.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable the maintenance tool on eSight server.

- In a Windows operating system, choose **Start** > **All Programs** > **eSight** > **Launch Maintenance Tools**.
- In a Linux operating system, execute the **run.sh** file in the **eSight\mttools\bin** directory.

Step 2 Connect to the URL for logging in to the maintenance tool by means of the client explorer.

URL example: http://10.135.23.61:8889.

NOTE

- The port number is fixed at **8889**.
- The default username is **admin** and password is **Changeme123**.

Step 3 Click **Set backup path** to set the path for saving backup files, and click **OK**.

NOTE

The default backup folder is **backupdata**, which is in the same path as the eSight installation directory.

Step 4 Click **Back Up**, set **Description**, and click **Backup**.

Step 5 **Optional:** Click  as required to restore the database.

Step 6 **Optional:** Select a backup task and click **Delete** to delete the backup task and the corresponding backed up files.

----End

13.7 Managing NE Packages

This topic describes how to install and upgrade NE packages.

Prerequisites

You are an NMS user with "super administrator" authority.

NE packages to be installed or upgraded have been obtained.

The NE package management tool has been started on the eSight server.

- Windows operating system: Double-click the **startup.bat** file in **eSight\mttools\bin\runtime.maintenance\bin**.
- Linux operating system: Double-click the **startup.sh** file in **eSight\mttools\bin\runtime.maintenance\bin**.

Context

NE packages can only be installed and upgraded and cannot be uninstalled or degraded.

The default user name and password for NE package management are the same as those for eSight. You can change the user name and password in eSight.

Do not stop Maintenance Tools or the database when the NE package management tool is running. If Maintenance Tools or the database stops unexpectedly, the NE package management

Copyright © Huawei Technologies Co., Ltd.

tool cannot work properly. You must restart Maintenance Tools and reinstall or re-upgrade NE packages.

To ensure that the NE package management tool manages NE packages successfully, do not change NE package data.

Procedure

Step 1 Open web browser, enter **http://eSight server IP address:8889/** in the address box, and press **Enter**.

Step 2 Choose **Component** > **NE Package Management**.

Step 3 Click **Upload NE Package**.

Step 4 On the **Upload NE Package** page, click to select the NE package to be installed or upgraded.

Step 5 Click 

.

Step 6 After successful upload, click **Back**.

Step 7 **Optional:** Click **Collapse All** or **Expand All** to view the detailed NE package information.

NOTE

To quickly search for an NE package, click **Search**. Fuzzy search is supported.

Step 8 Click or in the **Operation** column.

Step 9 In the **Information** window, click **Yes**.

Step 10 In the **Task List** area, view the current task status.

NOTE

If the task fails to be performed, the failure cause is displayed in the **Remarks** column. To facilitate reinstallation or reupgrade, the icon changes to or in the **Operation** column.

----End

Copyright © Huawei Technologies Co., Ltd.

14 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.

Copyright © Huawei Technologies Co., Ltd.

14.1 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. Refer to the table during the maintenance of the eSight.

Table 14-1 List of maintenance items

Maintenance Period	Routine Maintenance Task
Daily	**14.3.1 Browsing Current Alarms**
	14.3.2 Querying Security Logs
	14.3.3 Backing Up and Restoring the Database
Weekly	**14.4.1 Checking the Disk Status of the eSight Server**
	14.4.2 Checking the Disk Space of the eSight Server
	14.4.3 Checking Oracle Database Logs
	14.4.4 Checking the Running Status of Anti-Virus Software
	14.4.5 Checking the Logs of the OS
	14.4.6 Checking MySQL Database Logs
Monthly	**14.5.1 Changing the Password of the Current eSight User**
	14.5.2 Checking the Server Time of the eSight
	14.5.3 Releasing the Disk Space of the eSight Server
Quarterly	**14.6.1 Checking the Equipment Room Environment**
	14.6.2 Checking the Power Supply of the eSight Server
	14.6.3 Checking Hardware and Peripherals of the eSight Server

14.2 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 **support@huawei.com**. Go to **http://support.huawei.com** to obtain the latest technical materials of Huawei.

Before seeking technical support, collect the relevant information.

Copyright © Huawei Technologies Co., Ltd.

14.3 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.

14.3.1 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 the alarms have the same alarm source, location information, and alarm ID, the alarms are merged to one record.
- If the current filter criteria are modified, the system searches for alarms based on the modified filter criteria.

Procedure

Step 1 Choose **Fault** > **Current Alarms** from the main menu.

Step 2 In the **Current Alarms** window, select filter criteria from the **Filter criteria** drop-down list and perform a search. You can customize filter criteria if required. For details, see **5.3.3 Creating an Alarm Filter Rule**.

Step 3 In the **Current Alarms** window, you can perform the following steps:

Copyright © Huawei Technologies Co., Ltd.

Management Alarms	Operation Method	Description
Lock alarms	Click **Lock**. The alarms in the current list are locked. In addition, **Lock** is automatically changed to **Unlock**.	If the alarms in the current list are locked, note that: ● Newly reported alarms can be displayed in the current alarm list only after you click **Unlock**. ● 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. ● If you acknowledge or clear an alarm when you click **Lock**, the alarm can be updated to the historical alarm list only when you click **Unlock**.
Unlock alarms	Click **Unlock**. The eSight reports alarms to the alarm list automatically. In addition, **Unlock** is automatically changed to **Lock**.	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: ● Click **Search** without setting any search criteria. All alarms are displayed in the current list. ● 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 **Search**.	-
Acknowledge	Select one or more alarms and click **Acknowledge**.	● If the alarm is acknowledged, **Acknowledged By** displays the user who acknowledges the alarm. ● If the alarm is unacknowledged, **Acknowledged By** displays  .
Unacknowledge	Select one or more alarms and choose **More** > **Unacknowledge**.	After an alarm is unacknowledged, its status is changed from **Acknowledged** to **Unacknowledged**.

Copyright © Huawei Technologies Co., Ltd.

Management Alarms	Operation Method	Description
Clear	Select one or more uncleared alarms and click **Clear**.	● The background color of clear alarms is green. ● The background color of uncleared alarms is white.
Alarm Mask	1. Click in the **Operation** column where the required alarm is located, and select **Mask Rules**. 2. In the **Mask Rules** dialog box, set the rule name and shielding date. Click **OK**.	● The newly created alarm mask rule is in enabled status by default. ● 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. ● You cannot set a masking rule for a performance alarm or clear alarm.
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 **OK**.	-
Locate to Topo	Click  in the **Operation** column where the required alarm record is located.	eSight locates the NE in the managed object that generates the alarm in the topology view.
Alarm Details	Click **Alarm Name** of which you want to view details.	The **Alarm Details** dialog box displays the name, probable cause, and proposed repair actions for the selected alarm.
Alarm Logs	Click **Number of Occurrences** about which you want to view the log information.	The **Alarm Logs** dialog box displays the alarm log related to this alarm record.
Export	Select one or more alarms and choose **Export** > **Selected Records** to export the alarm information. If you want to export all alarms, choose **Export** > **All**.	-

----End

Copyright © Huawei Technologies Co., Ltd.

14.3.2 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.

Step 2 In the **Log Management** window, select **Query Logs** > **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**.

----End

14.3.3 Backing Up and Restoring the Database

To ensure eSight database security, you must back up and restore the database in time.

Procedure

Step 1 Enable the maintenance tool on eSight server.

- In a Windows operating system, choose **Start** > **All Programs** > **eSight** > **Launch Maintenance Tools**.
- In a Linux operating system, execute the **run.sh** file in the **eSight\mttools\bin** directory.

Step 2 Connect to the URL for logging in to the maintenance tool by means of the client explorer.

URL example: http://10.135.23.61:8889.

NOTE

- The port number is fixed at **8889**.
- The default username is **admin** and password is **Changeme123**.

Step 3 Click **Set backup path** to set the path for saving backup files, and click **OK**.

NOTE

The default backup folder is **backupdata**, which is in the same path as the eSight installation directory.

Step 4 Click **Back Up**, set **Description**, and click **Backup**.

Step 5 **Optional:** Click  as required to restore the database.

Copyright © Huawei Technologies Co., Ltd.

Step 6 **Optional:** Select a backup task and click **Delete** to delete the backup task and the corresponding backed up files.

----End

14.4 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.

14.4.1 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.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

If a disk does not function properly, contact the equipment supplier to repair or replace the disk in a timely manner.

14.4.2 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%.

14.4.3 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.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

See error information in the log file to rectify faults. If a fault persists, contact Oracle technical support.

14.4.4 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.

14.4.5 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:

Copyright © Huawei Technologies Co., Ltd.

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.

14.4.6 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.

14.5 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.

14.5.1 Changing the Password of the Current eSight User

This topic describes how to change the password of your account. It is suggested that you should change the password periodically to improve the password security of your account.

Prerequisites

The new password must comply with the password policy.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **System** > **User Settings**.

Step 2 In the navigation tree on the left, choose **Basic Settings** > **Change Password**.

Step 3 Set the new password for the current user and click **Apply**.

----End

14.5.2 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.

14.5.3 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.

Copyright © Huawei Technologies Co., Ltd.

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

14.6 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.

14.6.1 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

Item	Index
Temperature	Range: 15°C-35°C
Humidity	Range: 40%-65%
Dust condition	Clear and spotless

Copyright © Huawei Technologies Co., Ltd.

Item	Index
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.

14.6.2 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

Copyright © Huawei Technologies Co., Ltd.

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.

14.6.3 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.

Copyright © Huawei Technologies Co., Ltd.

15 Command Reference

About This Chapter

This topic describes commonly-used commands for maintaining the eSight.

15.1 eSight Command Reference
This topic describes eSight commands and their functions.

15.2 Oracle Database Command Reference
This topic describes common Oracle database commands and their functions and application cases.

Copyright © Huawei Technologies Co., Ltd.

15.1 eSight Command Reference

This topic describes eSight commands and their functions.

15.1.1 Starting the eSight Process and the Online Help Process

This topic describes the command reference for starting the eSight process and the online help process.

Prerequisite

The database is started.

Context

The eSight still runs properly after you start the processes successfully and exit the command line interface (CLI).

Procedure

You can start the eSight process and the online help process in the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **run.bat**
- **Input Example**
  1. Log in to the server as the **Administrator** user.
  2. Run the following command to switch the directory:

     cd /d eSight_ROOT\AppBase\bin

     NOTE

     eSight_ROOT is the eSight installation directory.
  3. Run the following command to start the eSight process and the online help process:

     run.bat

     NOTE

     A new command line window is open when this command runs.
- **Output Example**

  After the command is successfully executed, the following information is displayed:

```
[10:50:44] Help System: started
[10:51:35] Loading kernel
    [10:51:35] com.huawei.oms.bootstage: started
    [10:51:38] org.eclipse.virgo.kernel.userregion.springdm: started
    [10:51:41] org.eclipse.virgo.web: started
    [10:51:50] com.huawei.oms.base: started
    [10:52:29] com.huawei.oms.web.portal: started
[10:52:29] Loading PKG
    [10:52:32] com.huawei.oms.app.audit: started
    [10:52:35] com.huawei.oms.app.autodiscovery: started
```


Copyright © Huawei Technologies Co., Ltd.

```
    [10:52:38] com.huawei.oms.app.dump: started
    [10:52:41] com.huawei.oms.app.email: started
    [10:52:53] com.huawei.oms.app.license.monitor: started
    [10:52:56] com.huawei.oms.app.license: started
    [10:52:59] com.huawei.oms.app.nbi: started
    [10:53:02] com.huawei.oms.app.panel: started
    [10:53:14] com.huawei.oms.app.pm: started
    [10:53:26] com.huawei.oms.framework.core: started
    [10:53:26] com.huawei.oms.app.sm: started
    [10:53:26] com.huawei.oms.app.topo: started
    [10:53:32] com.huawei.oms.framework.eam: started
    [10:53:32] com.huawei.oms.framework.med.center: started
    [10:53:32] com.huawei.oms.framework.med.node: started
    [10:53:35] com.huawei.oms.framework.nem: started
    [10:53:35] com.huawei.oms.sdk.audit: started
    [10:53:35] com.huawei.oms.sdk.eam: started
    [10:53:35] com.huawei.oms.app.integrated: started
    [10:53:36] com.huawei.oms.sdk.fm: started
    [10:53:39] com.huawei.oms.app.fm: started
    [10:53:45] com.huawei.oms.sdk.med: started
    [10:53:45] com.huawei.oms.sdk.momgr: started
    [10:53:45] com.huawei.oms.sdk.topo: started
    [10:53:45] com.huawei.oms.sdk.sm: started
    [10:53:54] com.huawei.oms.test: started
[10:53:54] Activing system
    [10:53:54] MORE service: actived
    [10:53:54] PM SnmpByTable: actived
    [10:53:54] LICENSE: actived
    [10:53:54] PM SnmpByIndex: actived
    [10:53:54] MOPKG: actived
    [10:53:54] PM: actived
    [10:53:54] EAM AS: actived
    [10:53:54] TOPO: actived
    [10:53:57] FM probe: actived
    [10:53:57] FM: actived
    [10:54:00] EAM DS: actived
    [10:54:00] SM: actived
    [10:54:00] EAM IconMgr: actived
[10:54:00] System start completely
Finished
```

Linux

- **Format**: **run.sh**
- **Input Example**

  1. Log in to the server as user **root**.
  2. Run the following command to switch the directory:

     cd eSight_ROOT/AppBase/bin
  3. Run the following command to start the eSight process and the online help process:

     ./run.sh

     NOTE

     A new command line window is open when this command runs.

- **Output Example**

  After the command is successfully executed, the following information is displayed:

```
[11:00:35] Help System: started
[11:00:42] Loading kernel
    [11:00:42] com.huawei.oms.bootstage: started
    [11:00:45] org.eclipse.virgo.kernel.userregion.springdm: started
    [11:00:48] org.eclipse.virgo.web: started
    [11:00:51] com.huawei.oms.base: started
    [11:01:12] com.huawei.oms.web.portal: started
[11:01:12] Loading PKG
```


Copyright © Huawei Technologies Co., Ltd.

```
    [11:01:12] com.huawei.oms.sdk.sm: started
    [11:01:15] com.huawei.oms.sdk.med: started
    [11:01:15] com.huawei.oms.framework.med.center: started
    [11:01:15] com.huawei.oms.app.audit: started
    [11:01:18] com.huawei.oms.app.license.monitor: started
    [11:01:18] com.huawei.oms.app.panel: started
    [11:01:21] com.huawei.oms.app.license: started
    [11:01:21] com.huawei.oms.app.sm: started
    [11:01:21] com.huawei.oms.app.nbi: started
    [11:01:21] com.huawei.oms.sdk.audit: started
    [11:01:21] com.huawei.oms.sdk.fm: started
    [11:01:21] com.huawei.oms.sdk.momgr: started
    [11:01:21] com.huawei.oms.app.autodiscovery: started
    [11:01:24] com.huawei.oms.app.dump: started
    [11:01:24] com.huawei.oms.framework.nem: started
    [11:01:27] com.huawei.oms.test: started
    [11:01:27] com.huawei.oms.sdk.topo: started
    [11:01:27] com.huawei.oms.sdk.eam: started
    [11:01:27] com.huawei.oms.framework.core: started
    [11:01:27] com.huawei.oms.framework.eam: started
    [11:01:27] com.huawei.oms.app.integrated: started
    [11:01:27] com.huawei.oms.framework.med.node: started
    [11:01:30] com.huawei.oms.app.fm: started
    [11:01:33] com.huawei.oms.app.email: started
    [11:01:36] com.huawei.oms.app.topo: started
    [11:01:39] com.huawei.oms.app.pm: started
[11:01:39] Activing system
    [11:01:39] MORE service: actived
    [11:01:39] LICENSE: actived
    [11:01:39] MOPKG: actived
    [11:01:39] PM SnmpByTable: actived
    [11:01:39] PM SnmpByIndex: actived
    [11:01:39] PM: actived
    [11:01:39] EAM AS: actived
    [11:01:39] TOPO: actived
    [11:01:42] FM probe: actived
    [11:01:42] FM: actived
    [11:01:42] EAM IconMgr: actived
    [11:01:42] EAM DS: actived
    [11:01:42] SM: actived
[11:01:42] System start completely
Finished
```

15.1.2 Stopping the eSight Process and the Online Help Process

This topic describes the command reference for stopping the eSight process and the online help process.

You can start the eSight process and the online help process in the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **stop.bat**
- **Input Example**

  1. Log in to the server as the **Administrator** user.
  2. Run the following command to switch the directory:

     cd /d eSight_ROOT\AppBase\bin

     NOTE

     eSight_ROOT is the eSight installation directory.

Copyright © Huawei Technologies Co., Ltd.

3. Run the following command to start the eSight process and the online help process:

   stop.bat

   NOTE

   A new command line window is open when this command runs.

- **Output Example**

  After the command is successfully executed, the following information is displayed:

```
[11:00:18] Base Module: stopped
[11:00:18] Kernel Module: stopped
[11:00:19] Help System: stopped
Finished
```

Linux

- **Format**: **stop.sh**
- **Input Example**

  1. Log in to the server as user **root**.
  2. Run the following command to switch the directory:

     cd eSight_ROOT/AppBase/bin
  3. Run the following command to start the eSight process and the online help process:

     ./stop.sh

     NOTE

     A new command line window is open when this command runs.

- **Output Example**

  After the command is successfully executed, the following information is displayed:

```
[11:03:40] Base Module: stopped
[11:03:40] Kernel Module: stopped
[11:03:44] Help System: stopped
Finished
```

15.1.3 Viewing a Log Level

This topic describes the command for viewing a log level.

Prerequisite

The database is started.

Procedure

You can view the log level in the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **omscli.bat log** < [**all** | **logname**] >
- **Input Example**

  1. Log in to the server as the **Administrator** user.

Copyright © Huawei Technologies Co., Ltd.

2. Run the following command to switch the directory:

   cd /d eSight_ROOT\AppBase\bin\runtime.center\bin

   NOTE

   eSight_ROOT is the eSight installation directory.

3. Run the following command to start the eSight process:

   startup.bat

4. Run the following command to view the log level.
   - View the levels of all logs:

     omscli.bat log *all*
   - View the level of a module log.

     For example, run the following command to view the level of the **bme** log:

     omscli.bat log *bme*

- **Output Example**
  - After the command is successfully executed, the levels of all logs are displayed as follows:

```
No   Name                 Level
File
1    apache               WARN   D:\OMS\var\runtime.center\log\oms\core
\apache.log
2    asutil               DEBUG  D:\OMS\var\runtime.center\log\oms\asutil
\asutil.log
3    base                 DEBUG  D:\OMS\var\runtime.center\log\oms\core
\base.log
4    bme                  DEBUG  D:\OMS\var\runtime.center\log\bme
\bme.log
5    cache                DEBUG  D:\OMS\var\runtime.center\log\oms\core
\cache.log
6    configure            DEBUG  D:\OMS\var\runtime.center\log\oms\core
\configure.log
7    dbevtutil            DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\dbevtutil.log
8    dis_frame            DEBUG  D:\OMS\var\runtime.center\log\oms\autodis
\dis_frame.log
9    dis_lldp             DEBUG  D:\OMS\var\runtime.center\log\oms\autodis
\dis_lldp.log
10   dis_snmp             DEBUG  D:\OMS\var\runtime.center\log\oms\autodis
\dis_snmp.log
11   dump_ds              DEBUG  D:\OMS\var\runtime.center\log\oms\dump
\dump_ds.log
12   dump_support         DEBUG  D:\OMS\var\runtime.center\log\oms\dump
\dump_support.log
13   dump_ui              DEBUG  D:\OMS\var\runtime.center\log\oms\dump
\dump_ui.log
14   eam_as               DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\eam_as.log
15   eam_ds               DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\eam_ds.log
16   eam_sdk              DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\eam_sdk.log
17   eam_test             DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\eam_test.log
18   eam_ui               DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\eam_ui.log
19   email                DEBUG  D:\OMS\var\runtime.center\log\oms\email
\email.log
20   email.server.support DEBUG  D:\OMS\var\runtime.center\log\oms\email
\email.server.support.log
21   event                DEBUG  D:\OMS\var\runtime.center\log\oms\core
\event.log
22   fm                   DEBUG  D:\OMS\var\runtime.center\log\oms\fm
```


Copyright © Huawei Technologies Co., Ltd.

```
\fm.log
23   fmbackup              DEBUG  D:\OMS\var\runtime.center\log\oms\fm
\fmbackup.log
24   fmcolor               DEBUG  D:\OMS\var\runtime.center\log\oms\fm
\fmcolor.log
25   fmconnect             DEBUG  D:\OMS\var\runtime.center\log\oms\fm
\fmconnect.log
26   fmprobe               DEBUG  D:\OMS\var\runtime.center\log\oms\fm
\fmprobe.log
27   fmtest                DEBUG  D:\OMS\var\runtime.center\log\oms\fm
\fmtest.log
28   fmui                  DEBUG  D:\OMS\var\runtime.center\log\oms\fm
\fmui.log
29   framework.portal.ds   DEBUG  D:\OMS\var\runtime.center\log\oms\core
\framework.portal.ds.log
30   fsm                   DEBUG  D:\OMS\var\runtime.center\log\oms\core
\fsm.log
31   ftp.client            DEBUG  D:\OMS\var\runtime.center\log\oms\med
\ftp.client.log
32   ftp.med               DEBUG  D:\OMS\var\runtime.center\log\oms\med
\ftp.med.log
33   ftp.server            DEBUG  D:\OMS\var\runtime.center\log\oms\med
\ftp.server.log
34   iconmgr               DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\iconmgr.log
35   ip.validate           DEBUG  D:\OMS\var\runtime.center\log\oms\core
\ip.validate.log
36   log.mgmt              DEBUG  D:\OMS\var\runtime.center\log\oms\core
\log.mgmt.log
37   mapping               DEBUG  D:\OMS\var\runtime.center\log\oms\topo
\mapping.log
38   med                   DEBUG  D:\OMS\var\runtime.center\log\oms\med
\med.log
39   med.enter             DEBUG  D:\OMS\var\runtime.center\log\oms\med
\med.enter.log
40   med.node              DEBUG  D:\OMS\var\runtime.center\log\oms\med
\med.node.log
41   med.util              DEBUG  D:\OMS\var\runtime.center\log\oms\med
\med.util.log
42   mim                   DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\mim.log
43   mimcache              DEBUG  D:\OMS\var\runtime.center\log\oms\eam
\mimcache.log
44   mml.client            DEBUG  D:\OMS\var\runtime.center\log\oms\med
\mml.client.log
45   mml.med               DEBUG  D:\OMS\var\runtime.center\log\oms\med
\mml.med.log
46   moTypeUpdate          DEBUG  D:\OMS\var\runtime.center\log\demo
\moTypeUpdate.log
47   moconfig              DEBUG  D:\OMS\var\runtime.center\log\oms\momgr
\moconfig.log
48   monitor               DEBUG  D:\OMS\var\runtime.center\log\oms\license
\monitor.log
49   mopkg                 DEBUG  D:\OMS\var\runtime.center\log\oms\core
\mopkg.log
50   more                  DEBUG  D:\OMS\var\runtime.center\log\oms\momgr
\more.log
51   moservice             DEBUG  D:\OMS\var\runtime.center\log\demo
\moservice.log
52   moui                  DEBUG  D:\OMS\var\runtime.center\log\oms\momgr
\moui.log
53   nbi                   DEBUG  D:\OMS\var\runtime.center\log\oms\nbi
\nbi.log
54   nePermitGate          DEBUG  D:\OMS\var\runtime.center\log\oms\sm
\nePermitGate.log
55   oms.license.as        DEBUG  D:\OMS\var\runtime.center\log\oms\license
\oms.license.as.log
56   oms.license.ui        DEBUG  D:\OMS\var\runtime.center\log\oms\license
\oms.license.ui.log
```


Copyright © Huawei Technologies Co., Ltd.

```
57   oms_audit            DEBUG  D:\OMS\var\runtime.center\log\oms\audit
\oms_audit.log
58   oms_audit_as         DEBUG  D:\OMS\var\runtime.center\log\oms\audit
\oms_audit_as.log
59   panel_ds             DEBUG  D:\OMS\var\runtime.center\log\oms\panel
\panel_ds.log
60   panel_gapi           DEBUG  D:\OMS\var\runtime.center\log\oms\panel
\panel_gapi.log
61   panel_ui             DEBUG  D:\OMS\var\runtime.center\log\oms\panel
\panel_ui.log
62   persistence          DEBUG  D:\OMS\var\runtime.center\log\oms\core
\persistence.log
63   pm                   DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pm.log
64   pmdata               DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmdata.log
65   pmds                 DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmds.log
66   pmmeastype           DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmmeastype.log
67   pmprobe              DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmprobe.log
68   pmtest               DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmtest.log
69   pmthreshold          DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmthreshold.log
70   pmui                 DEBUG  D:\OMS\var\runtime.center\log\oms\pm
\pmui.log
71   portal.client        DEBUG  D:\OMS\var\runtime.center\log\oms\core
\portal.client.log
72   portal.server        DEBUG  D:\OMS\var\runtime.center\log\oms\core
\portal.server.log
73   root                 DEBUG  D:\OMS\var\runtime.center\log
\root.log
74   sbus                 DEBUG  D:\OMS\var\runtime.center\log\oms\core
\sbus.log
75   sbus.client          DEBUG  D:\OMS\var\runtime.center\log\oms\core
\sbus.client.log
76   sbus.heartbeat       DEBUG  D:\OMS\var\runtime.center\log\oms\core
\sbus.heartbeat.log
77   sbus.server          DEBUG  D:\OMS\var\runtime.center\log\oms\core
\sbus.server.log
78   sm                   DEBUG  D:\OMS\var\runtime.center\log\oms\sm
\sm.log
79   snmp4j               DEBUG  D:\OMS\var\runtime.center\log\oms\med
\snmp4j.log
80   ssh.client           DEBUG  D:\OMS\var\runtime.center\log\oms\med
\ssh.client.log
81   ssh.med              DEBUG  D:\OMS\var\runtime.center\log\oms\med
\ssh.med.log
82   task                 DEBUG  D:\OMS\var\runtime.center\log\oms\core
\task.log
83   telnet.client        DEBUG  D:\OMS\var\runtime.center\log\oms\med
\telnet.client.log
84   telnet.med           DEBUG  D:\OMS\var\runtime.center\log\oms\med
\telnet.med.log
85   topo_ds              DEBUG  D:\OMS\var\runtime.center\log\oms\topo
\topo_ds.log
86   topo_sdk             DEBUG  D:\OMS\var\runtime.center\log\oms\topo
\topo_sdk.log
87   topo_ui              DEBUG  D:\OMS\var\runtime.center\log\oms\topo
\topo_ui.log
88   topomgr              DEBUG  D:\OMS\var\runtime.center\log\oms\topo
\topomgr.log
```

- After the command is successfully executed, the level of the **bme** log is displayed as follows:

```
No   Name  Level  File
1    bme   DEBUG  D:\OMS\var\runtime.center\log\bme\bme.log
```


Copyright © Huawei Technologies Co., Ltd.

Linux

- **Format**: **omscli.sh log** < [**all** | **logname**] >
- **Input Example**

  1. Log in to the server as the **root** user.
  2. Run the following command to switch the directory:

     cd eSight_ROOT/AppBase/bin/runtime.center/bin
  3. Run the following command to start the eSight process:

     ./startup.sh
  4. Run the following command to view the log level.
     - View the levels of all logs:

       ./omscli.sh log *all*
     - View the level of a module log.

       For example, run the following command to view the level of the **bme** log:

       ./omscli.sh log *bme*

- **Output Example**
  - After the command is successfully executed, the levels of all logs are displayed as follows:

```
No   Name                 Level
File
1    apache               WARN   /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/apache.log
2    asutil               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/asutil/asutil.log
3    base                 DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/base.log
4    bme                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/bme/bme.log
5    cache                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/cache.log
6    configure            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/configure.log
7    dbevtutil            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/dbevtutil.log
8    dis_frame            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/autodis/dis_frame.log
9    dis_lldp             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/autodis/dis_lldp.log
10   dis_snmp             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/autodis/dis_snmp.log
11   dump_ds              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/dump/dump_ds.log
12   dump_support         DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/dump/dump_support.log
13   dump_ui              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/dump/dump_ui.log
14   eam_as               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/eam_as.log
15   eam_ds               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/eam_ds.log
16   eam_sdk              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/eam_sdk.log
17   eam_test             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/eam_test.log
18   eam_ui               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/eam_ui.log
19   email                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/email/email.log
20   email.server.support DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
```


Copyright © Huawei Technologies Co., Ltd.

```
runtime.center/log/oms/email/email.server.support.log
21   event                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/event.log
22   fm                   DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fm.log
23   fmbackup             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fmbackup.log
24   fmcolor              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fmcolor.log
25   fmconnect            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fmconnect.log
26   fmprobe              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fmprobe.log
27   fmtest               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fmtest.log
28   fmui                 DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/fm/fmui.log
29   framework.portal.ds  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/framework.portal.ds.log
30   fsm                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/fsm.log
31   ftp.client           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/ftp.client.log
32   ftp.med              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/ftp.med.log
33   ftp.server           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/ftp.server.log
34   iconmgr              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/iconmgr.log
35   ip.validate          DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/ip.validate.log
36   log.mgmt             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/log.mgmt.log
37   mapping              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/topo/mapping.log
38   med                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/med.log
39   med.enter            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/med.enter.log
40   med.node             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/med.node.log
41   med.util             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/med.util.log
42   mim                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/mim.log
43   mimcache             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/eam/mimcache.log
44   mml.client           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/mml.client.log
45   mml.med              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/mml.med.log
46   moTypeUpdate         DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/demo/moTypeUpdate.log
47   moconfig             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/momgr/moconfig.log
48   monitor              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/license/monitor.log
49   mopkg                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/mopkg.log
50   more                 DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/momgr/more.log
51   moservice            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/demo/moservice.log
52   moui                 DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/momgr/moui.log
53   nbi                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/nbi/nbi.log
54   nePermitGate         DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/sm/nePermitGate.log
```


Copyright © Huawei Technologies Co., Ltd.

```
55   oms.license.as        DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/license/oms.license.as.log
56   oms.license.ui        DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/license/oms.license.ui.log
57   oms_audit             DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/audit/oms_audit.log
58   oms_audit_as          DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/audit/oms_audit_as.log
59   panel_ds              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/panel/panel_ds.log
60   panel_gapi            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/panel/panel_gapi.log
61   panel_ui              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/panel/panel_ui.log
62   persistence           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/persistence.log
63   pm                    DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pm.log
64   pmdata                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmdata.log
65   pmds                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmds.log
66   pmmeastype            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmmeastype.log
67   pmprobe               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmprobe.log
68   pmtest                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmtest.log
69   pmthreshold           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmthreshold.log
70   pmui                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/pm/pmui.log
71   portal.client         DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/portal.client.log
72   portal.server         DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/portal.server.log
73   root                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/root.log
74   sbus                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/sbus.log
75   sbus.client           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/sbus.client.log
76   sbus.heartbeat        DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/sbus.heartbeat.log
77   sbus.server           DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/sbus.server.log
78   sm                    DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/sm/sm.log
79   snmp4j                DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/snmp4j.log
80   ssh.client            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/ssh.client.log
81   ssh.med               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/ssh.med.log
82   task                  DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/core/task.log
83   telnet.client         DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/telnet.client.log
84   telnet.med            DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/med/telnet.med.log
85   topo_ds               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/topo/topo_ds.log
86   topo_sdk              DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/topo/topo_sdk.log
87   topo_ui               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/topo/topo_ui.log
88   topomgr               DEBUG  /opt/OMS/OMS_run/17_12_sub/var/
runtime.center/log/oms/topo/topomgr.log
```


Copyright © Huawei Technologies Co., Ltd.

- After the command is successfully executed, the level of the **bme** log is displayed as follows:

```
No    Name   Level
File
1     bme    DEBUG  /opt/OMS/SUBtr51201/../../var/runtime.center/log/bme/
bme.log
```

15.1.4 Changing a Log Level

This topic describes the command for changing a log level.

Prerequisite

The database is started.

Procedure

You can change the log level in the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **omscli.bat log** < [**all** | **logname**] > < [**level** | **default**] >
- **Input Example**
  1. Log in to the server as the **Administrator** user.
  2. Run the following command to switch the directory:

     cd /d eSight_ROOT\AppBase\bin\runtime.center\bin

     NOTE

     eSight_ROOT is the eSight installation directory.
  3. Run the following command to start the eSight process:

     startup.bat
  4. Run the following command to change the log level.
     - Change the levels of all logs.

       For example, change the levels of all logs to **error**:

       omscli.bat log *all error*
     - Change the level of a module log.

       For example, change the level of the **bme** log to **debug**:

       omscli.bat log *bme debug*
- **Output Example**
  - After the command is successfully executed, the levels of all logs are changed to **error**. The output information is as follows:

```
Change log level of apache              from WARN  to ERROR
Change log level of asutil              from DEBUG to ERROR
Change log level of base                from DEBUG to ERROR
Change log level of bme                 from DEBUG to ERROR
Change log level of cache               from DEBUG to ERROR
Change log level of configure           from DEBUG to ERROR
Change log level of dbevtutil           from DEBUG to ERROR
Change log level of dis_frame           from DEBUG to ERROR
Change log level of dis_lldp            from DEBUG to ERROR
```


Copyright © Huawei Technologies Co., Ltd.

```
Change log level of dis_snmp             from DEBUG to ERROR
Change log level of dump_ds              from DEBUG to ERROR
Change log level of dump_support         from DEBUG to ERROR
Change log level of dump_ui              from DEBUG to ERROR
Change log level of eam_as               from DEBUG to ERROR
Change log level of eam_ds               from DEBUG to ERROR
Change log level of eam_sdk              from DEBUG to ERROR
Change log level of eam_test             from DEBUG to ERROR
Change log level of eam_ui               from DEBUG to ERROR
Change log level of email                from DEBUG to ERROR
Change log level of email.server.support from DEBUG to ERROR
Change log level of event                from DEBUG to ERROR
Change log level of fm                   from DEBUG to ERROR
Change log level of fmbackup             from DEBUG to ERROR
Change log level of fmcolor              from DEBUG to ERROR
Change log level of fmconnect            from DEBUG to ERROR
Change log level of fmprobe              from DEBUG to ERROR
Change log level of fmtest               from DEBUG to ERROR
Change log level of fmui                 from DEBUG to ERROR
Change log level of framework.portal.ds  from DEBUG to ERROR
Change log level of fsm                  from DEBUG to ERROR
Change log level of ftp.client           from DEBUG to ERROR
Change log level of ftp.med              from DEBUG to ERROR
Change log level of ftp.server           from DEBUG to ERROR
Change log level of iconmgr              from DEBUG to ERROR
Change log level of ip.validate          from DEBUG to ERROR
Change log level of log.mgmt             from DEBUG to ERROR
Change log level of mapping              from DEBUG to ERROR
Change log level of med                  from DEBUG to ERROR
Change log level of med.enter            from DEBUG to ERROR
Change log level of med.node             from DEBUG to ERROR
Change log level of med.util             from DEBUG to ERROR
Change log level of mim                  from DEBUG to ERROR
Change log level of mimcache             from DEBUG to ERROR
Change log level of mml.client           from DEBUG to ERROR
Change log level of mml.med              from DEBUG to ERROR
Change log level of moTypeUpdate         from DEBUG to ERROR
Change log level of moconfig             from DEBUG to ERROR
Change log level of monitor              from DEBUG to ERROR
Change log level of mopkg                from DEBUG to ERROR
Change log level of more                 from DEBUG to ERROR
Change log level of moservice            from DEBUG to ERROR
Change log level of moui                 from DEBUG to ERROR
Change log level of nbi                  from DEBUG to ERROR
Change log level of nePermitGate         from DEBUG to ERROR
Change log level of oms.license.as       from DEBUG to ERROR
Change log level of oms.license.ui       from DEBUG to ERROR
Change log level of oms_audit            from DEBUG to ERROR
Change log level of oms_audit_as         from DEBUG to ERROR
Change log level of panel_ds             from DEBUG to ERROR
Change log level of panel_gapi           from DEBUG to ERROR
Change log level of panel_ui             from DEBUG to ERROR
Change log level of persistence          from DEBUG to ERROR
Change log level of pm                   from DEBUG to ERROR
Change log level of pmdata               from DEBUG to ERROR
Change log level of pmds                 from DEBUG to ERROR
Change log level of pmmeastype           from DEBUG to ERROR
Change log level of pmprobe              from DEBUG to ERROR
Change log level of pmtest               from DEBUG to ERROR
Change log level of pmthreshold          from DEBUG to ERROR
Change log level of pmui                 from DEBUG to ERROR
Change log level of portal.client        from DEBUG to ERROR
Change log level of portal.server        from DEBUG to ERROR
Change log level of root                 from DEBUG to ERROR
Change log level of sbus                 from DEBUG to ERROR
Change log level of sbus.client          from DEBUG to ERROR
Change log level of sbus.heartbeat       from DEBUG to ERROR
Change log level of sbus.server          from DEBUG to ERROR
Change log level of sm                   from DEBUG to ERROR
```


Copyright © Huawei Technologies Co., Ltd.

```
Change log level of snmp4j              from DEBUG to ERROR
Change log level of ssh.client          from DEBUG to ERROR
Change log level of ssh.med             from DEBUG to ERROR
Change log level of task                from DEBUG to ERROR
Change log level of telnet.client       from DEBUG to ERROR
Change log level of telnet.med          from DEBUG to ERROR
Change log level of topo_ds             from DEBUG to ERROR
Change log level of topo_sdk            from DEBUG to ERROR
Change log level of topo_ui             from DEBUG to ERROR
Change log level of topomgr             from DEBUG to ERROR
```

- After the command is successfully executed, the level of the **bme** log is changed to **debug**. The output information is as follows:

```
Change log level of bme                 from ERROR to DEBUG
```

Linux

- **Format**: **omscli.sh log** < [**all** | **logname**] > < [**level** | **default**] >
- **Input Example**
  1. Log in to the server as the **root** user.
  2. Run the following command to switch the directory:

     cd eSight_ROOT/AppBase/bin/runtime.center/bin
  3. Run the following command to start the eSight process:

     ./startup.sh
  4. Run the following command to change the log level.
     - Change the levels of all logs.

       For example, run the following command to change the levels of all logs to **error**:

       ./omscli.sh log *all error*
     - Change the level of a module log.

       For example, change the level of the **bme** log to **error**:

       ./omscli.sh log *bme error*
- **Output Example**
  - After the command is successfully executed, the levels of all logs are changed to **error**. The output information is as follows:

```
Change log level of apache              from WARN  to ERROR
Change log level of asutil              from DEBUG to ERROR
Change log level of base                from DEBUG to ERROR
Change log level of bme                 from DEBUG to ERROR
Change log level of cache               from DEBUG to ERROR
Change log level of configure           from DEBUG to ERROR
Change log level of dbevtutil           from DEBUG to ERROR
Change log level of dis_frame           from DEBUG to ERROR
Change log level of dis_lldp            from DEBUG to ERROR
Change log level of dis_snmp            from DEBUG to ERROR
Change log level of dump_ds             from DEBUG to ERROR
Change log level of dump_support        from DEBUG to ERROR
Change log level of dump_ui             from DEBUG to ERROR
Change log level of eam_as              from DEBUG to ERROR
Change log level of eam_ds              from DEBUG to ERROR
Change log level of eam_sdk             from DEBUG to ERROR
Change log level of eam_test            from DEBUG to ERROR
Change log level of eam_ui              from DEBUG to ERROR
Change log level of email               from DEBUG to ERROR
Change log level of email.server.support from DEBUG to ERROR
Change log level of event               from DEBUG to ERROR
Change log level of fm                  from DEBUG to ERROR
Change log level of fmbackup            from DEBUG to ERROR
```


Copyright © Huawei Technologies Co., Ltd.

```
Change log level of fmcolor              from DEBUG to ERROR
Change log level of fmconnect            from DEBUG to ERROR
Change log level of fmprobe              from DEBUG to ERROR
Change log level of fmtest               from DEBUG to ERROR
Change log level of fmui                 from DEBUG to ERROR
Change log level of framework.portal.ds  from DEBUG to ERROR
Change log level of fsm                  from DEBUG to ERROR
Change log level of ftp.client           from DEBUG to ERROR
Change log level of ftp.med              from DEBUG to ERROR
Change log level of ftp.server           from DEBUG to ERROR
Change log level of iconmgr              from DEBUG to ERROR
Change log level of ip.validate          from DEBUG to ERROR
Change log level of log.mgmt             from DEBUG to ERROR
Change log level of mapping              from DEBUG to ERROR
Change log level of med                  from DEBUG to ERROR
Change log level of med.enter            from DEBUG to ERROR
Change log level of med.node             from DEBUG to ERROR
Change log level of med.util             from DEBUG to ERROR
Change log level of mim                  from DEBUG to ERROR
Change log level of mimcache             from DEBUG to ERROR
Change log level of mml.client           from DEBUG to ERROR
Change log level of mml.med              from DEBUG to ERROR
Change log level of moTypeUpdate         from DEBUG to ERROR
Change log level of moconfig             from DEBUG to ERROR
Change log level of monitor              from DEBUG to ERROR
Change log level of mopkg                from DEBUG to ERROR
Change log level of more                 from DEBUG to ERROR
Change log level of moservice            from DEBUG to ERROR
Change log level of moui                 from DEBUG to ERROR
Change log level of nbi                  from DEBUG to ERROR
Change log level of nePermitGate         from DEBUG to ERROR
Change log level of oms.license.as       from DEBUG to ERROR
Change log level of oms.license.ui       from DEBUG to ERROR
Change log level of oms_audit            from DEBUG to ERROR
Change log level of oms_audit_as         from DEBUG to ERROR
Change log level of panel_ds             from DEBUG to ERROR
Change log level of panel_gapi           from DEBUG to ERROR
Change log level of panel_ui             from DEBUG to ERROR
Change log level of persistence          from DEBUG to ERROR
Change log level of pm                   from DEBUG to ERROR
Change log level of pmdata               from DEBUG to ERROR
Change log level of pmds                 from DEBUG to ERROR
Change log level of pmmeastype           from DEBUG to ERROR
Change log level of pmprobe              from DEBUG to ERROR
Change log level of pmtest               from DEBUG to ERROR
Change log level of pmthreshold          from DEBUG to ERROR
Change log level of pmui                 from DEBUG to ERROR
Change log level of portal.client        from DEBUG to ERROR
Change log level of portal.server        from DEBUG to ERROR
Change log level of root                 from DEBUG to ERROR
Change log level of sbus                 from DEBUG to ERROR
Change log level of sbus.client          from DEBUG to ERROR
Change log level of sbus.heartbeat       from DEBUG to ERROR
Change log level of sbus.server          from DEBUG to ERROR
Change log level of sm                   from DEBUG to ERROR
Change log level of snmp4j               from DEBUG to ERROR
Change log level of ssh.client           from DEBUG to ERROR
Change log level of ssh.med              from DEBUG to ERROR
Change log level of task                 from DEBUG to ERROR
Change log level of telnet.client        from DEBUG to ERROR
Change log level of telnet.med           from DEBUG to ERROR
Change log level of topo_ds              from DEBUG to ERROR
Change log level of topo_sdk             from DEBUG to ERROR
Change log level of topo_ui              from DEBUG to ERROR
Change log level of topomgr              from DEBUG to ERROR
```

- After the command is successfully executed, the level of the **bme** log is changed to **error**. The output information is as follows:

```
Change log level of bme                  from DEBUG to ERROR
```


Copyright © Huawei Technologies Co., Ltd.

15.1.5 Checking Whether the eSight Is Started

This topic describes the command for Checking Whether the eSight Is Started.

You can check whether the eSight is started on the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **omscli.bat checkstate startup**
- **Input Example**
  1. Log in to the server as the **Administrator** user.
  2. Run the following command to switch the directory:
     cd /d eSight_ROOT\AppBase\bin\runtime.center\bin
     NOTE
     eSight_ROOT is the eSight installation directory.
  3. Run the following command to check whether the eSight is started:
     omscli.bat checkstate startup
- **Output Example**
  After the command is successfully executed, the following information is displayed:
  ```
  System already loaded bundle.
  ```

Linux

- **Format**: **omscli.sh checkstate startup**
- **Input Example**
  1. Log in to the server as user **root**.
  2. Run the following command to switch the directory:
     cd eSight_ROOT/AppBase/bin/runtime.center/bin
  3. Run the following command to check whether the eSight is started:
     ./omscli.sh checkstate startup
- **Output Example**
  After the command is successfully executed, the following information is displayed:
  ```
  System already loaded bundle.
  ```

15.1.6 Viewing the Status of the eSight Process

This topic describes the command for Viewing the Status of the eSightProcess.

You can view the status of the eSight process on the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **omscli.bat checkstate process**

Copyright © Huawei Technologies Co., Ltd.

- **Input Example**

  1. Log in to the server as the **Administrator** user.
  2. Run the following command to switch the directory:

     cd /d eSight_ROOT\AppBase\bin\runtime.center\bin

     NOTE

     eSight_ROOT is the eSight installation directory.
  3. Run the following command to view the status of the eSight process:

     omscli.bat checkstate process

- **Output Example**

  After the command is successfully executed, the following information is displayed:

  ```
  System process already started.
  ```

Linux

- **Format**: **omscli.sh checkstate process**
- **Input Example**

  1. Log in to the server as user **root**.
  2. Run the following command to switch the directory:

     cd /d eSight_ROOT/AppBase/bin/runtime.center/bin
  3. Run the following command to view the status of the eSight process:

     ./omscli.sh checkstate process

- **Output Example**

  After the command is successfully executed, the following information is displayed:

  ```
  System process already started.
  ```

15.1.7 Viewing the SBus Information

This topic describes the command for viewing the Service Bus (SBus) information.

You can view the SBus information on the following operating systems:

- **Windows**
- **Linux**

Windows

- **Format**: **omscli.bat service** < [*all* | *ip* | *self*] >
- **Input Example**

  1. Log in to the server as the **Administrator** user.
  2. Run the following command to switch the directory:

     cd /d eSight_ROOT\AppBase\bin\runtime.center\bin

     NOTE

     eSight_ROOT is the eSight installation directory.
  3. Run the following command to view the SBus information:
     - View all service information that the eSight releases by using the SBus:

       omscli.bat service *all*

Copyright © Huawei Technologies Co., Ltd.

- View all service information that a remote environment releases by using the SBus. For example, view all service information of the environment with **12.62.34.228** as its IP address.

  ./omscli.sh service *12.62.34.228*

  omscli.bat service *12.62.34.228*

- View all service information that the current environment releases by using the SBus:

  omscli.bat service *self*

- **Output Example**
  - After the command is successfully executed, all service information that the eSight releases by using the SBus is displayed:

```
No   Host                  Type     Date                Interface

1    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.OperationDetailManager
2    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.OperationLogManager
3    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.SecurityLogManager
4    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.SystemLogManager
5    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:11
com.huawei.oms.app.dump
.api.DumpConfigManager
6    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:44
com.huawei.oms.app.pm.S
tatusChangedOperation
7    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:42
com.huawei.oms.app.pm.T
emplateManager
8    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:38
com.huawei.oms.app.pm.a
larm.AlarmManager
9    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:40
com.huawei.oms.app.pm.m
omgr.InternalPMProbeCenter
10   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:46
com.huawei.oms.app.pm.m
omgr.PMMoreManager
11   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.app.pm.m
onitoring.InternalMonitoringManager
12   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:51
com.huawei.oms.app.sm.a
pi.as.SecurityManager
13   12.66.90.215:31902    JSON     2012-02-28 11:08:51
com.huawei.oms.app.sm.a
pi.as.SecurityManager
14   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.OperationLogManager
15   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.SecurityLogManager
16   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.SystemLogManager
17   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:22
com.huawei.oms.eam.am.A
ccessManager
```


Copyright © Huawei Technologies Co., Ltd.

```
18   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:59
com.huawei.oms.eam.mim.
MITManager
19   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:13
com.huawei.oms.email.ap
i.emailserver.EmailServerManager
20   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.event.Ev
entService
21   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.event.Ev
entServiceExt
22   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:23
com.huawei.oms.fm.api.F
aultManager
23   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.api.p
robe.ProbeCenter
24   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.custo
mfault.CustomFaultManager
25   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.probe
dao.HandlerReaderDao
26   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:06
com.huawei.oms.fm.uiapi
.InternalFaultManager
27   12.66.90.215:31902    JSON     2012-02-28 11:08:55
com.huawei.oms.gapi.cor
e.mopkg.ChangeInfoMgr
28   12.66.90.215:31902    JSON     2012-02-28 11:07:38
com.huawei.oms.homepage
.ext.HomepageExtension
29   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:29
com.huawei.oms.license.
as.api.LicenseControl
30   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:29
com.huawei.oms.license.
as.api.LicenseManager
31   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:26
com.huawei.oms.log.mgmt
.LogMgmtService
32   12.66.90.215:31902    JSON     2012-02-28 11:07:26
com.huawei.oms.log.mgmt
.LogMgmtService
33   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:02
com.huawei.oms.med.Medi
ation
34   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:00
com.huawei.oms.momgr.ea
m.MOLifeCycleManager
35   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.momgr.ea
m.MOLifeCycleManager
36   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:40
com.huawei.oms.momgr.pm
.PMProbeCenter
37   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:30
com.huawei.oms.nbi.api.
ds.bus.INBIJsonEventService
38   12.66.90.215:31902    JSON     2012-02-28 11:08:30
com.huawei.oms.nbi.api.
ds.bus.INBIJsonEventService
39   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:22
com.huawei.oms.nem.more
.server.MoreService
40   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:14
com.huawei.oms.net.ftp.
server.FtpService
```


Copyright © Huawei Technologies Co., Ltd.

```
41   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:14
com.huawei.oms.net.ftp.
server.FtpsService
42   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:15
com.huawei.oms.net.ftp.
server.SftpService
43   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:45
com.huawei.oms.pm.DataC
enter
44   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.pm.monit
oring.MonitoringManager
45   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ValidateService
46   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.callback.CallbackService
47   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusHeartbeatService
48   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusInfoService
49   12.66.90.215:31902    JSON     2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusInfoService
50   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.sync.SyncService
51   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:51
com.huawei.oms.sm.as.ap
i.Administration
52   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:26
com.huawei.oms.task.Tas
kManager
53   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:06
com.huawei.oms.topo.map
ping.MappingManager
54   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:56
com.huawei.oms.topo.top omgr.TopoManager
```

- After the command is successfully executed, all service information of the environment with **12.62.34.228** as its IP address is displayed:

```
No   Host                  Type     Date                Interface

1    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.OperationDetailManager
2    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.OperationLogManager
3    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.SecurityLogManager
4    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.SystemLogManager
5    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:11
com.huawei.oms.app.dump
.api.DumpConfigManager
6    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:44
com.huawei.oms.app.pm.S
tatusChangedOperation
7    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:42
com.huawei.oms.app.pm.T
emplateManager
8    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:38
com.huawei.oms.app.pm.a
larm.AlarmManager
```


Copyright © Huawei Technologies Co., Ltd.

```
9    12.62.34.228:31903    HESSIAN  2012-02-28 11:08:40
com.huawei.oms.app.pm.m
omgr.InternalPMProbeCenter
10   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:46
com.huawei.oms.app.pm.m
omgr.PMMoreManager
11   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.app.pm.m
onitoring.InternalMonitoringManager
12   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:51
com.huawei.oms.app.sm.a
pi.as.SecurityManager
13   12.62.34.228:31902    JSON     2012-02-28 11:08:51
com.huawei.oms.app.sm.a
pi.as.SecurityManager
14   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.OperationLogManager
15   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.SecurityLogManager
16   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.SystemLogManager
17   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:22
com.huawei.oms.eam.am.A
ccessManager
18   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:59
com.huawei.oms.eam.mim.
MITManager
19   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:13
com.huawei.oms.email.ap
i.emailserver.EmailServerManager
20   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.event.Ev
entService
21   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.event.Ev
entServiceExt
22   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:23
com.huawei.oms.fm.api.F
aultManager
23   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.api.p
robe.ProbeCenter
24   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.custo
mfault.CustomFaultManager
25   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.probe
dao.HandlerReaderDao
26   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:06
com.huawei.oms.fm.uiapi
.InternalFaultManager
27   12.62.34.228:31902    JSON     2012-02-28 11:08:55
com.huawei.oms.gapi.cor
e.mopkg.ChangeInfoMgr
28   12.62.34.228:31902    JSON     2012-02-28 11:07:38
com.huawei.oms.homepage
.ext.HomepageExtension
29   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:29
com.huawei.oms.license.
as.api.LicenseControl
30   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:29
com.huawei.oms.license.
as.api.LicenseManager
31   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:26
com.huawei.oms.log.mgmt
.LogMgmtService
```


Copyright © Huawei Technologies Co., Ltd.

```
32   12.62.34.228:31902    JSON     2012-02-28 11:07:26
com.huawei.oms.log.mgmt
.LogMgmtService
33   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:02
com.huawei.oms.med.Medi
ation
34   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:00
com.huawei.oms.momgr.ea
m.MOLifeCycleManager
35   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.momgr.ea
m.MOLifeCycleManager
36   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:40
com.huawei.oms.momgr.pm
.PMProbeCenter
37   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:30
com.huawei.oms.nbi.api.
ds.bus.INBIJsonEventService
38   12.62.34.228:31902    JSON     2012-02-28 11:08:30
com.huawei.oms.nbi.api.
ds.bus.INBIJsonEventService
39   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:22
com.huawei.oms.nem.more
.server.MoreService
40   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:14
com.huawei.oms.net.ftp.
server.FtpService
41   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:14
com.huawei.oms.net.ftp.
server.FtpsService
42   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:15
com.huawei.oms.net.ftp.
server.SftpService
43   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:45
com.huawei.oms.pm.DataC
enter
44   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.pm.monit
oring.MonitoringManager
45   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ValidateService
46   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.callback.CallbackService
47   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusHeartbeatService
48   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusInfoService
49   12.62.34.228:31902    JSON     2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusInfoService
50   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.sync.SyncService
51   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:51
com.huawei.oms.sm.as.ap
i.Administration
52   12.62.34.228:31903    HESSIAN  2012-02-28 11:07:26
com.huawei.oms.task.Tas
kManager
53   12.62.34.228:31903    HESSIAN  2012-02-28 11:09:06
com.huawei.oms.topo.map
ping.MappingManager
54   12.62.34.228:31903    HESSIAN  2012-02-28 11:08:56
com.huawei.oms.topo.top
omgr.TopoManager
```


Copyright © Huawei Technologies Co., Ltd.

- After the command is successfully executed, all service information that the current environment releases by using the SBus is displayed:

```
No   Host                  Type     Date                Interface

1    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.OperationDetailManager
2    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.OperationLogManager
3    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.SecurityLogManager
4    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.app.audi
t.api.SystemLogManager
5    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:11
com.huawei.oms.app.dump
.api.DumpConfigManager
6    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:44
com.huawei.oms.app.pm.S
tatusChangedOperation
7    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:42
com.huawei.oms.app.pm.T
emplateManager
8    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:38
com.huawei.oms.app.pm.a
larm.AlarmManager
9    12.66.90.215:31903    HESSIAN  2012-02-28 11:08:40
com.huawei.oms.app.pm.m
omgr.InternalPMProbeCenter
10   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:46
com.huawei.oms.app.pm.m
omgr.PMMoreManager
11   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.app.pm.m
onitoring.InternalMonitoringManager
12   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:51
com.huawei.oms.app.sm.a
pi.as.SecurityManager
13   12.66.90.215:31902    JSON     2012-02-28 11:08:51
com.huawei.oms.app.sm.a
pi.as.SecurityManager
14   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.OperationLogManager
15   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.SecurityLogManager
16   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:04
com.huawei.oms.audit.as
.api.SystemLogManager
17   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:22
com.huawei.oms.eam.am.A
ccessManager
18   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:59
com.huawei.oms.eam.mim.
MITManager
19   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:13
com.huawei.oms.email.ap
i.emailserver.EmailServerManager
20   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.event.Ev
entService
21   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.event.Ev
entServiceExt
22   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:23
com.huawei.oms.fm.api.F
```


Copyright © Huawei Technologies Co., Ltd.

```
aultManager
23   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.api.p
robe.ProbeCenter
24   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.custo
mfault.CustomFaultManager
25   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:20
com.huawei.oms.fm.probe
dao.HandlerReaderDao
26   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:06
com.huawei.oms.fm.uiapi
.InternalFaultManager
27   12.66.90.215:31902    JSON     2012-02-28 11:08:55
com.huawei.oms.gapi.cor
e.mopkg.ChangeInfoMgr
28   12.66.90.215:31902    JSON     2012-02-28 11:07:38
com.huawei.oms.homepage
.ext.HomepageExtension
29   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:29
com.huawei.oms.license.
as.api.LicenseControl
30   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:29
com.huawei.oms.license.
as.api.LicenseManager
31   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:26
com.huawei.oms.log.mgmt
.LogMgmtService
32   12.66.90.215:31902    JSON     2012-02-28 11:07:26
com.huawei.oms.log.mgmt
.LogMgmtService
33   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:02
com.huawei.oms.med.Medi
ation
34   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:00
com.huawei.oms.momgr.ea
m.MOLifeCycleManager
35   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.momgr.ea
m.MOLifeCycleManager
36   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:40
com.huawei.oms.momgr.pm
.PMProbeCenter
37   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:30
com.huawei.oms.nbi.api.
ds.bus.INBIJsonEventService
38   12.66.90.215:31902    JSON     2012-02-28 11:08:30
com.huawei.oms.nbi.api.
ds.bus.INBIJsonEventService
39   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:22
com.huawei.oms.nem.more
.server.MoreService
40   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:14
com.huawei.oms.net.ftp.
server.FtpService
41   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:14
com.huawei.oms.net.ftp.
server.FtpsService
42   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:15
com.huawei.oms.net.ftp.
server.SftpService
43   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:45
com.huawei.oms.pm.DataC
enter
44   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:43
com.huawei.oms.pm.monit
oring.MonitoringManager
45   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
```


Copyright © Huawei Technologies Co., Ltd.

```
.ValidateService
46   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.callback.CallbackService
47   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusHeartbeatService
48   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusInfoService
49   12.66.90.215:31902    JSON     2012-02-28 11:07:25
com.huawei.oms.sbus.api
.ext.SbusInfoService
50   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:25
com.huawei.oms.sbus.api
.sync.SyncService
51   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:51
com.huawei.oms.sm.as.ap
i.Administration
52   12.66.90.215:31903    HESSIAN  2012-02-28 11:07:26
com.huawei.oms.task.Tas
kManager
53   12.66.90.215:31903    HESSIAN  2012-02-28 11:09:06
com.huawei.oms.topo.map
ping.MappingManager
54   12.66.90.215:31903    HESSIAN  2012-02-28 11:08:56
com.huawei.oms.topo.top
omgr.TopoManager
```

Linux

- **Format**: **omscli.sh service** < [*all* | *ip* | *self*] >
- **Input Example**
  1. Log in to the server as the **root** user.
  2. Run the following command to switch the directory:

     cd eSight_ROOT/AppBase/bin/runtime.center/bin
  3. Run the following command to view the SBus information:
     - View all service information that the eSight releases by using the SBus:

       ./omscli.sh service *all*
     - View all service information that a remote environment releases by using the SBus. For example, view all service information of the environment with **12.62.34.228** as its IP address.

       ./omscli.sh service *12.62.34.228*
     - View all service information that the current environment releases by using the SBus:

       ./omscli.sh service *self*
- **Output Example**
  - After the command is successfully executed, all service information that the eSight releases by using the SBus is displayed:

```
o   Host                 Type     Date
Interface

1    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationDetailManager
2    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationLogManager

3    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
```


Copyright © Huawei Technologies Co., Ltd.

```
com.huawei.oms.app.audit.api.SecurityLogManager
4    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SystemLogManager
5    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:02
com.huawei.oms.app.dump.api.DumpConfigManager
6    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.StatusChangedOperation
7    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:15
com.huawei.oms.app.pm.TemplateManager
8    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:13
com.huawei.oms.app.pm.alarm.AlarmManager
9    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:14
com.huawei.oms.app.pm.momgr.InternalPMProbeCenter
10   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.app.pm.momgr.PMMoreManager
11   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.monitoring.InternalMonitoringManager
12   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
13   12.67.176.108:31902   JSON     2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
14   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.OperationLogManager
15   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SecurityLogManager
16   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SystemLogManager
17   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.eam.am.AccessManager
18   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:06
com.huawei.oms.eam.mim.MITManager
19   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:10
com.huawei.oms.email.api.emailserver.EmailServerManager
20   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventService
21   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventServiceExt
22   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:18
com.huawei.oms.fm.api.FaultManager
23   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.api.probe.ProbeCenter
24   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.customfault.CustomFaultManager
25   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.probedao.HandlerReaderDao
26   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:10
com.huawei.oms.fm.uiapi.InternalFaultManager
27   12.67.176.108:31902   JSON     2012-02-28 11:07:05
com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28   12.67.176.108:31902   JSON     2012-02-28 11:06:39
com.huawei.oms.homepage.ext.HomepageExtension
29   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseControl
30   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseManager
31   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
32   12.67.176.108:31902   JSON     2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
33   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.med.Mediation
34   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:04
com.huawei.oms.momgr.eam.MOLifeCycleManager
35   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.momgr.eam.MOLifeCycleManager
36   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:14
com.huawei.oms.momgr.pm.PMProbeCenter
37   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
```


Copyright © Huawei Technologies Co., Ltd.

```
38   12.67.176.108:31902   JSON     2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.nem.more.server.MoreService
40   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpService
41   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpsService
42   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.SftpService
43   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.pm.DataCenter
44   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.pm.monitoring.MonitoringManager
45   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ValidateService
46   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.callback.CallbackService
47   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
49   12.67.176.108:31902   JSON     2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
50   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.sync.SyncService
51   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:58
com.huawei.oms.sm.as.api.Administration
52   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.task.TaskManager
53   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:11
com.huawei.oms.topo.mapping.MappingManager
54   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:11
com.huawei.oms.topo.topomgr.TopoManager
```

- After the command is successfully executed, all service information of the environment with **12.62.34.228** as its IP address is displayed:

```
No   Host                  Type     Date
Interface
1    12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationDetailManager
2    12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationLogManager
3    12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SecurityLogManager
4    12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SystemLogManager
5    12.62.34.228:31903   HESSIAN  2012-02-28 11:07:02
com.huawei.oms.app.dump.api.DumpConfigManager
6    12.62.34.228:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.StatusChangedOperation
7    12.62.34.228:31903   HESSIAN  2012-02-28 11:07:15
com.huawei.oms.app.pm.TemplateManager
8    12.62.34.228:31903   HESSIAN  2012-02-28 11:07:13
com.huawei.oms.app.pm.alarm.AlarmManager
9    12.62.34.228:31903   HESSIAN  2012-02-28 11:07:14
com.huawei.oms.app.pm.momgr.InternalPMProbeCenter
10   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.app.pm.momgr.PMMoreManager
11   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.monitoring.InternalMonitoringManager
12   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
13   12.62.34.228:31902   JSON     2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
14   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.OperationLogManager
15   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SecurityLogManager
16   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:56
```


Copyright © Huawei Technologies Co., Ltd.

```
com.huawei.oms.audit.as.api.SystemLogManager
17   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.eam.am.AccessManager
18   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:06
com.huawei.oms.eam.mim.MITManager
19   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:10
com.huawei.oms.email.api.emailserver.EmailServerManager
20   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventService
21   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventServiceExt
22   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:18
com.huawei.oms.fm.api.FaultManager
23   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.api.probe.ProbeCenter
24   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.customfault.CustomFaultManager
25   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.probedao.HandlerReaderDao
26   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:10
com.huawei.oms.fm.uiapi.InternalFaultManager
27   12.62.34.228:31902   JSON     2012-02-28 11:07:05
com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28   12.62.34.228:31902   JSON     2012-02-28 11:06:39
com.huawei.oms.homepage.ext.HomepageExtension
29   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseControl
30   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseManager
31   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
32   12.62.34.228:31902   JSON     2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
33   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.med.Mediation
34   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:04
com.huawei.oms.momgr.eam.MOLifeCycleManager
35   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.momgr.eam.MOLifeCycleManager
36   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:14
com.huawei.oms.momgr.pm.PMProbeCenter
37   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
38   12.62.34.228:31902   JSON     2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.nem.more.server.MoreService
40   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpService
41   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpsService
42   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.SftpService
43   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.pm.DataCenter
44   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.pm.monitoring.MonitoringManager
45   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ValidateService
46   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.callback.CallbackService
47   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
49   12.62.34.228:31902   JSON     2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
50   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.sync.SyncService
```


Copyright © Huawei Technologies Co., Ltd.

```
51   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:58
com.huawei.oms.sm.as.api.Administration
52   12.62.34.228:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.task.TaskManager
53   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:11
com.huawei.oms.topo.mapping.MappingManager
54   12.62.34.228:31903   HESSIAN  2012-02-28 11:07:11
com.huawei.oms.topo.topomgr.TopoManager
```

- After the command is successfully executed, all service information that the current environment releases by using the SBus is displayed:

```
No   Host                  Type     Date
Interface
1    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationDetailManager
2    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationLogManager

3    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SecurityLogManager
4    12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SystemLogManager
5    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:02
com.huawei.oms.app.dump.api.DumpConfigManager
6    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.StatusChangedOperation
7    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:15
com.huawei.oms.app.pm.TemplateManager
8    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:13
com.huawei.oms.app.pm.alarm.AlarmManager
9    12.67.176.108:31903   HESSIAN  2012-02-28 11:07:14
com.huawei.oms.app.pm.momgr.InternalPMProbeCenter
10   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.app.pm.momgr.PMMoreManager
11   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.monitoring.InternalMonitoringManager
12   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
13   12.67.176.108:31902   JSON     2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
14   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.OperationLogManager
15   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SecurityLogManager
16   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SystemLogManager
17   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.eam.am.AccessManager
18   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:06
com.huawei.oms.eam.mim.MITManager
19   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:10
com.huawei.oms.email.api.emailserver.EmailServerManager
20   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventService
21   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventServiceExt
22   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:18
com.huawei.oms.fm.api.FaultManager
23   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.api.probe.ProbeCenter
24   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.customfault.CustomFaultManager
25   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.probedao.HandlerReaderDao
26   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:10
com.huawei.oms.fm.uiapi.InternalFaultManager
27   12.67.176.108:31902   JSON     2012-02-28 11:07:05
com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28   12.67.176.108:31902   JSON     2012-02-28 11:06:39
com.huawei.oms.homepage.ext.HomepageExtension
```


Copyright © Huawei Technologies Co., Ltd.

```
29   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseControl
30   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseManager
31   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
32   12.67.176.108:31902   JSON     2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
33   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.med.Mediation
34   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:04
com.huawei.oms.momgr.eam.MOLifeCycleManager
35   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.momgr.eam.MOLifeCycleManager
36   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:14
com.huawei.oms.momgr.pm.PMProbeCenter
37   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
38   12.67.176.108:31902   JSON     2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.nem.more.server.MoreService
40   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpService
41   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpsService
42   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.SftpService
43   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:17
com.huawei.oms.pm.DataCenter
44   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:16
com.huawei.oms.pm.monitoring.MonitoringManager
45   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ValidateService
46   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.callback.CallbackService
47   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
49   12.67.176.108:31902   JSON     2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
50   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.sbus.api.sync.SyncService
51   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:58
com.huawei.oms.sm.as.api.Administration
52   12.67.176.108:31903   HESSIAN  2012-02-28 11:06:32
com.huawei.oms.task.TaskManager
53   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:11
com.huawei.oms.topo.mapping.MappingManager
54   12.67.176.108:31903   HESSIAN  2012-02-28 11:07:11
com.huawei.oms.topo.topomgr.TopoManager
```

15.2 Oracle Database Command Reference

This topic describes common Oracle database commands and their functions and application cases.

For details about more command references, see the Oracle command reference manual.

15.2.1 sqlplus Command

This topic describes the **sqlplus** command for accessing the Oracle database.

Copyright © Huawei Technologies Co., Ltd.

Function

The **sqlplus** command is used to connect to the Oracle database. You can run SQL statements in the SQL command line window or configure the Oracle database.

Format

sqlplus *Parameter*

Parameters

Table 15-1 describes the parameters of the **sqlplus** command.

Table 15-1 Parameters

Parameter	Description
/ as sysdba	**/ as sysdba** indicates that the user connects the Oracle database as **sysdba**. The **sysdba** user has permission to start and stop the Oracle database. This connection mode is applicable only to the Oracle user.
dbuser/ password	**dbuser/password** indicates that the database user connects the Oracle database as **dbuser**. **password** is the password of the **dbuser** user. In this mode, the **dbuser** user performs operations according to the permission assigned.

NOTE

Only parameters that are used to access the Oracle database are described here. They are classified into two types: **/ as sysdba** and **dbuser/password**. For more parameter setting methods, see the related documents provided by the Oracle company.

Example

Assume that the **root** user already logs in to the SuSE Linux. The OS user name of the Oracle database is **oracle**.

On the CLI, run the following command to connect to the Oracle database:

- Method 1: Run the following commands to switch to the **oracle** user.

  su - *oracle*

  Run the following commands to connect the Oracle database as user **sysdba**.

  sqlplus / **as** *sysdba*

  NOTE

  The user name and password are required in remote login mode. The following describes how to use the command to connect the system user to the Oracle database with password testpwd.

  sqlplus system/testpwd as *sysdba*

  If the following information is displayed, the Oracle database is connected successfully. In the case of a failure, find out the cause as prompted.

  ```
  SQL>
  ```

- Method 2: Log in to the SuSE Linux as the **root** user and then connect the Oracle database as the **system** user. Assume that the password of the **system** user is **testpwd**.

Copyright © Huawei Technologies Co., Ltd.

system/testpwd

If the following information is displayed, the Oracle database is connected successfully. In the case of a failure, find out the cause as prompted.

```
SQL>
```

15.2.2 startup Command

This topic describes the **startup** command for starting the Oracle database.

Function

In the SQL command line window, the **startup** command is used to start the Oracle database.

Format

startup Parameter

Parameters

Table 15-2 describes the parameters of the **startup** command.

Table 15-2 Parameters

Parameter	Description
Null	The database is started properly. After the **startup** command is executed, the instances are started, then the database is installed, and finally the database is started.
force	The database is restarted forcibly. When the database cannot be closed properly, the **startup force** command is used to close and then start the database.
nomount	Only the instances are started.
mount	The database is installed after the instances are started.

Example

Assume that the user who logs in to the SUSE Linux is the user who manages the Oracle database, namely, **oracle**.

On the CLI, run the following command to connect to the Oracle database.

sqlplus / **as** *sysdba*

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The user name and password are required in remote login mode. The following describes how to use the command to connect the system user to the Oracle database with password testpwd.

  $ **sqlplus system/testpwd as** *sysdba*

- For information on how to use the **sqlplus** command, see **15.2.1 sqlplus Command**.

Run the **startup** command to start the Oracle database.

startup

The following information is displayed:

```
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size 2046264 bytes
Variable Size 385877704 bytes
Database Buffers 1207959552 bytes
Redo Buffers 14729216 bytes
Database mounted.
Database opened.
```

ORACLE instance started, **Database mounted**, and **Database opened** indicate that the Oracle database is started properly.

15.2.3 shutdown Command

This topic describes the **shutdown** command for shutting down the Oracle database.

Function

In the SQL command line window, the **shutdown** command is used to shut down the Oracle database.

Format

shutdown *Parameter*

Parameters

Table 15-3 describes the parameters of the **shutdown** command.

Table 15-3 Parameters

Parameter	Description
normal	Closes the database, uninstalls the database, and closes the instances after all users are disconnected.
immediate (recommended)	Rolls back all user transactions, and then closes the database, uninstalls the database, and closes the instances.
transactional	Closes the database, uninstalls the database, and closes the instances when all user transactions end.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
abort	Terminates the instances immediately. Ongoing user transactions are restored at next start. **NOTE** The **abort** parameter is used when the database cannot be closed properly. The use of this parameter may lead to data loss.

Example

Assume that the user who logs in to the SUSE Linux is the user who manages the Oracle database, namely, **oracle**.

On the CLI, run the following command to connect to the Oracle database.

sqlplus / **as** *sysdba*

NOTE

- The user name and password are required in remote login mode. The following describes how to use the command to connect the system user to the Oracle database with password testpwd.

  $ **sqlplus system/testpwd as** *sysdba*

- For information on how to use the **sqlplus** command, see **15.2.1 sqlplus Command**.

Run the **shutdown** command to close the Oracle database.

shutdown immediate

The following information is displayed.

```
Database closed.
Database dismounted.
ORACLE instance shut down.
```

Database closed indicates that the Oracle database is closed successfully. **Database dismounted** indicates that the database is uninstalled successfully. **ORACLE instance shut down** indicates that the database instances are closed successfully.

15.2.4 show Command

This topic describes the **show** command for viewing the operating parameters of the Oracle database.

Function

In the SQL command line window, the **show** command is used to view operating parameters of the Oracle database.

Format

show parameter *parameter*

Parameters

Table 15-4 describes the parameters of the **show** command.

Copyright © Huawei Technologies Co., Ltd.

Table 15-4 Parameters

Parameter	Description
Null	Lists all operating parameters of the Oracle database, such as **NAME** (parameter name), **TYPE** (parameter type), and **VALUE** (parameter value).
Parameter	Shows the value of the specified **parameter**.

Example 1

Assume that the user who logs in to the SUSE Linux is the user who manages the Oracle database, namely, **oracle**.

This example describes how to view all operating parameters of the Oracle database.

On the command line interface (CLI), run the following command to connect to the Oracle database.

sqlplus / **as** *sysdba*

NOTE

- The user name and password are required in remote login mode. The following describes how to use the command to connect the system user to the Oracle database with password testpwd.

  $ **sqlplus system/testpwd as** *sysdba*

- For information on how to use the **sqlplus** command, see **15.2.1 sqlplus Command**.

Run the **show** command to view all operating parameters of the Oracle database.

show parameter

The following is part of the output information.

```
NAME TYPE VALUE
---------------------------------- ----------- ------------------------------
undo_management string AUTO
undo_retention integer 900
undo_tablespace string UNDOTBS1
use_indirect_data_buffers boolean FALSE
user_dump_dest string /opt/oracle/oradb/home/admin/i
mapdb/udump
utl_file_dir string
workarea_size_policy string AUTO
```

Example 2

Assume that the user who logs in to the SUSE Linux is the user who manages the Oracle database, namely, **oracle**.

This example describes how to view the value of the **processes** parameter.

On the CLI, run the following command to connect to the Oracle database.

sqlplus / **as** *sysdba*

Run the **show** command to view the operating parameters of the Oracle database.

show parameter *process*

Copyright © Huawei Technologies Co., Ltd.

The information about the parameters containing **processes** is displayed.

```
NAME TYPE VALUE
---------------------------------- ----------- ------------------------------
aq_tm_processes integer 0
db_writer_processes integer 1
gcs_server_processes integer 0
job_queue_processes integer 10
log_archive_max_processes integer 2
processes integer 150
```

15.2.5 alter Command

This topic describes the **alter** command for modifying the operating parameters of the Oracle database.

Function

The **alter** command for modifying the operating parameters of the Oracle database in the SQL command line window.

Format

alter Option 1 *Parameter 1* **Option 2** *Parameter 2……*

Parameters

Table 15-5 describes the parameters of the **alter** command.

Table 15-5 Parameters

Parameter	Description
user	Sets the password of an Oracle database user. **NOTE** The example in this topic only describes how to change the password of an Oracle user. For details about parameter settings, see related documents provided by the Oracle company.
system set	Sets the system parameters of the Oracle database. **NOTE** The example in this topic only describes how to modify the system parameters of the Oracle database. Parameter values are selected based on actual applications. This example is only for reference. For details about parameter settings, see the related documents provided by the Oracle company.

Example 1

Assume that the user who logs in to the SUSE Linux is the user who manages the Oracle database, namely, **oracle**.

On the command line interface (CLI), run the following command to connect to the Oracle database:

sqlplus / **as** *sysdba*

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The user name and password are required in remote login mode. The following describes how to use the command to connect the system user to the Oracle database with password testpwd.

  $ **sqlplus system/testpwd as** *sysdba*

- For information on how to use the **sqlplus** command, see **15.2.1 sqlplus Command**.

Run the following command to change the password of the database user **system**:

alter user system identified by *"testpwd"*

To be specific, **system** is the database user name to be changed, and **testpwd** is the password of the user-defined **system** user.

If the return value is **User altered**, the password is successfully changed. Otherwise, locate the cause as prompted.

Example 2

Assume that the user who logs in to the SUSE Linux is the user who manages the Oracle database, namely, **oracle**.

Initialization operating parameter **processes**: set the number of processes for connecting to the Oracle database instance is **1024**.

On the CLI, run the following command to connect to the Oracle database:

sqlplus / **as** *sysdba*

Run the following command to modify the operating parameters of the Oracle database:

alter system set processes=1024 scope=spfile

To be specific, **processes** is the name of the operating parameter to be modified, and **scope=spfile** indicates that **processes** is the initialization parameter of the Oracle database. See **15.2.4 show Command** to view the current value of **processes**.

If the return value is **System altered**, the password is successfully changed. Otherwise, locate the cause as prompted.

Copyright © Huawei Technologies Co., Ltd.

16 FAQs

About This Chapter

This topic describes the solutions to the frequently asked questions (FAQs) about the eSight.

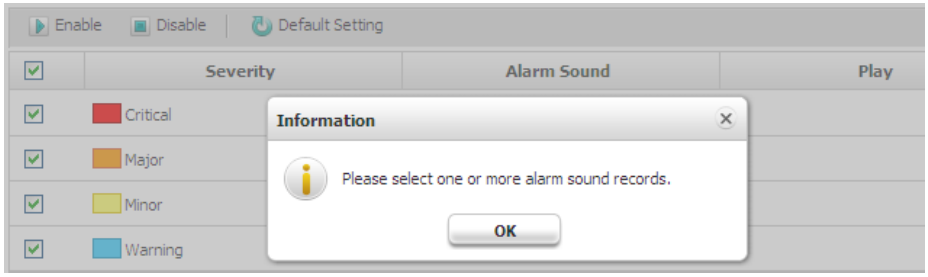
Copyright © Huawei Technologies Co., Ltd.

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.

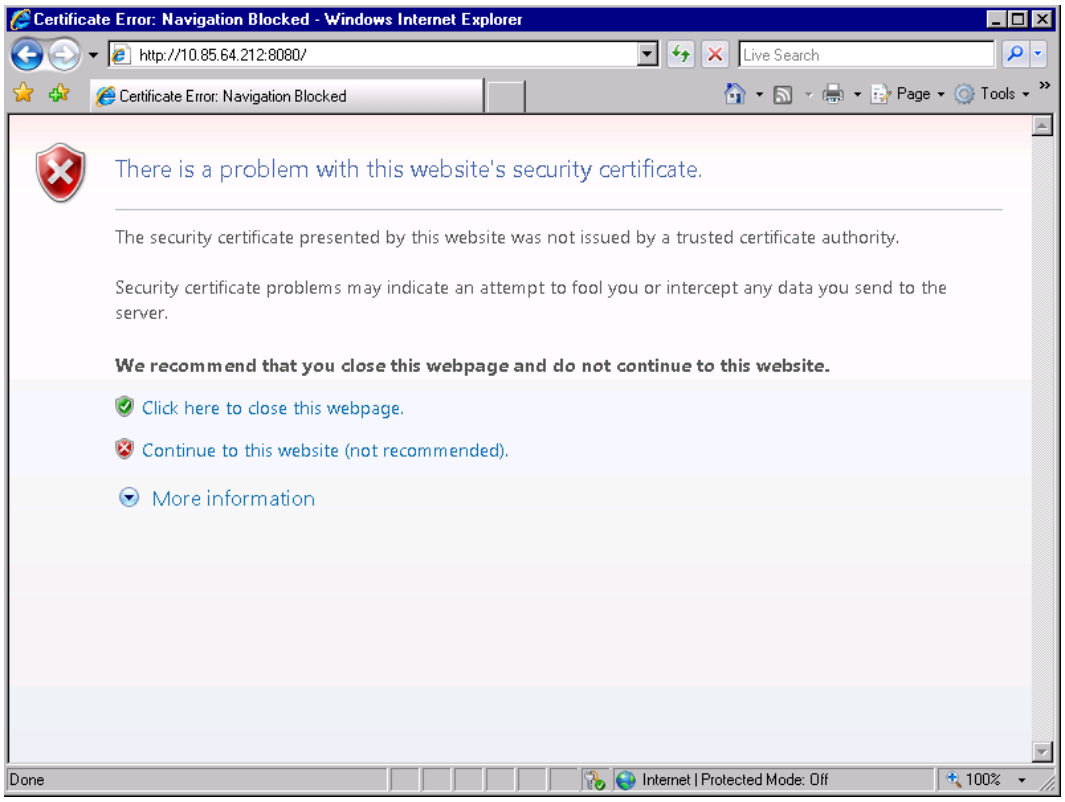
Symptom

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.

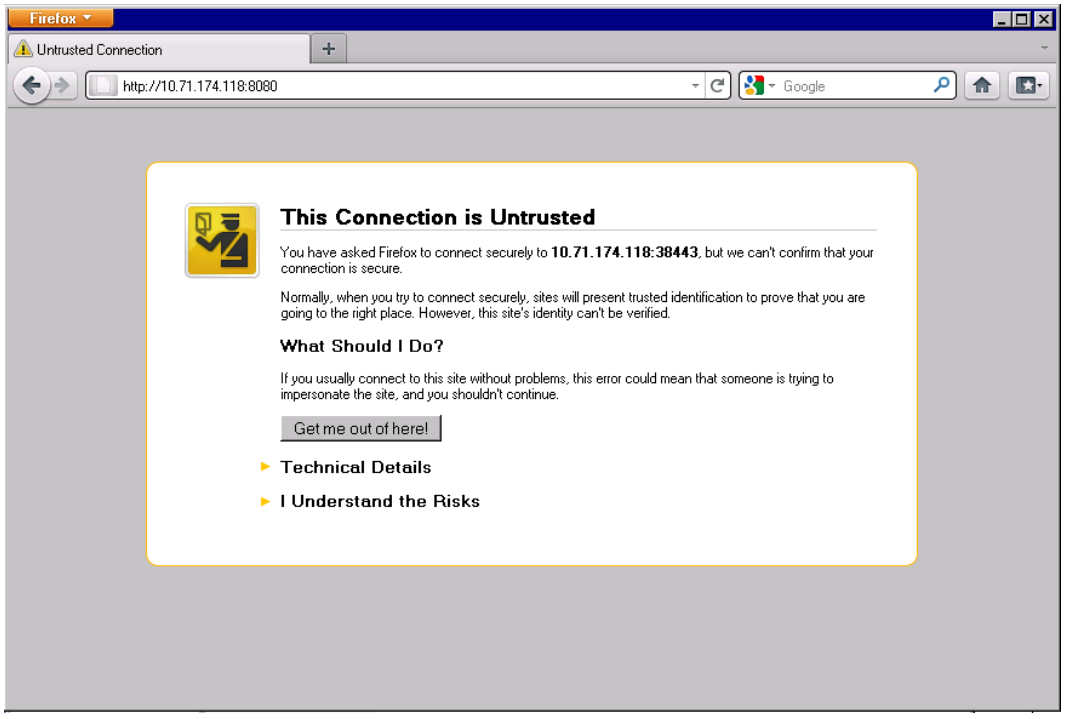
Copyright © Huawei Technologies Co., Ltd.

Figure 16-2 Error message (IE)



- The following figure shows the security certificate error prompted by Firefox.

Figure 16-3 Error message (Firefox)



Copyright © Huawei Technologies Co., Ltd.

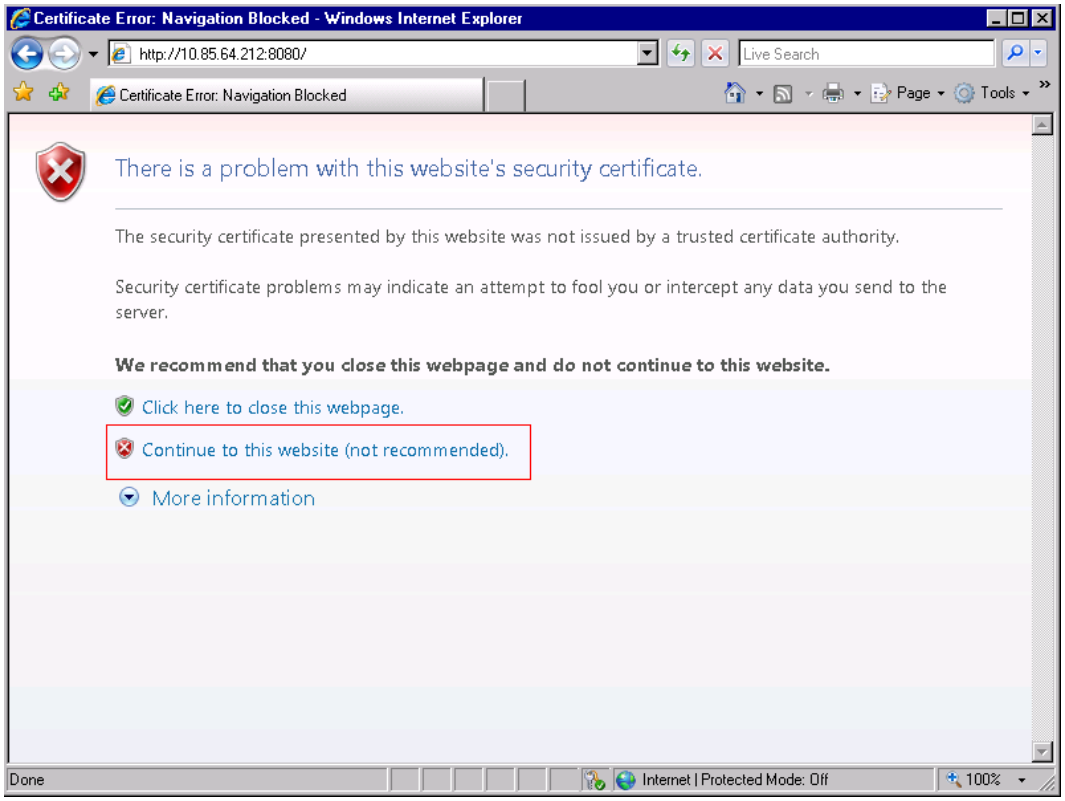
Possible Causes

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)**.

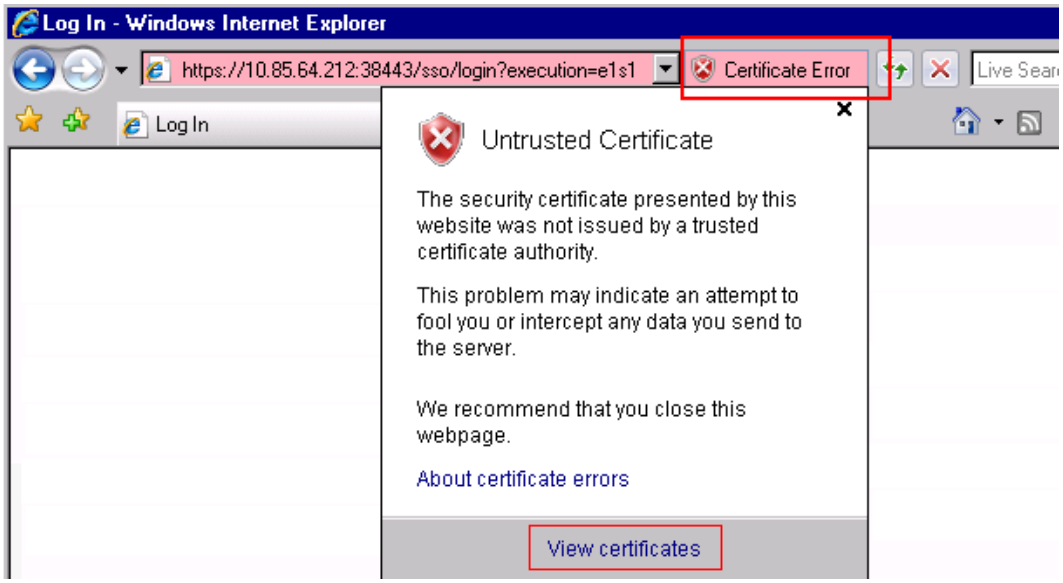
Figure 16-4 Error message (IE)



  2. Click **Certificate Error**. In the **Untrusted Certificate** dialog box, click **View certificates**.

Copyright © Huawei Technologies Co., Ltd.

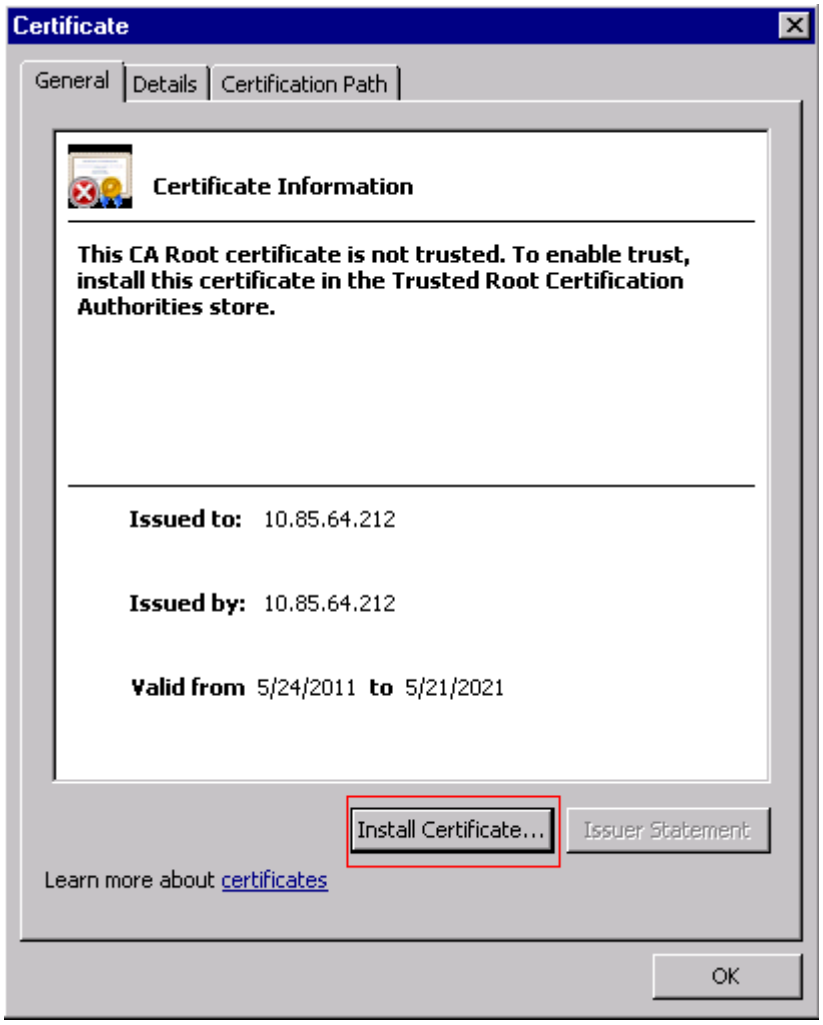
Figure 16-5 Untrusted Certificate



3. On the **General** tab page, click **Install Certificate**.

Copyright © Huawei Technologies Co., Ltd.

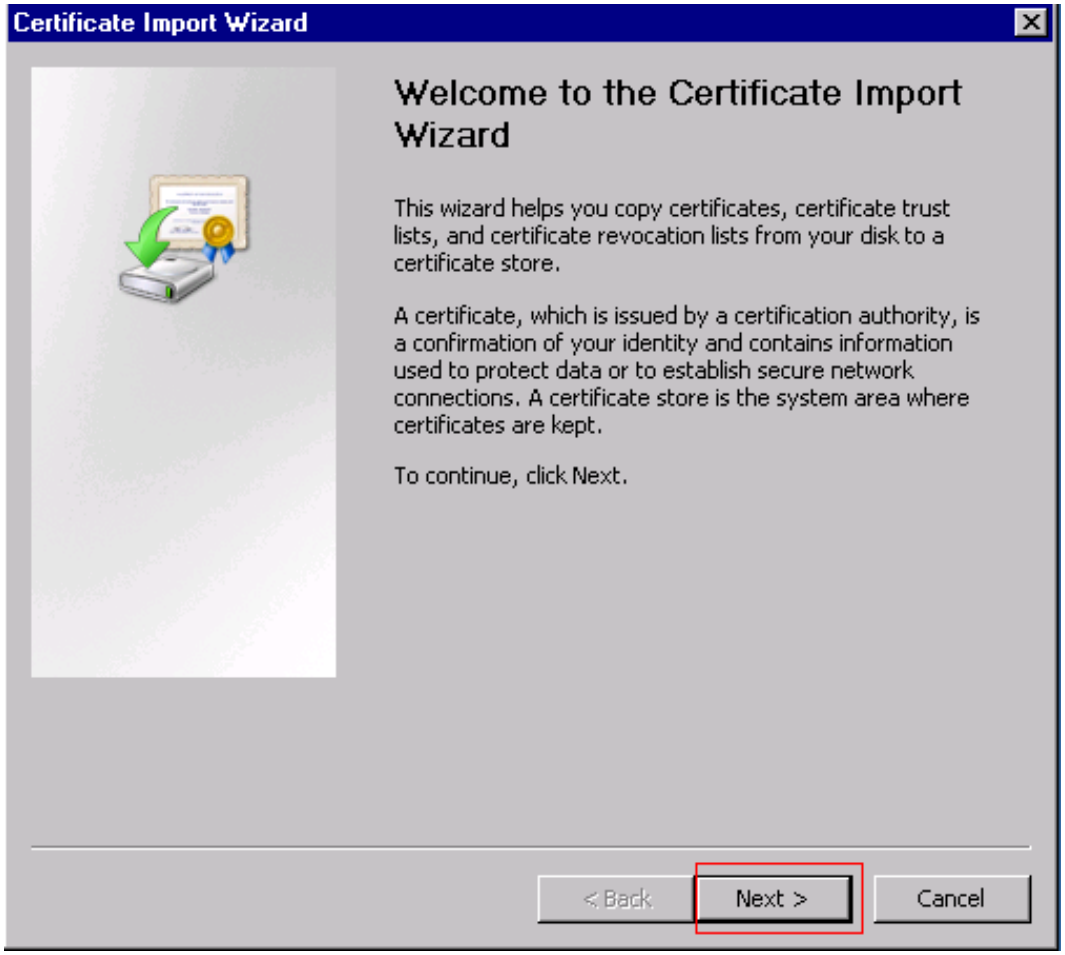
Figure 16-6 Certificate Information



4. In the **Certificate Import Wizard** dialog box, click **Next**.

Copyright © Huawei Technologies Co., Ltd.

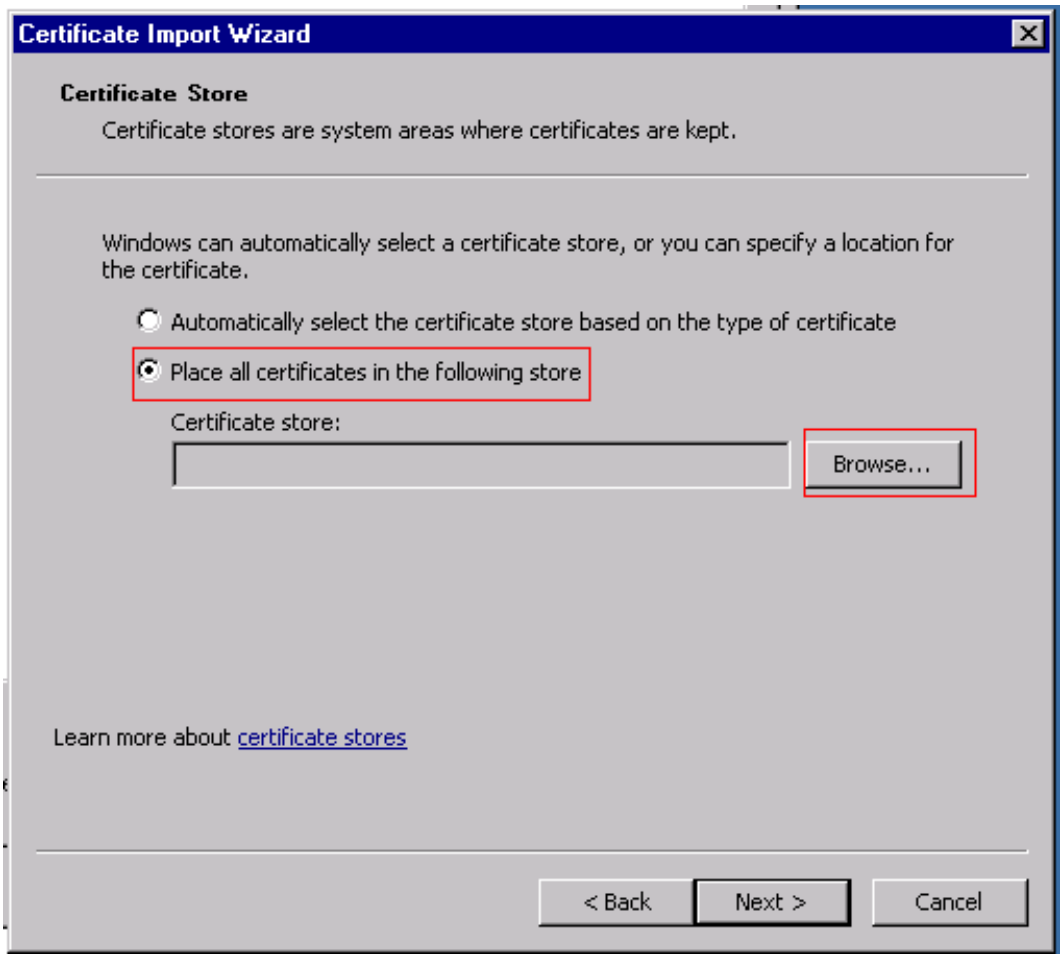
Figure 16-7 Certificate Import Wizard



5. Select **Please all certificates in the following store** and click **Browse**.

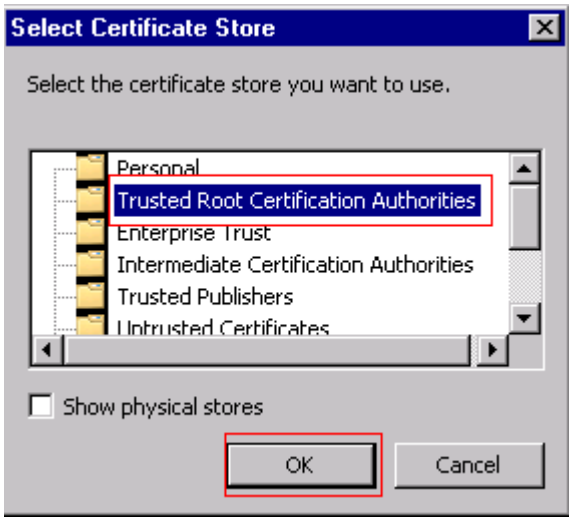
Copyright © Huawei Technologies Co., Ltd.

Figure 16-8 Import Certificate



6. In the **Select Certificate Store** dialog box, select **Trusted Root Certification Authorities** and click **OK**.

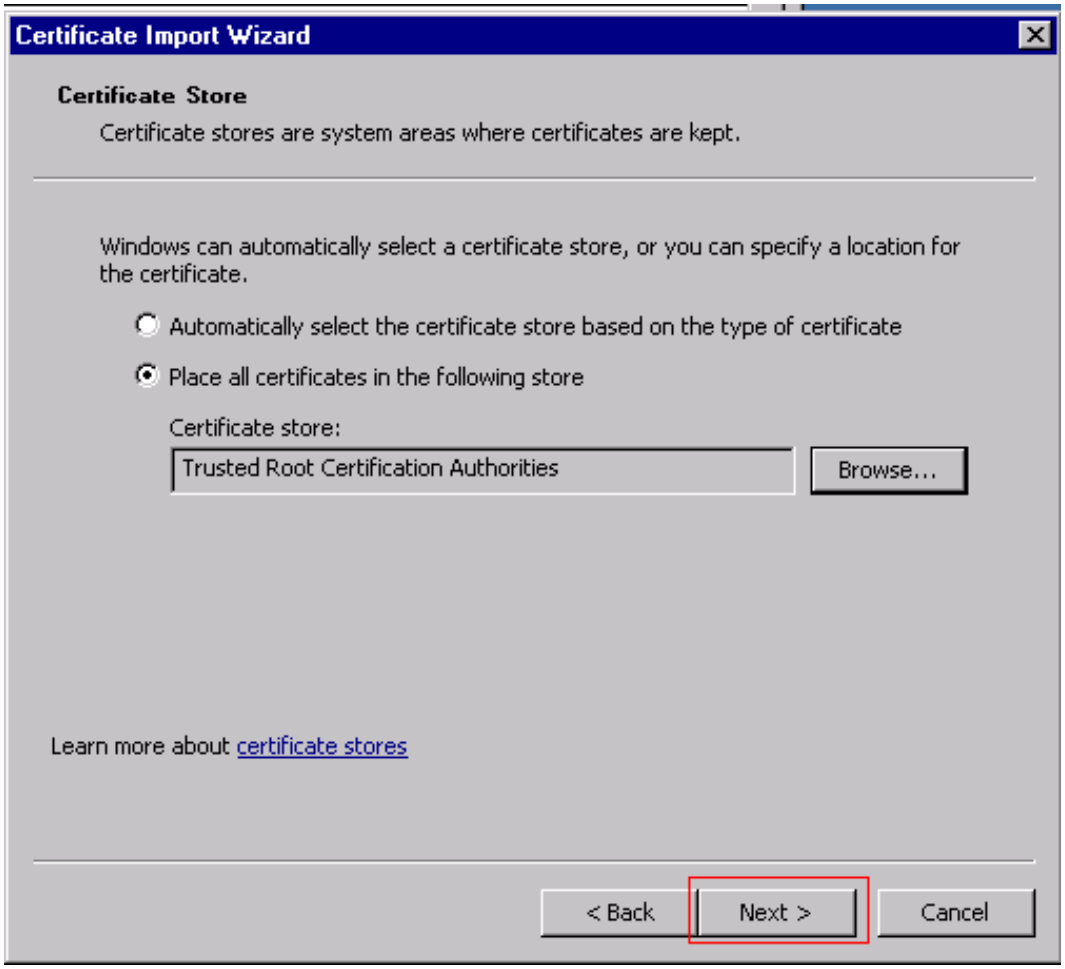
Figure 16-9 Select Certificate Store



Copyright © Huawei Technologies Co., Ltd.

7. Click **Next**.

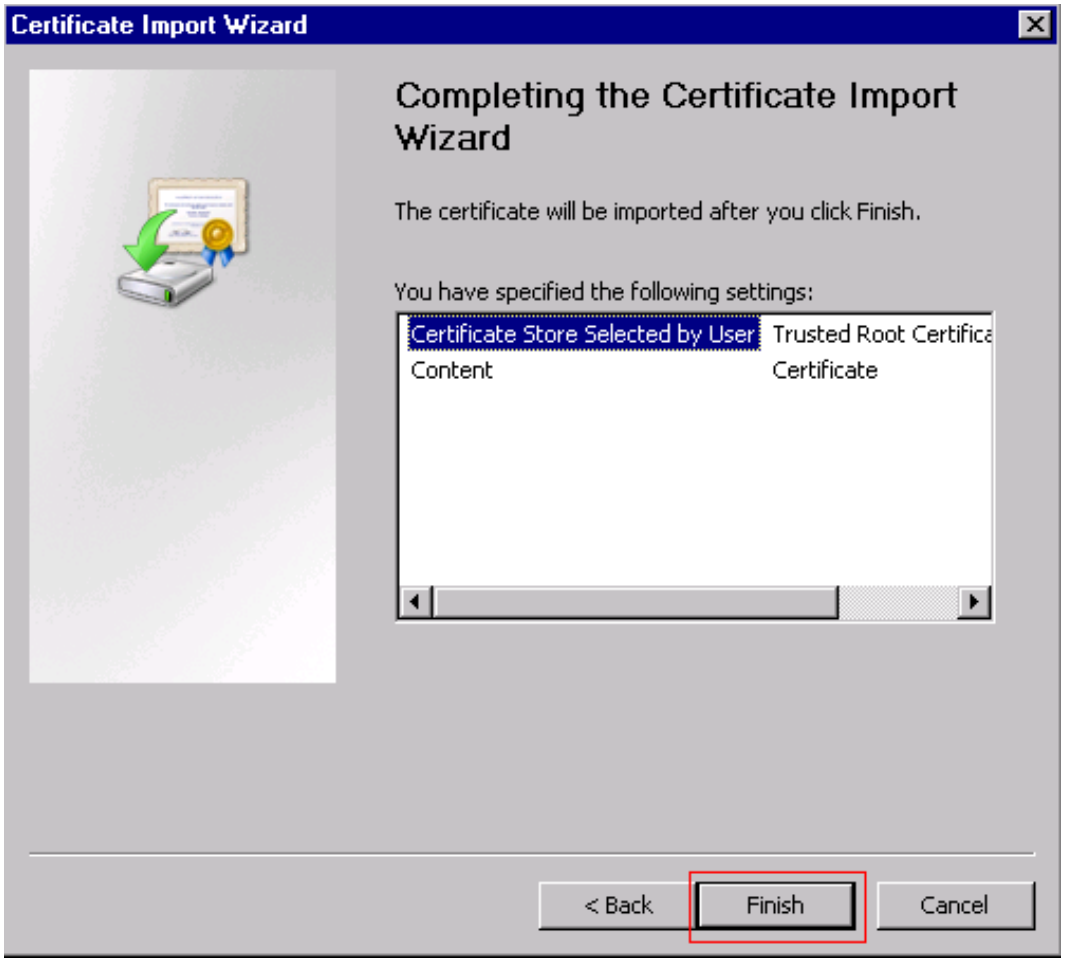
Figure 16-10 Certificate Store



8. In the **Certificate Import Wizard** dialog box, click **Finish**.

Copyright © Huawei Technologies Co., Ltd.

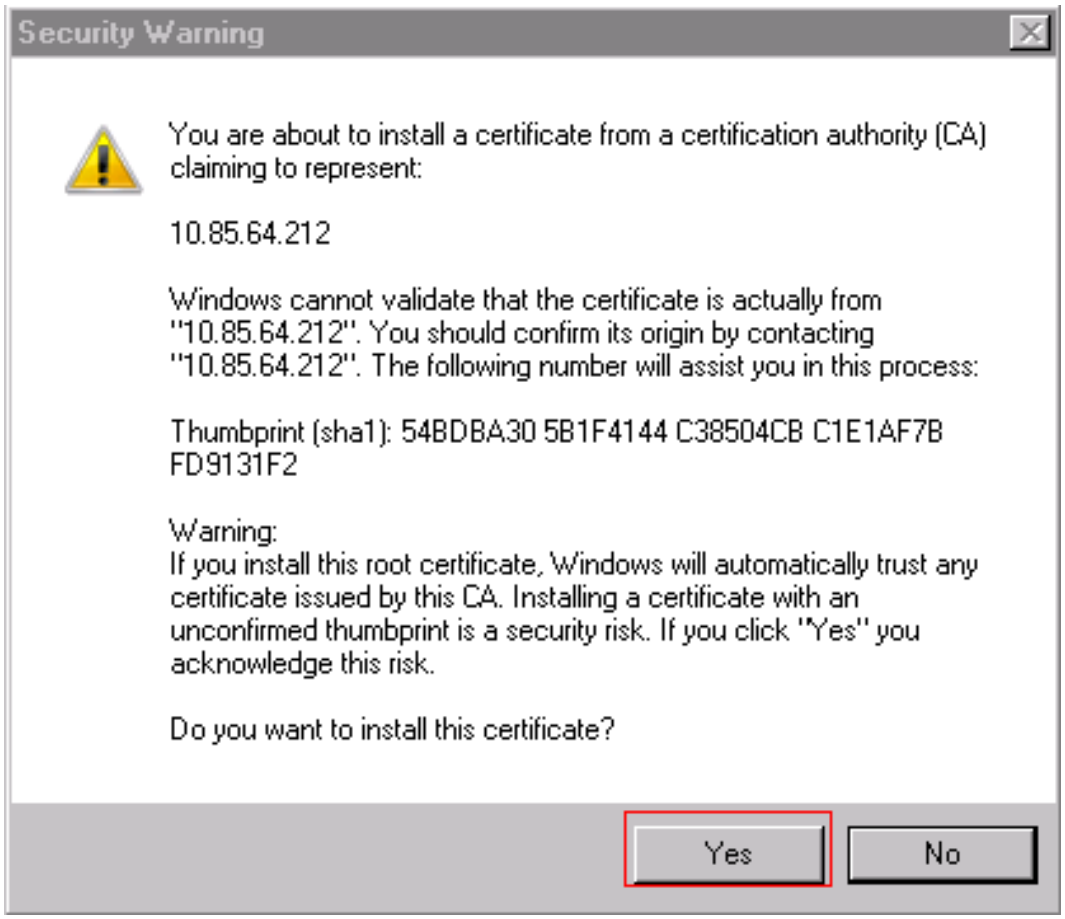
Figure 16-11 Complete the Certificate Import Wizard



9. In the **Security Warning** dialog box, click **Yes**.

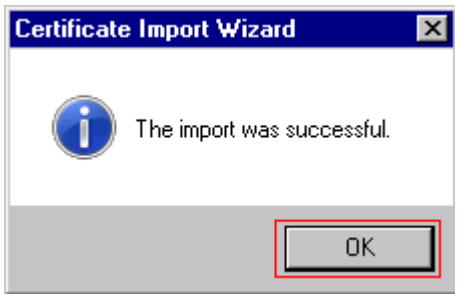
Copyright © Huawei Technologies Co., Ltd.

Figure 16-12 Install Certificate



10. In the **Certificate Import Wizard** dialog box, click **OK**.

Figure 16-13 Certificate importing succeeded

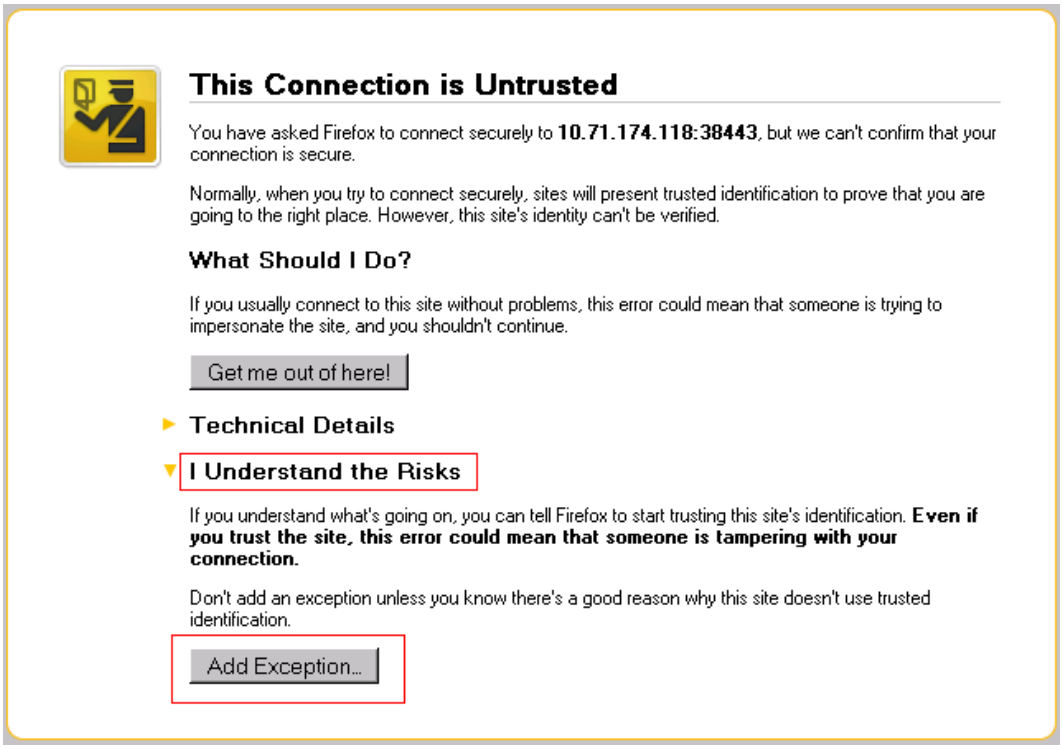


11. Close Internet Explorer and open it again to log in to the eSight.

- Install the security certificate in Mozilla Firefox.
  1. On the error message page, expand **I Understand the Risks** and click **Add Exception**.

Copyright © Huawei Technologies Co., Ltd.

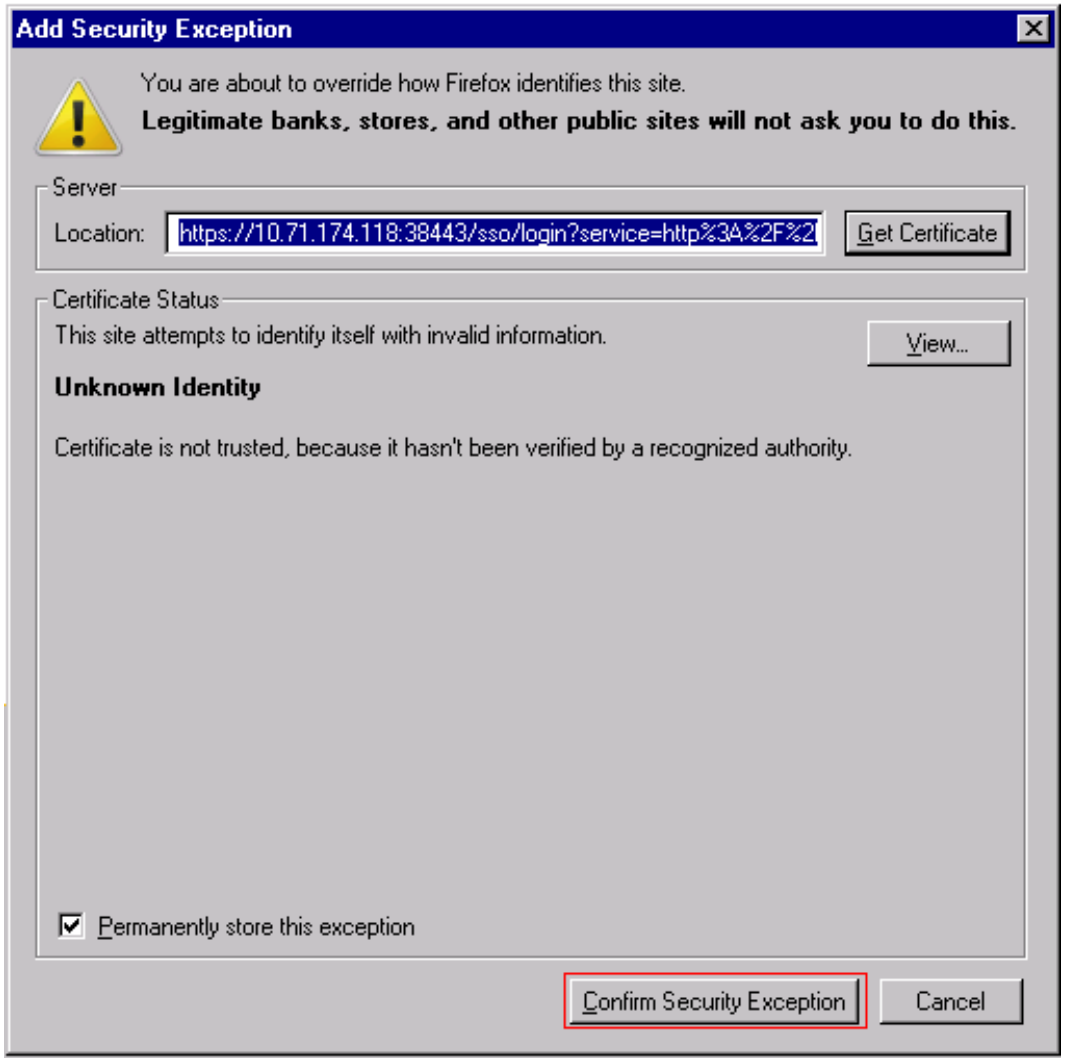
Figure 16-14 Add Exception



2. In the **Add Security Exception** dialog box, click **Confirm Security Exception**.

Copyright © Huawei Technologies Co., Ltd.

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.

Symptom

The Web browser displays a security alarm when you log in to the eSight

Copyright © Huawei Technologies Co., Ltd.

Figure 16-16 Internet Explorer

Possible Causes

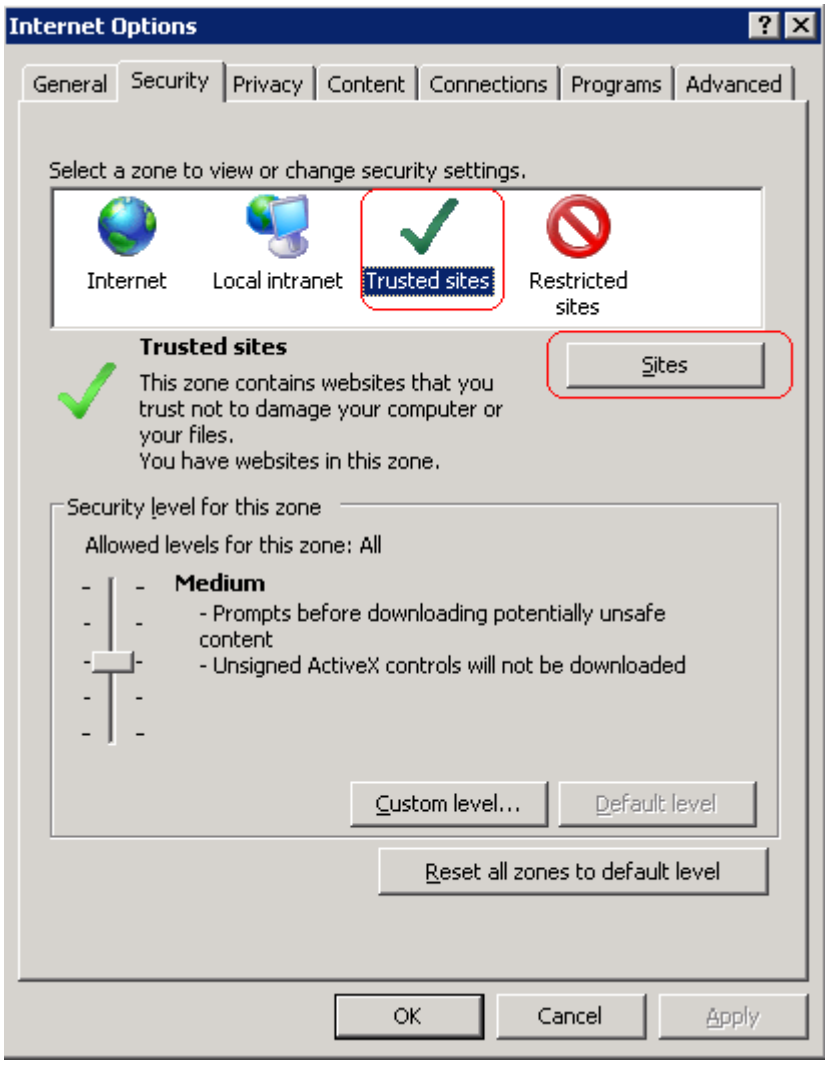
The security level of the browser is too high. To solve this problem, you can add the website of the I2000 as a trusted website or set the security level of the browser to a low level.

Procedure

- Solution 1: Add Trusted Websites
  1. In the dialog box shown in **Figure 16-16**, click **Add**.
  2. On the **Security** tab page, select **Trusted sites** and then click **Sites**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-17 Internet Options



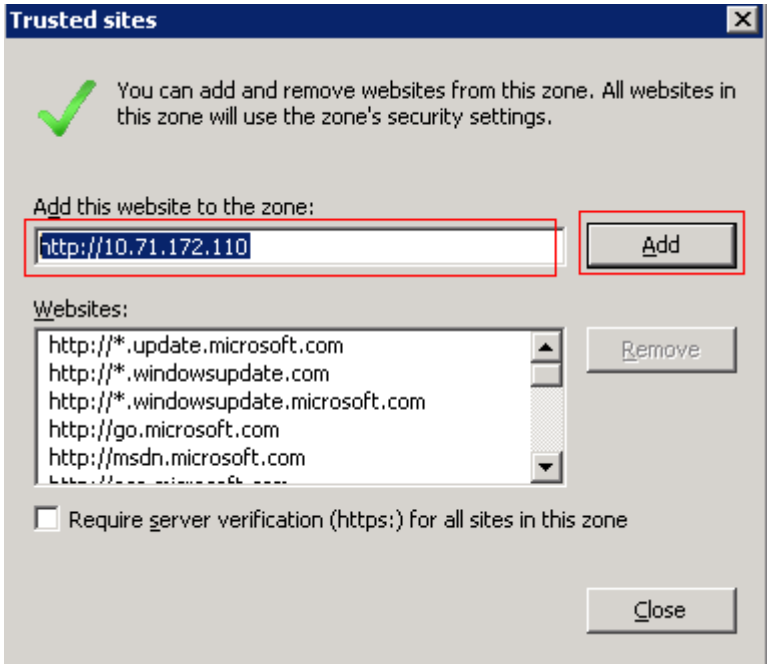
3. In the **Add this website to the zone** text box, enter the website for accessing the eSight, and click **Add** to add the website to the list of trusted websites.

   NOTE

   The websites for accessing theeSight over HTTP or HTTPS must be added to the list of trusted websites.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-18 Trusted sites

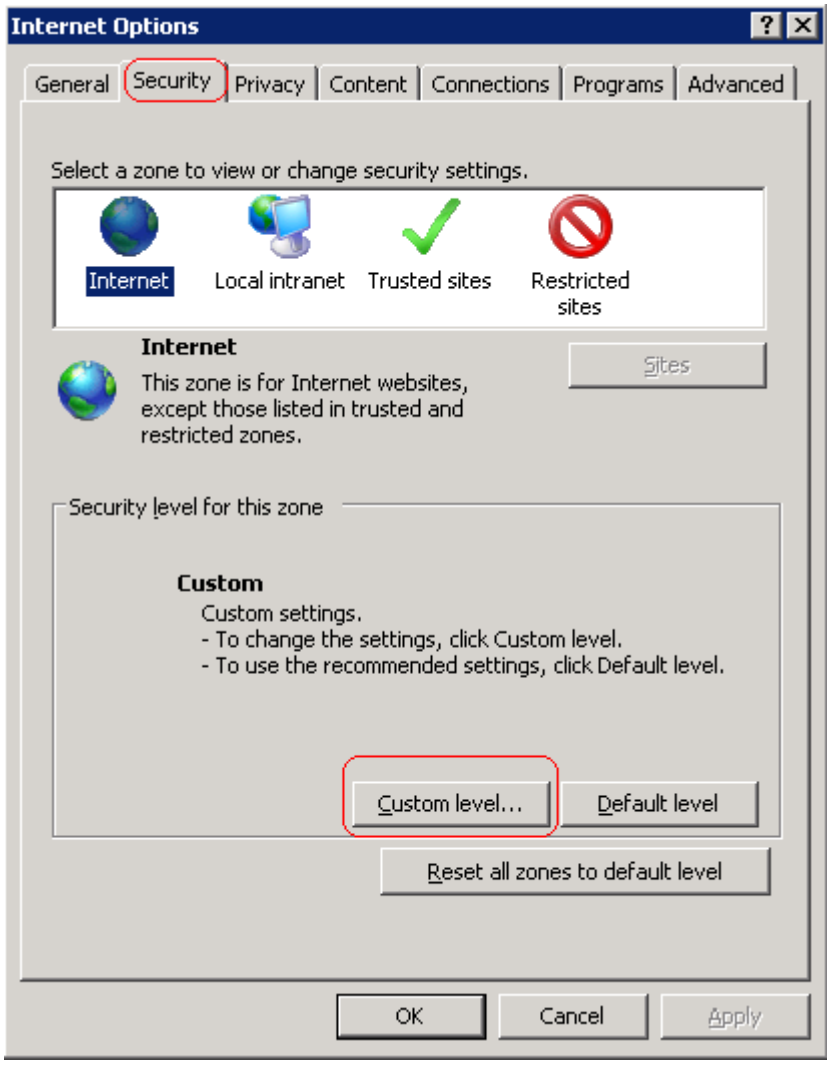


4. Click **Close**.

- Solution 2: Set the Security Level of the Browser
  1. Open Microsoft Internet Explorer, and choose **Tools** > **Internet Options**.
  2. In the **Internet Options** window, click the **Security** tab, and click **Custom level**.

Copyright © Huawei Technologies Co., Ltd.

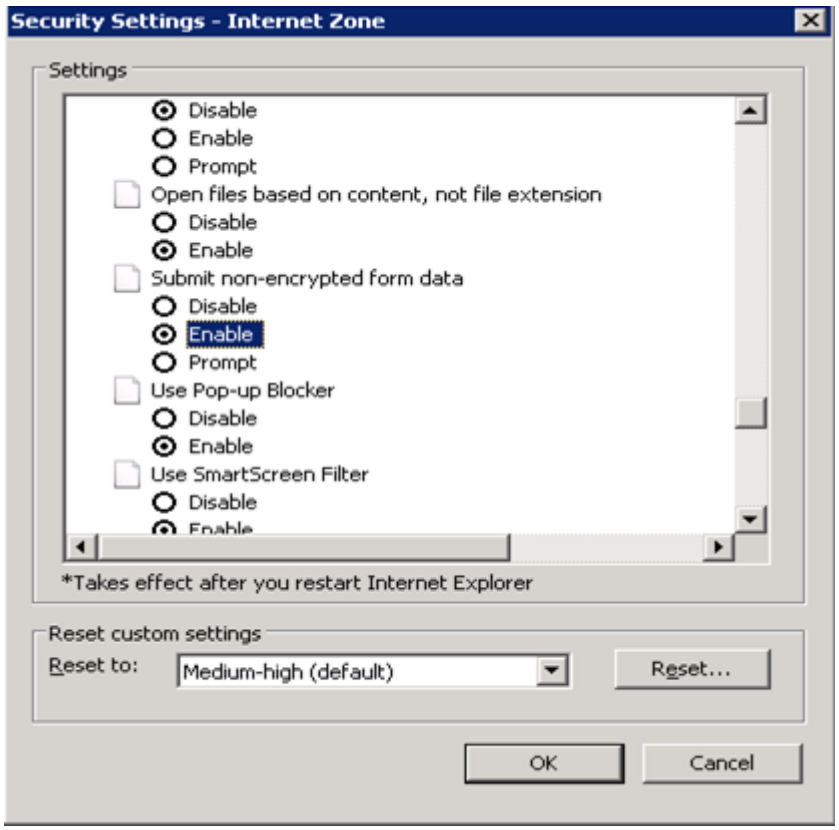
Figure 16-19 Internet Options



3. In the **Security Settings-Internet Zone** window, select **Enable** under **Submit non-encrypted from data** and **Enable** under **Active scripting**, and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-20 Security Settings-Internet Zone



4. In the **Internet Options** window, click **OK**.

----End

16.4 How Do I View All English Fields Completely on the eSight English GUI When a Chinese-Version Firefox Is Used?

Symptom

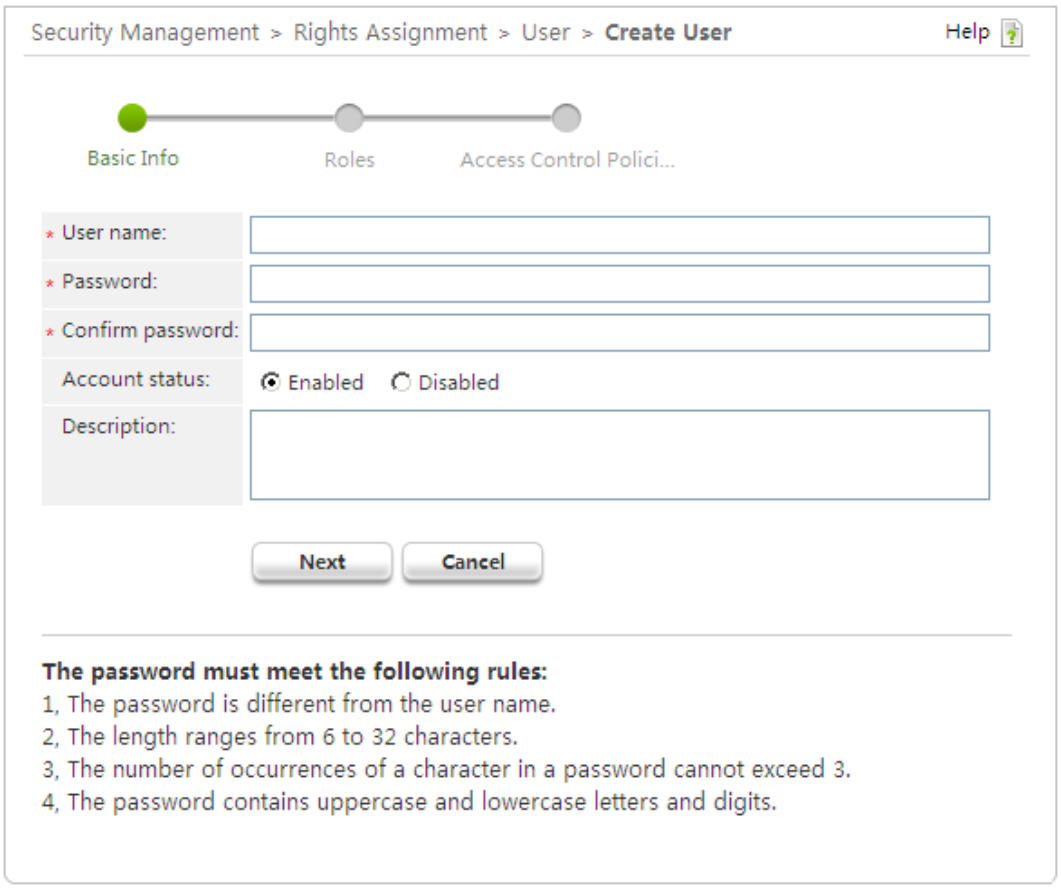
A few English fields cannot be displayed completely during the process of creating roles or users when Mozilla Firefox of the eSight GUI in English. However, this problem does not occur if Internet Explorer is used.

The problem may occur in the following scenarios:

- Scenario 1: On the English UI for creating users, the fields shown in **Figure 16-21** cannot be displayed completely.

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

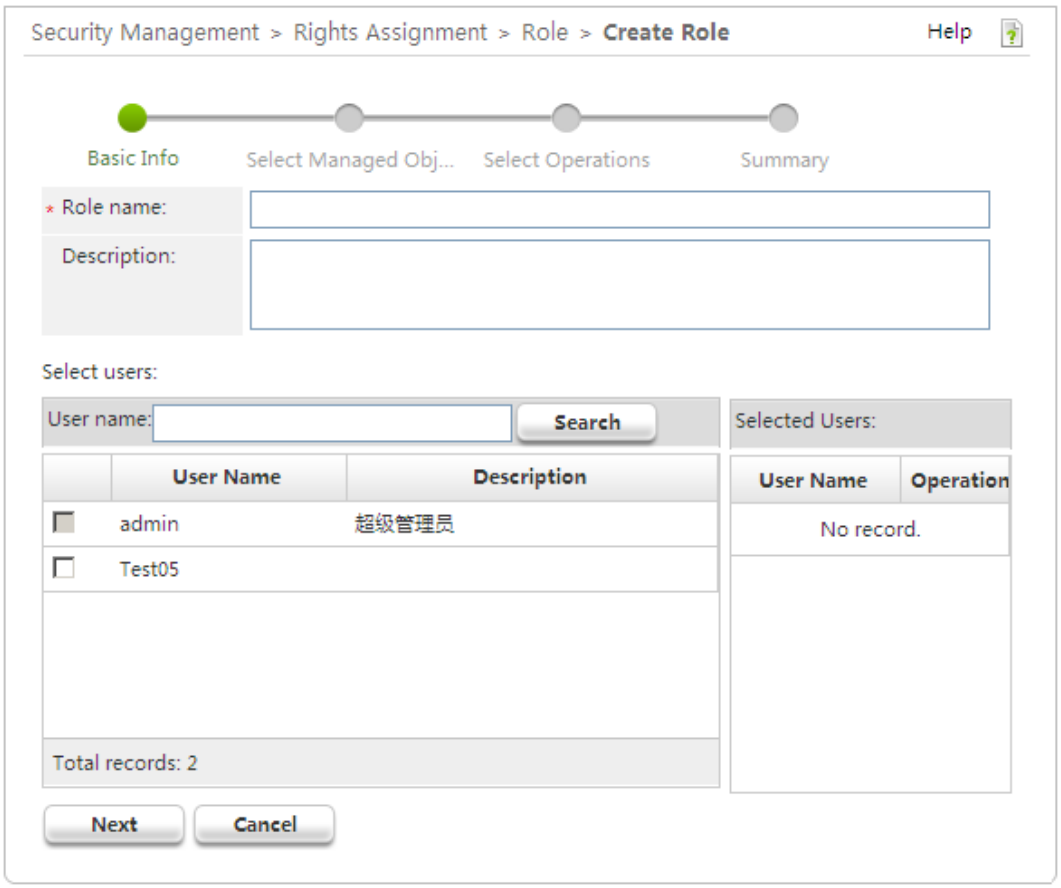
Figure 16-21 Fields that cannot be displayed completely



- Scenario 1: On the English UI for creating roles, the fields shown in **Figure 16-22** cannot be displayed completely.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-22 Fields that cannot be displayed completely



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

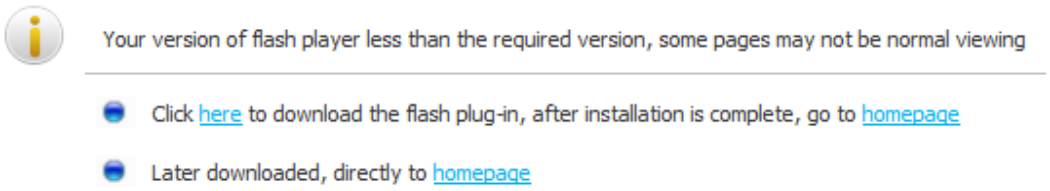
Copyright © Huawei Technologies Co., Ltd.

16.5 How Do I Solve the Problem When Adobe Flash Player Provided by eSight Fails to Be Installed in Internet Explorer?

Symptom

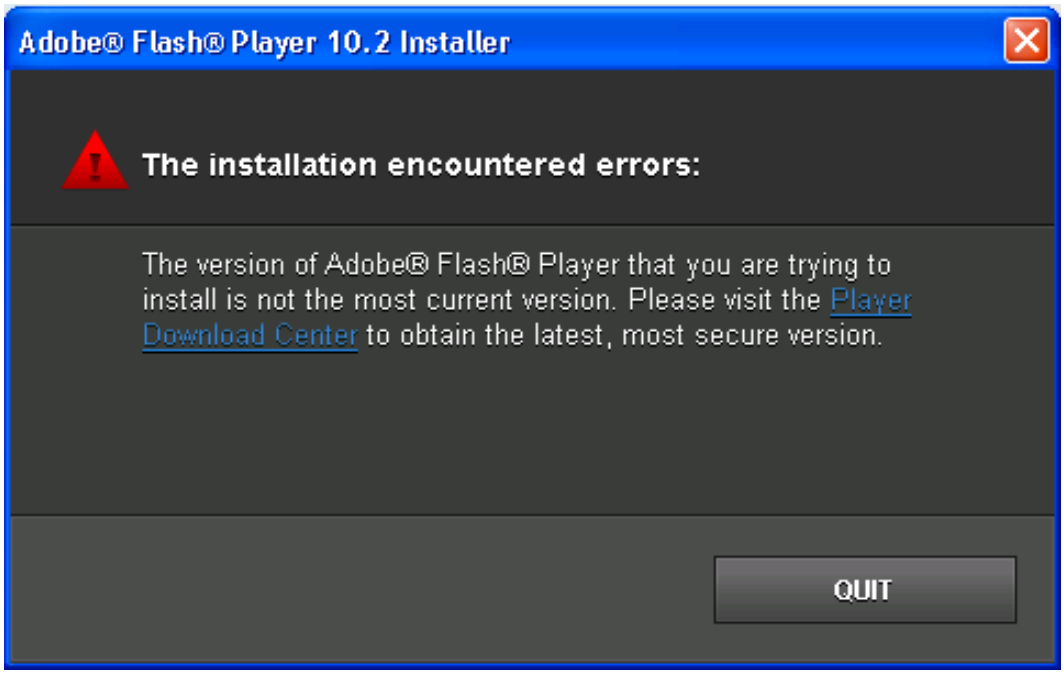
If Internet Explorer is used to access theeSight, the message shown in **Figure 16-23** is displayed after you log in.

Figure 16-23 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 16-24** is displayed, indicating installation failure.

Figure 16-24 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.

Copyright © Huawei Technologies Co., Ltd.

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.

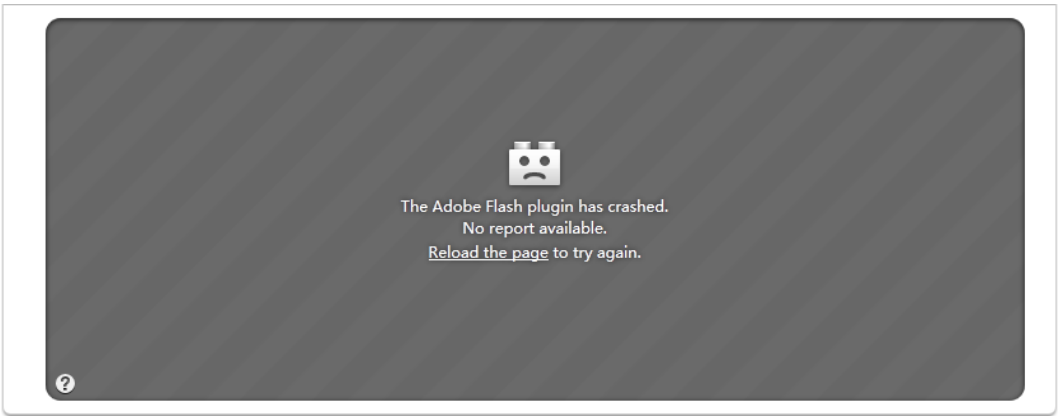
----End

16.6 How Do I Solve the Problem When a Message Indicating That the Flash Plug-in Crashes Is Displayed When I Use Firefox to Access the eSight Flash Pages?

Symptom

When I use Firefox Mozilla to access the eSight flash pages, such as the alarm bar chart, topology page, and performance monitoring page, the system displays a message shown in **Figure 16-25**.

Figure 16-25 The flash plug-in crashes



Possible Causes

- During the running of the Flash plug-in, a conflict occurs when reading and writing the memory. Firefox Mozilla automatically ends the plug-in management process to ensure normal running, which causes that the Flash plug-in crashes.

Copyright © Huawei Technologies Co., Ltd.

- The memory and CPU of the operating system where Firefox Mozilla is running is insufficient so that Firefox Mozilla automatically ends the plug-in management process, which causes that the Flash plug-in crashes.

Procedure

Step 1 Click the **Reload the page** link.

The first page of the eSight is displayed, and 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 in the **Topology Management** window.

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 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.

Copyright © Huawei Technologies Co., Ltd.

Answer

Step 1 Click **Start**, and enter **firewall.cpl** in **Search Programs and files**.

The **Windows Firewall** window is displayed.

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 **Home or work(private) network location settings** or **Public network location settings** area based on your actual network location, and click **OK**.

The **Windows Firewall** window is displayed.

Step 3 Click **Advanced Settings** on the left.

The **Windows Firewall with Advanced Security** window is displayed.

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**.

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**.

Step 8 Click **Allow the connection**, and click **Next**.

Step 9 Click **Next**.

Step 10 Click **Next**, and set **Name** and **Description**.

Click **Finish**.

----End

16.9 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.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Stop eSight services.

- Windows operating system:
  1. Choose **Start** > **All Programs** > **eSight** > **shutdown eSight**.
- SUSE Linux operating system:
  1. **cd /opt/eSight/AppBase/bin**
  2. **./stop.sh**

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**:

Copyright © Huawei Technologies Co., Ltd.

```
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 /opt/eSight/AppBase/bin**
  2. **./run.sh**

----End

16.10 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

Copyright © Huawei Technologies Co., Ltd.

ranges from 20 GB to 320 GB. For details, see the *Huawei eSight V200R002C00 Release Notes*.

----End

16.11 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.
  3. In the **Features** window, click **Add Features**.

     The **Add Features Wizard** dialog box is displayed.
  4. Select **SNMP services**, and click **Next**.
  5. Click **Install**. The system starts to install the SNMP service.
  6. Choose **Start** > **Administrative Tools** > **Services**.
  7. In the **Services** window, right-click **SNMP Service**, and choose **Properties** from the shortcut menu.

     The **SNMP Service Properties** dialog box is displayed.
  8. Click the **Security** tab.
  9. Click **Add**.

     The **SNMP Service Configuration** dialog box is displayed.
  10. Set **Community rights** to **READ ONLY** and **Community Name** to **public**, and click **Add**.
  11. Click **Add**.

      The **SNMP Service Configuration** dialog box is displayed.
  12. Set **Community rights** to **READ WRITE** and **Community Name** to **private**, and click **Add**.
  13. Select **Accept SNMP packets from any host**, and click **OK**.
- 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**.
  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**.

Copyright © Huawei Technologies Co., Ltd.

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

16.12 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

Copyright © Huawei Technologies Co., Ltd.

A Glossary

A

AAA	See **Authentication, Authorization and Accounting.**
ABR	See **available bit rate.**
AC	See **access controller.**
ACL	See **access control list.**
ADMC	auto detected manual confirmed
AES	See **Advanced Encryption Standard.**
AH	See **Authentication Header.**
AIS	alarm indication signal
ANCP	See **Access Node Control Protocol.**
APS	automatic protection switching
ARP	See **Address Resolution Protocol.**
ARQ	See **automatic repeat request.**
AS	See **autonomous system.**
ASE	amplified spontaneous emission
ASIC	See **application-specific integrated circuit.**
ASM	See **any-source multicast.**
ATAE	See **Advanced Telecommunications Application Environment.**
ATM	asynchronous transfer mode
Access Node Control Protocol (ANCP)	An IP-based protocol that operates between the access node (AN) and the network access server (NAS), over a DSL access and aggregation network.
Address Resolution Protocol (ARP)	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.
Advanced Encryption Standard (AES)	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.

Copyright © Huawei Technologies Co., Ltd.

Advanced Telecommunications Application Environment (ATAE)	A carrier-class processing platform that is designed to meet the service application requirement of high performance, high specialization, and high integration.
Authentication Header (AH)	A protocol that provides connectionless integrity, data origin authentication, and anti-replay protection for IP data.
Authentication, Authorization and Accounting (AAA)	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.
access control list (ACL)	A list of entities, together with their access rights, which are authorized to have access to a resource.
access controller (AC)	A device that controls and manages all associated access points (APs) in a WLAN. An AC can work with the authentication server to provide the authentication service for WLAN users.
any-source multicast (ASM)	A multicast service mode. In ASM mode, any sender can become the multicast source to send information to a multicast group address. After joining the multicast group identified by this address, multiple receivers can receive all the information sent to this multicast group.
application-specific integrated circuit (ASIC)	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.
attack	An attempt to bypass security controls in a system with the mission of using that system or compromising it. An attack is usually accomplished by exploiting a current vulnerability.
automatic repeat request (ARQ)	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.
autonomous system (AS)	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.
available bit rate (ABR)	A kind of service categories defined by the ATM forum. ABR only provides possible forwarding service and applies to the connections that does not require the real-time quality. It does not provide any guarantee in terms of cell loss or delay.

B

B-VLAN	backbone virtual local area network
BFD	See **Bidirectional Forwarding Detection.**
BGP	Border Gateway Protocol
BITS	See **building integrated timing supply.**
BPDU	See **bridge protocol data unit.**
BRAS	See **broadband remote access server.**
BSSID	basic service set identifier

Copyright © Huawei Technologies Co., Ltd.

Bidirectional Forwarding Detection (BFD)	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.
backplane	An electronic circuit board containing circuits and sockets into which additional electronic devices on other circuit boards or cards can be plugged.
blacklist	A method of filtering packets based on their source IP addresses. Compared with ACL, the match condition for the black list is much simpler. Therefore, the black list can filter packets at a higher speed and can effectively screen the packet sent from the specific IP address.
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	A means of delivering information to all members in a network. The broadcast range is determined by the broadcast address.
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.
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.

C

CA	Certificate Authority
CAC	See **connection admission control.**
CAR	committed access rate
CC	ceramic capacitor
CCC	circuit cross connect
CCM	call control module
CDR	See **call detail record.**

Copyright © Huawei Technologies Co., Ltd.

CE	See **customer edge.**
CES	See **circuit emulation service.**
CF	See **call forwarding.**
CFM	connectivity fault management
CG	See **charging gateway.**
CHAP	See **Challenge Handshake Authentication Protocol.**
CLC	cluster line-card chassis
CLI	command-line interface
CMPP	China Mobile Peer to Peer Protocol
CPLD	complex programmable logical device
CR-LSP	constraint-based routed label switched path
CRC	See **cyclic redundancy check.**
CRD	call rerouting distribution
CRL	See **certificate revocation list.**
CSPF	constraint shortest path first
Challenge Handshake Authentication Protocol (CHAP)	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 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.
call detail record (CDR)	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.
call forwarding (CF)	A feature on telephone networks that allows an incoming call to a called party, who is unavailable, to be redirected to another telephone.
certificate revocation list (CRL)	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.
charging gateway (CG)	A charging function component that provides functions such as charging data collection, rating, charging, and service control in the network. For services, the CGW exists in the way similar to a router. The CGW does not function as a proxy or gateway.
circuit emulation service (CES)	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.
clock source	A device that provides standard time for the NTP configuration.
cluster	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.

Copyright © Huawei Technologies Co., Ltd.

collection period	An interval at which the measurement results are output. During the measurement time, the system selects the given period as granularity to perform test and output the results. The EMS BMS supports multiple collection periods such as 5 minutes, 15 minutes, 30 minutes, 1 hour, and 1 day.
configuration file	A file that contains machine-readable operating specifications for a piece of hardware or software or that contains information on another file or on a specific user, such as the user's login ID.
connection admission control (CAC)	A control process in which the network takes actions in the call set-up phase (or call re-negotiation phase) to determine which connection request is admitted.
customer edge (CE)	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.
cyclic redundancy check (CRC)	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.

D

DES	See **Data Encryption Standard.**
DHCP	See **Dynamic Host Configuration Protocol.**
DIMM	See **dual in-line memory module.**
DNS	See **domain name system.**
DOD	dial-on-demand
DPI	deep packet inspection
DR	dielectric resonator
DRR	dynamic rate repartitioning
DSP	See **digital signal processor.**
Data Encryption Standard (DES)	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.
Dynamic Host Configuration Protocol (DHCP)	A client-server networking protocol. A DHCP server provides configuration 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.
device panel	The interface that is used to indicate the panel of physical devices and their status in the NMS.
digital signal processor (DSP)	A microprocessor designed specifically for digital signal processing, generally in real time.
domain name system (DNS)	A mechanism of mapping easy-to-remember domain names to IP addresses recognizable for network devices.
downstream	In an access network, the direction of transmission toward the subscriber end of the link.

Copyright © Huawei Technologies Co., Ltd.

dual in-line memory module (DIMM)	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.
E	
E1	A European standard for high-speed data transmission at 2.048 Mbit/s. It provides thirty-two 64 kbit/s channels.
EBGP	External Border Gateway Protocol
ECC	error checking and correcting
ECM	entitlement control message
EEPROM	See **electrically erasable programable read-only memory.**
EFM	Ethernet in the first mile
EMC	See **electromagnetic compatibility.**
EPLD	See **erasable programmable logic device.**
EPON	See **Ethernet passive optical network.**
ESN	See **equipment serial number.**
ESP	See **Encapsulating Security Payload.**
Encapsulating Security Payload (ESP)	A protocol that uses encryption and authentication mechanisms. It authenticates the source of IP packets, and ensures data integrity, anti-replay and confidentiality.
Ethernet passive optical network (EPON)	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.
electrically erasable programable read-only memory (EEPROM)	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 reprograming. EEPROMs contain less memory than RAM, take longer to reprogram, and can be reprogramed only a limited number of times before wearing out.
electromagnetic compatibility (EMC)	A condition which prevails when telecommunications equipment is performing its 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.
equipment serial number (ESN)	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".
erasable programmable logic device (EPLD)	A logic 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.

Copyright © Huawei Technologies Co., Ltd.

explicit path	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.
F	
FAD	fabric adapter
FDI	See **forward defect indication.**
FE	See **fast Ethernet.**
FEC	See **forward error correction.**
FIB	See **forward information base.**
FPGA	See **field programmable gate array.**
FPIC	flexible plug-in card
FR	See **frame relay.**
FRR	See **fast reroute.**
FSM	finite state machine
FTP	File Transfer Protocol
FUP	fair usage policy
Fabric	A kind of bus/plane used to exchange system service data.
fast Ethernet (FE)	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).
fast reroute (FRR)	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.
field programmable gate array (FPGA)	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.
forward defect indication (FDI)	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.
forward error correction (FEC)	A bit error correction technology that adds the correction information to the payload at the transmit end. Based on the correction information, the bit errors generated during transmission are corrected at the receive end.

Copyright © Huawei Technologies Co., Ltd.

forward information base (FIB)	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.
frame relay (FR)	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.

G

GE	See **gigabit Ethernet.**
GEM	GPON encapsulation mode
GGSN	See **gateway GPRS support node.**
GR	See **graceful restart.**
GR helper	A neighbor of a GR restarter. The GR helper must support GR.
GTP	GPRS tunneling protocol
GUI	graphical user interface
gateway	A device that connects two network segments using different protocols. It is used to translate the data in the two network segments.
gateway GPRS support node (GGSN)	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.
gigabit Ethernet (GE)	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.
graceful restart (GR)	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.
group address	An address used by sources and the receivers to send and receive multicast messages.

H

HA	See **high availability.**
HCT	health check tool

Copyright © Huawei Technologies Co., Ltd.

HDLC	High-Level Data Link Control
HGMP	Huawei Group Management Protocol
HTTPS	See **Hypertext Transfer Protocol Secure.**
Hypertext Transfer Protocol Secure (HTTPS)	The HTTP running on top of TLS or SSL for secured transactions.
high availability (HA)	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.
hop	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.

I

IC	See **integrated circuit.**
ICMP	See **Internet Control Message Protocol.**
IGMP	See **Internet Group Management Protocol.**
IGP	See **Interior Gateway Protocol.**
IKE	See **Internet Key Exchange.**
IP Security (IPSec)	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.
IP address	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.
IPSec	See **IP Security.**
IPv4	See **Internet Protocol version 4.**
IPv6	See **Internet Protocol version 6.**
IS-IS	See **Intermediate System to Intermediate System.**
ISAKMP	See **Internet Security Association and Key Management Protocol.**
ISP	See **Internet service provider.**
ISSU	See **in-service software upgrade.**
Interior Gateway Protocol (IGP)	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).
Intermediate System to Intermediate System (IS-IS)	A protocol used by network devices (routers) to determine the best way to forward datagram or packets through a packet-based network.

Copyright © Huawei Technologies Co., Ltd.

Internet Control Message Protocol (ICMP)	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).
Internet Group Management Protocol (IGMP)	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.
Internet Key Exchange (IKE)	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 provides users with access to the Internet and related services.
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.
integrated circuit (IC)	A combination of inseparable associated circuit elements that are formed in place and interconnected on or within a single base material to perform a microcircuit function.

J

jitter	Short waveform variations caused by vibration, voltage fluctuations, and control system instability.

L

L2TP	Layer 2 Tunneling Protocol
L2TP network server (LNS)	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.
L2VPN	Layer 2 virtual private network

Copyright © Huawei Technologies Co., Ltd.

L3VPN	Layer 3 virtual private network
LA	See **link aggregation.**
LAC	link access control
LACP	See **Link Aggregation Control Protocol.**
LAG	See **link aggregation group.**
LC	line card
LCP	Link Control Protocol
LCT	local craft terminal
LDAP	See **Lightweight Directory Access Protocol.**
LDP	Label Distribution Protocol
LDP peer	Two LSRs that use LDP to exchange labels or FEC mappings. LDP sessions exist between them.
LIG	lawful interception gateway
LLDP	See **Link Layer Discovery Protocol.**
LNS	See **L2TP network server.**
LOS	See **loss of signal.**
LPU	line interface processing unit
LSA	link state advertisement
LSDB	link state database
LSP	locally significant part
LSR	See **label switching router.**
Layer 2 multicast	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.
Lightweight Directory Access Protocol (LDAP)	A TCP/IP based network protocol that enables access to a DSA. It involves some reduced functionality from X.500 DAP specification.
Link Aggregation Control Protocol (LACP)	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.
Link Layer Discovery Protocol (LLDP)	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.
label switching router (LSR)	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.
link aggregation (LA)	A method for bundling a group of physical ports into a logical port to increase the bandwidth.

Copyright © Huawei Technologies Co., Ltd.

link aggregation group (LAG)	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.
loss of signal (LOS)	No transitions occurring in the received signal.
M	
MAC address	A link layer address or physical address. It is six bytes long.
MAC address authentication	An authentication method based on port and MAC address and used to control the network access authority of users. In the MAC address authentication mode, a list of permitted MAC addresses is maintained manually and serves as the criterion for filtering the MAC addresses of STAs. However, the efficiency of this method decreases as the number of STAs increases. Therefore, this method is applicable to scenarios that do not have a high requirement on security, such as the home scenario and small office scenario.
MD	See **maintenance domain.**
MD5	See **message digest algorithm 5.**
MEG	See **maintenance entity group.**
MEP	maintenance association end point
MIB	See **management information base.**
MLD	See **multicast listener discovery.**
MLR	media loss ratio
MP	Multilink Protocol
MPLS	See **Multiprotocol Label Switching.**
MPLS TE	multiprotocol label switching traffic engineering
MPLS TP	See **Multiprotocol Label Switching traffic policing.**
MPLS VPN	See **multiprotocol label switching virtual private network.**
MPU	main processing unit
MSDP	See **Multicast Source Discovery Protocol.**
MSTP	See **multi-service transmission platform.**
MTU	See **maximum transmission unit.**
Multicast Source Discovery Protocol (MSDP)	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.
Multiprotocol Label Switching (MPLS)	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.

Copyright © Huawei Technologies Co., Ltd.

Multiprotocol Label Switching traffic policing (MPLS TP)	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.
mVRRP	management Virtual Router Redundancy Protocol
maintenance domain (MD)	The network or the part of the network for which connectivity is managed by connectivity fault management (CFM). The devices in a maintenance domain are managed by a single Internet service provider (ISP).
maintenance entity group (MEG)	A MEG consists of MEs that meet the following criteria: ● Exist within the same management edges. ● Have the same MEG hierarchy. ● Belong to the same P2P or P2MP connection.
management information base (MIB)	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.
masked alarm	An alarm whose correlation action is set to masked in alarm correlation analysis.
maximum transmission unit (MTU)	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.
message digest algorithm 5 (MD5)	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.
multi-service transmission platform (MSTP)	A platform based on the SDH platform, capable of accessing, processing and transmitting TDM services, ATM services, and Ethernet services, and providing unified management of these services.
multicast listener discovery (MLD)	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.
multiprotocol label switching virtual private network (MPLS VPN)	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

NAP	network access point

Copyright © Huawei Technologies Co., Ltd.

NAS	network access server
NCP	Network Control Protocol
NDP	See **Neighbor Discovery Protocol.**
NE	network element
NM	network management
NP	See **network processor.**
NPE	network provider edge
NQA	network quality analysis
NVRAM	nonvolatile random access memory
Neighbor Discovery Protocol (NDP)	A protocol that is used to discover the information of the neighboring Huawei device that is connected with the local device.
network processor (NP)	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.
network segment	A part of an Ethernet or other network, on which all message traffic is common to all nodes, that is, it is broadcast from one node on the segment and received by all others.
node	A managed device in the network. For a device with a single frame, one node stands for one device. For a device with multiple frames, one node stands for one frame of the device. Therefore, a node does not always mean a device.

O

OAM	See **operation, administration and maintenance.**
OAMPDU	operation, administration and maintenance protocol data unit
OB	outside broadcast
ODR	origin dependent routing
OFC	optical fiber communication conference and exhibit
OID	object identifier
OLT	optical line terminal
OM	optical multiplexing
OMC	See **operation and maintenance center.**
OMS	operational management system
ONU	See **optical network unit.**
OPM	optical performance monitor
OSPF	See **Open Shortest Path First.**
OWD	one-way delay

Copyright © Huawei Technologies Co., Ltd.

Open Shortest Path First (OSPF)	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.
operation and maintenance center (OMC)	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.
operation, administration and maintenance (OAM)	A group of network support functions that monitor and sustain segment operation, activities that are concerned with, but not limited to, failure detection, 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.
optical attenuator	A passive device that increases the attenuation in a fiber link. It is used to ensure that the optical power of the signals received at the receive end is not extremely high. It is available in two types: fixed attenuator and variable attenuator.
optical fiber	A thin filament of glass or other transparent material, through which a signal-encoded light beam may be transmitted using total internal reflection.
optical network unit (ONU)	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.

P

P2P	See **point-to-point service.**
PA	See **planned area.**
PAP	push access protocol
PCB	See **printed circuit board.**
PCI	physical cell identifier
PCS	physical coding sublayer
PD	product daemon
PDSN	See **packet data serving node.**
PE	See **provider edge.**
PHB	See **per-hop behavior.**
PIC	parallel interference cancellation
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast - Sparse Mode
PLL	See **phase-locked loop.**
PON	passive optical network
POS	See **packet over SDH/SONET.**

Copyright © Huawei Technologies Co., Ltd.

PPP	Point-to-Point Protocol
PRI	primary rate interface
PSN	See **packet switched network.**
PSP	principal state of polarization
PTN	public telecommunications network
PTP	Precision Time Protocol
PTP clock	See **Precision Time Protocol clock.**
PVC	See **permanent virtual circuit.**
PW	See **pseudo wire.**
PWE3	See **pseudo wire emulation edge-to-edge.**
PoE	power over Ethernet
Precision Time Protocol clock (PTP clock)	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.
packet data serving node (PDSN)	A gateway used to connect the mobile network and the IP backbone network. It provides access to packet data service for mobile subscribers.
packet loss	The discarding of data packets in a network when a device is overloaded and cannot accept any incoming data at a given moment.
packet over SDH/ SONET (POS)	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.
packet switched network (PSN)	A telecommunications network that works in packet switching mode.
per-hop behavior (PHB)	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).
performance alarm	An alarm generated when the actual result of a measurement entity equals the predefined logical expression for threshold or exceeds the predefined threshold.
performance monitoring task	A task of monitoring performance in real time. The user can set the real-time monitoring counters or counter calculation expression. The real-time data is displayed in the form of table or figure, and is periodically refreshed based on the monitoring conditions.
permanent virtual circuit (PVC)	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.

Copyright © Huawei Technologies Co., Ltd.

phase-locked loop (PLL)	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.
physical layer	Layer 1 in the Open System Interconnection (OSI) architecture; the layer that provides services to transmit bits or groups of bits over a transmission link between open systems and which entails electrical, mechanical and handshaking.
physical link	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.
ping	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.
ping test	A test that is performed to send a data packet to the target IP address (a unique IP address on the device on the network) to check whether the target host exists according to the data packet of the same size returned from the target host.
planned area (PA)	A data area that serves as an off-line workspace where data is synchronized with the current data area before data configuration.
point-to-point service (P2P)	A service between two terminal users. In P2P services, senders and recipients are terminal users.
ppm	parts per million
printed circuit board (PCB)	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.
provider edge (PE)	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.
pseudo wire (PW)	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.
pseudo wire emulation edge-to-edge (PWE3)	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.

Q

QinQ	A layer 2 tunnel protocol based on IEEE 802.1Q encapsulation. It add a public VLAN tag to a frame with a private VLAN tag to allow the frame with double VLAN tags to be transmitted over the service provider's backbone network based on the public VLAN tag. This provides a layer 2 VPN tunnel for customers and enables transparent transmission of packets over private VLANs.
QoS	See **quality of service.**

Copyright © Huawei Technologies Co., Ltd.

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

RAC	See **Real Application Clusters.**
RADIUS	See **Remote Authentication Dial-In User Service.**
RBS	record bill server
RDI	remote defect indication
RDS	See **replicated data set.**
RF	See **radio frequency.**
RM	See **redundancy machine.**
RMEP	remote maintenance association end point
RMON	See **remote monitor.**
RP	routing performer
RPC	See **remote procedure call.**
RPU	resource process unit
RRPP	See **Rapid Ring Protection Protocol.**
RSSI	See **received signal strength indicator.**
RSVP-TE	See **Resource ReserVation Protocol-Traffic Engineering.**
RTD	See **round-trip delay.**
RTN	radio transmission node
RTT	round trip time
Rapid Ring Protection Protocol (RRPP)	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.
Real Application Clusters (RAC)	A component of the Oracle database that allows a database to be installed across multiple servers and to run any packaged or customized application software without any modification.
Remote Authentication Dial-In User Service (RADIUS)	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.
Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)	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.

Copyright © Huawei Technologies Co., Ltd.

radio frequency (RF)	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.
received signal strength indicator (RSSI)	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
redundancy machine (RM)	A machine that provides the redundancy function for the production machine. The redundancy machine is a single-node system.
remote monitor (RMON)	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.
remote neighbor	If two adjacent devices are not directly connected but through intermediate devices, they are called remote neighbors.
remote procedure call (RPC)	An inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programer explicitly coding the details for this remote interaction. That is, the programer writes essentially the same code whether the subroutine is local to the executing program, or remote. When the software in question uses object-oriented principles, RPC is called remote invocation or remote method invocation.
replicated data set (RDS)	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.
round-trip delay (RTD)	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.
route	The path that network traffic takes from its source to its destination. In a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.
router ID	A unique identifier of a router in an AS, which is an integer of 32 bits.
routing table	A table that stores and updates the locations (addresses) of network devices. Routers regularly share routing table information to be up to date. A router relies on the destination address and on the information in the table that gives the possible routes--in hops or in number of jumps--between itself, intervening routers, and the destination. Routing tables are updated frequently as new information is available.

S

SA	See **security association.**
SAS	serial attached SCSI
SDH	See **synchronous digital hierarchy.**
SDRAM	See **synchronous dynamic random access memory.**

Copyright © Huawei Technologies Co., Ltd.

SEE	See **service execution environment.**
SFU	signal filtering unit
SGIP	Short Message Gateway Interface Protocol
SIG	See **security immunity gateway.**
SLA	See **service level agreement.**
SM	switching module
SMG	See **short message gateway.**
SMPP	See **Short Message Peer to Peer.**
SMS	Service Management System
SMTP	See **Simple Mail Transfer Protocol.**
SNMP	See **Simple Network Management Protocol.**
SOAP	Simple Object Access Protocol
SPI	synchronous physical interface
SPS	See **Service Process Server.**
SPU	service process unit
SQ	See **subscriber queue.**
SRAM	See **static random access memory.**
SRU	SHDSL regenerator unit
SSL	See **Secure Sockets Layer.**
SSM	source-specific multicast
STP	Spanning Tree Protocol
SVC	See **switched virtual circuit.**
Secure Sockets Layer (SSL)	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.
Service Process Server (SPS)	An internal module of the EIE for parsing and running service scripts defined by users.
Short Message Peer to Peer (SMPP)	An open message-transfer protocol that enables short message entities (SMEs) outside the mobile network to interface with an SMSC. Nonmobile entities that submit messages to, or receive messages from an SMSC are known as External Short Message Entities (ESMEs).
Simple Mail Transfer Protocol (SMTP)	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.
Simple Network Management Protocol (SNMP)	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.

Copyright © Huawei Technologies Co., Ltd.

security association (SA)	Security information that is shared by the BS and the MS and is used for communication encryption. The SA includes key information and encryption algorithms.
security immunity gateway (SIG)	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.
service execution environment (SEE)	A platform that is developed over the enhanced network intelligent platform (ENIP) CORE. The open messaging enabler (OME) is the core of the SEE.
service level agreement (SLA)	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.
short message gateway (SMG)	A gateway that provides a short message access platform with the interconnection function in the entire network for Service Providers (SPs). It provides the bearing function so that SPs can provide value-added short message services to mobile subscribers throughout the nation.
static random access memory (SRAM)	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.
subscriber queue (SQ)	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.
switched virtual circuit (SVC)	A logical connection between two nodes on a packet-switching network that is established only when data is to be transmitted.
synchronous digital hierarchy (SDH)	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.**
TE	terminal equipment
TFTP	See **Trivial File Transfer Protocol.**
TLV	See **type-length-value.**
TNS	transit network selection

Copyright © Huawei Technologies Co., Ltd.

TP	See **topology protection.**
TTL	See **time to live.**
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.
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.
timer	Symbolic representation for a timer object (for example, a timer object may have a primitive designated as T-Start Request). Various MAC entities utilize timer entities that provide triggers for certain MAC state transitions.
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.
topology checksum (TC)	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.
topology object	A basic element in the NMS topology view, which includes submap, node, connection, and so on.
topology protection (TP)	Frames that are used to quickly detect topology changes and perform protection switching within 50 ms. In addition, the frames can be sent strictly according to the sequence without disorder or repeated sending. TP frames contain the topology information including the east and west span protection states, protection configuration information and whether to allow the jumbo frame pass through.
topology view	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.
traffic statistics	An activity of measuring and collecting statistics of various data on devices and telecommunications networks. With the statistics, operators can be aware of the operating status, signaling, users, system resource usage of the devices or networks. The statistics also help the operators manage the device operating, locate problems, monitor and maintain the networks, and plan the networks.
transparent transmission	A process during which the signaling protocol or data is not processed in the content but encapsulated in the format for the processing of the next phase.

Copyright © Huawei Technologies Co., Ltd.

trap message	An unprogramed conditional jump to a specified address that is automatically activated by hardware, a recording being made of the location from which the jump occurred.
trunk	Physical communications line between two offices. It transports media signals such as speech, data and video signals.
type-length-value (TLV)	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.

U

UDP	See **User Datagram Protocol.**
UPS	uninterruptible power supply
URPF	See **unicast reverse path forwarding.**
USAU	See **universal signaling access unit.**
User Datagram Protocol (UDP)	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.
unicast	The process of sending data from a source to a single recipient.
unicast reverse path forwarding (URPF)	A feature that helps to prevent network attacks based on spoofed IP source addresses.
universal signaling access unit (USAU)	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.
upper limit	The maximum consumption amount that a carrier sets for a subscriber in a bill cycle. If the consumption amount if a subscriber exceeds the maximum consumption amount that the carrier sets, the OCS still deducts the maximum consumption amount that the carrier sets.
upstream	In an access network, the direction that is far from the subscriber end of the link.
user group	The group of users that share a specific service, for example, user groups of the virtual private network (VPN) and enterprise private branch exchange (PBX). The user group is set to enjoy the special tariff, service, and reward. A user can belong to none or multiple user groups.

V

VB	virtual bridge
VCS	Veritas Cluster Server
VGMP	VRRP Group Management Protocol
VLAN	virtual local area network

Copyright © Huawei Technologies Co., Ltd.

VP	See **virtual path.**
VPLS	virtual private LAN segment
VPN	virtual private network
VPN instance	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.
VPN routing and forwarding (VRF)	A technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.
VRF	See **VPN routing and forwarding.**
VRP	See **Versatile Routing Platform.**
VRRP	See **Virtual Router Redundancy Protocol.**
VSI	virtual switch interface
VTY	See **virtual type terminal.**
Versatile Routing Platform (VRP)	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.
Virtual Router Redundancy Protocol (VRRP)	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.
VoIP	See **voice over IP.**
virtual IP address	The IP address that is used by the active node for the communication between the host and the LMT.
virtual NE	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.

Copyright © Huawei Technologies Co., Ltd.

virtual link	The logical connection between topological objects in the NMS topology view.
virtual path (VP)	A bundle of virtual channels, all of which are switched transparently across an ATM network based on a common VPI.
virtual type terminal (VTY)	A logical terminal line that is used to access the device through Telnet.
voice over IP (VoIP)	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

WAN	See **wide area network.**
WAPI	WLAN Authentication and Privacy Infrastructure
WEP	wired equivalent privacy
WLAN	See **wireless local area network.**
WTR	See **wait to restore.**
wait to restore (WTR)	The number of minutes to wait before services are switched back to the working line.
wide area network (WAN)	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.
wireless local area network (WLAN)	A hybrid of the computer network and the wireless communication technology. It uses wireless multiple address channels as transmission media and carriers out data interaction through electromagnetic wave to implement the functions of the traditional LAN.

X

XAUI	10 gigabit Ethernet Attachment Unit Interface

Copyright © Huawei Technologies Co., Ltd.