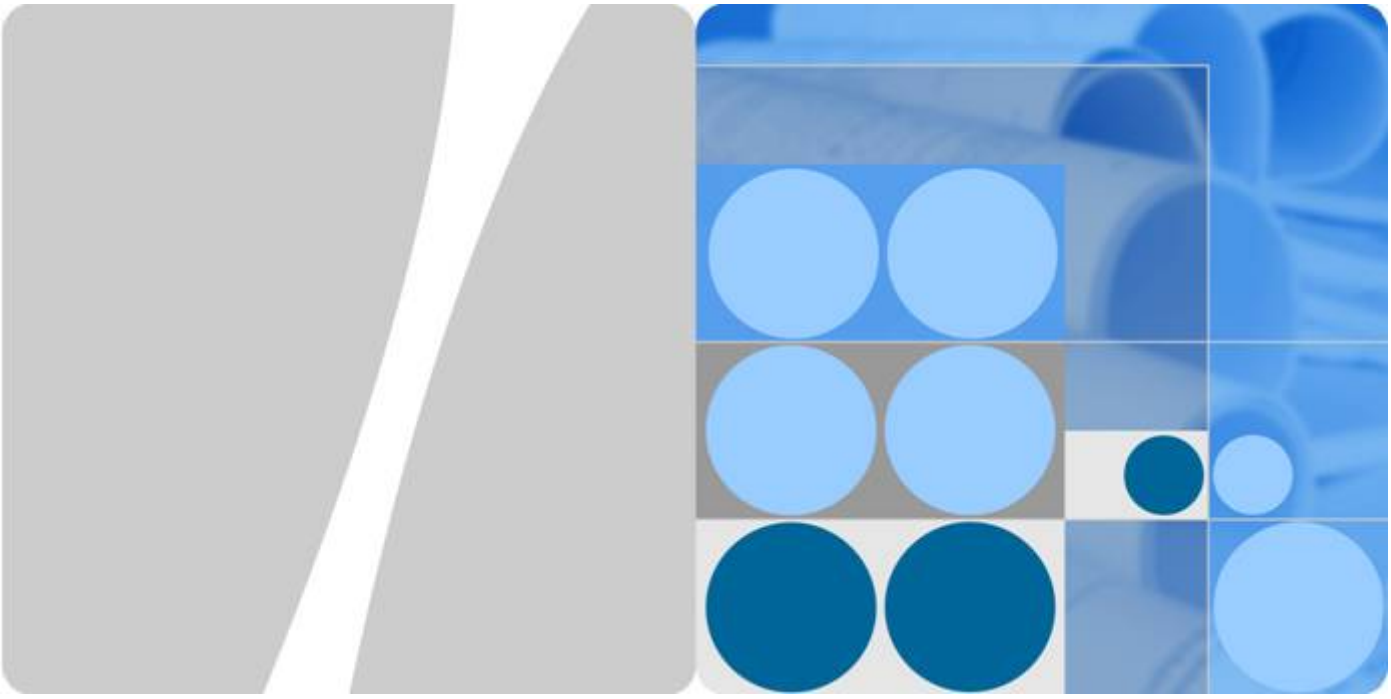


Huawei eSight AppBase

V200R001C00

Operation Guide

Issue 02

Date 2011-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Related Versions

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

Product Name	Version
eSight AppBase	V200R001C00

Intended Audience

This document guides the user to understand basic operations of the eSight.

The intended audiences of this document are:

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

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
TIP	Indicates a tip that may help you solve a problem or save you time.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A maximum of all or none can be selected.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.

Convention	Description
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Change History

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

Updates in Issue 02 (2011-09-30) Based on Product Version V200R001C00

The second release of the eSight V200R001C00.

Some bugs in the manual of the previous version are fixed.

Updates in Issue 01 (2011-08-31) Based on Product Version V200R001C00

The first release.

Contents

1 Getting Started

About This Chapter

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

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

1.11 Add a Lower-layer NMS

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

1.1 eSight Functions

This topic describes functions provided by eSight.

Table 1-1 Functions provided by eSight

Function	Description
Security management	The security management function is based on the role model. Users can manage specified devices and perform specified operations based on the assigned rights. ● eSight provides the functions of monitoring online users in real time and forcing users to go offline. ● eSight provides the function of defining requirements for accessing eSight server. ● Security policies on accounts and passwords.
Log management	Logs record important user operations. You can view and filter logs, and view a system log record. eSight manages operation logs, security logs, and system logs and provides information at warning, minor, and risky levels. ● Operation logs record operations on eSight. ● Security logs record activities related to system security. ● System logs record key information generated during eSight running and task execution.
Alarm management	The real-time alarm management involves in viewing the alarm board and event list, and browsing real-time and history alarms. You can set alarm remote notification rules, alarm suppression rules, and alarm sound.
Performance management	eSight can monitor key performance indicators (KPIs) of a network in real time, and collect statistics on performance data. On eSight> graphical user interfaces (GUIs), you can manage network performance easily.

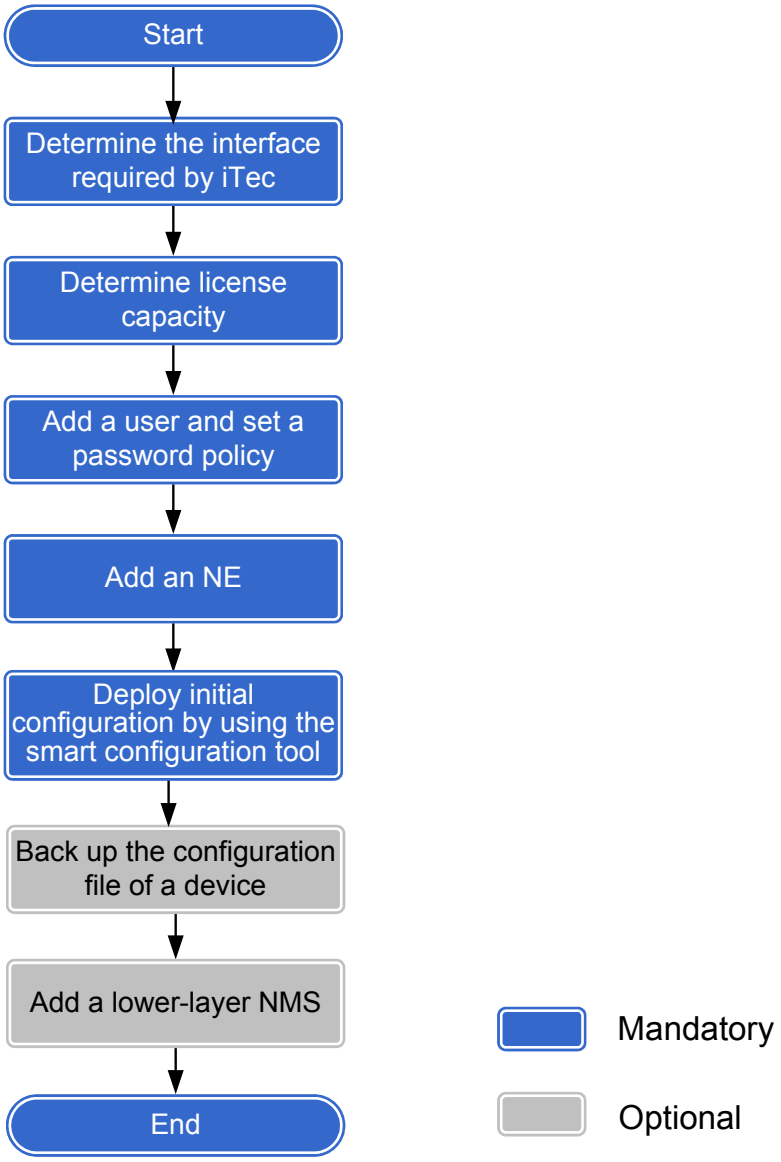
Function	Description
Report management	eSight provides various predefined reports and the easy-to-use report design function so that users can design reports to meet their own needs.
Configuration file management	eSight provides the function of automatically backing up, restoring, and comparing device configuration files so that device configuration data is recorded in real time and security of device configuration data is ensured.
NMSs of multiple layers	eSight provides the function of maintaining lower-layer Network Management Systems (NMSs) by the upper-layer NMS. You can display the page of a lower-layer NMS directly by clicking a link. This helps implement single sign-on (SS0) to lower-layer NMSs and the functions such as viewing alarms, topology, performance, and reports of lower-layer NMSs.
Resource management	eSight provides the functions such as managing, accessing, and moving resource models, adding, deleting, modifying, and querying resource attributes, auditing resources and controlling rights, managing version upgrade, controlling license capacity, and secondary development capabilities.
Topology management	On eSight GUI, a navigation tree is displayed on the left to show the network structure; objects of specified network layers are displayed with different coordinates on the background diagram on the right.
NE management	eSight provides the functions of managing Huawei routers, switches, access routers (ARs), and security devices and managing third-party devices based on the standard Management Information Base (MIB) by integrating with third-party devices. To manage Huawei devices, you can manage basic information, view device panels, manage device interface information, and view IP addresses.
Service	eSight provides the function of managing and monitoring Internet Protocol Security (IPSec) Virtual Private Network (VPN) and Wireless Local Area Network (WLAN) services.

1.2 Commissioning Process

This topic verifies eSight basic functions.

Figure 1-1 shows the commissioning process.

Figure 1-1 Commissioning process



Operation	Remarks
1.**1.3.1 Verifying Ports**	Verify that the required ports in the eSight port list are enabled so that eSight can use these ports properly.

Operation	Remarks
2. **1.3.2 Determining License Capacity**	Check the license capacity so that eSight can function properly.
3. **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. **1.8.2 Adding NEs to eSight**	Add network elements (NEs) to eSight and manage the NEs.
5. **1.9 Initialize the NEs By Using the SCT**	Deliver NE configuration scripts to NEs by using the intelligent configuration tool to initialize the NEs.
7. (Optional) **1.10 Back Up Device Configuration Files**	Back up device configuration files in a timely manner so that you can use the device configuration files for restore in case of accidents or misoperations. This helps enhance the configuration file security.
8. (Optional) **1.11 Add a Lower-layer NMS**	You can define lower-layer NMSs or each upper-layer NMS to implement the function of monitoring performance and alarms of lower-layer NMSs.

1.3 Commissioning Preparation

Before commissioning, verify that the required ports are enabled and the license capacity meets the requirements.

1.3.1 Verifying Ports

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

Table 1-2 describes ports in the port list.

Table 1-2 eSight port list

Port Number	Description	Enable When eSight Deployed Independently	Enable When eSight Connected to the Upper-Layer NMS	Enable on the Firewall of the Destination Device
8888	Hyper Text Transfer Protocol (HTTP) access port of the graphical command line.	Yes	Yes	Yes
8899	Port provided by the fault collection tool and report server for the eSight client to download reports.	Yes	Yes	Yes
8443	Port for logging in to the eSight main page.	Yes	Yes	Yes
38080	Online help port.	Yes	Yes	Yes
8030	Web service port.	Yes	Yes	Yes
8080	Web service port.	Yes	Yes	Yes
8009	Standard port used by tomcat's Apache JServ Protocol (AJP).	Yes	Yes	Yes
38988	Debug port of the backup tool Virgo.	Yes	Yes	No
9975	JMX management port of the backup tool Virgo.	Yes	Yes	No

Port Number	Description	Enable When eSight Deployed Independently	Enable When eSight Connected to the Upper-Layer NMS	Enable on the Firewall of the Destination Device
8533	Port for the database backup tool to log in to the database backup page.	Yes	Yes	Yes
8130	Web service port of the database backup tool.	Yes	Yes	Yes
38005	Port for stopping the Operation and Maintenance (OM) Web service.	Yes	Yes	No
38085	Port for stopping the Hedex Web service.	Yes	Yes	No
31004	JavaScript Object Notation (JSON) bus port.	Yes	Yes	No
31005	Hessian bus port.	Yes	Yes	No
31002	Open Services Gateway initiative (OSGI) management port of the Virgo.	Yes	Yes	No
39875	Java Management Extensions (JMX) management port of the Virgo.	Yes	Yes	No
38788	Debug port of the Virgo.	Yes	Yes	No

Port Number	Description	Enable When eSight Deployed Independently	Enable When eSight Connected to the Upper-Layer NMS	Enable on the Firewall of the Destination Device
32403	Operation and Maintenance System (OMS) state monitor port.	Yes	Yes	No
30999	Shell port of the Virgo.	Yes	Yes	No
31003	Port for eSight to obtain security management data from the SSO server.	Yes	Yes	No
31006	Port for connecting the Med Node to the Center.	Yes	Yes	No
33306	Port for connecting to the MySQL database.	Yes	Yes	Yes
8097	Debug port of the eSight installation disk.	Yes	Yes	No
31021	Port for the File Transfer Protocol (FTP) server to transferring files.	Yes	Yes	Yes
162	Port for receiving traps reported by managed devices.	Yes	Yes	Yes
10162	Port for receiving trap packets reported by managed devices.	Yes	Yes	No

Port Number	Description	Enable When eSight Deployed Independently	Enable When eSight Connected to the Upper-Layer NMS	Enable on the Firewall of the Destination Device
39008	Port for the Mediation to receive Simple Object Access Protocol (SOAP) protocol packets.	Yes	Yes	No
23	Telnet port.	Yes	Yes	Yes
161	Port for devices to receive Simple Network Management Protocol (SNMP) requests.	Yes	Yes	Yes
Random port	Port for sending trap packets to the upper-layer NMS.	No	Yes	Yes
4700	Port for eSight to receive commands from the upper-layer NMS.	No	Yes	Yes
7890	China Mobile Peer to Peer (CMPP) 2.0/2.1 protocol port.	The port is enabled when the corresponding Short Message Gateway (SMG) is used.	The port is enabled when the corresponding SMG is used.	Yes
7891	CMPP3.0 protocol port.	The port is enabled when the corresponding SMG is used.	The port is enabled when the corresponding SMG is used.	Yes
5018	Short Message Peer to Peer (SMPP) 3.3/3.4 protocol port.	The port is enabled when the corresponding SMG is used.	The port is enabled when the corresponding SMG is used.	Yes

Port Number	Description	Enable When eSight Deployed Independently	Enable When eSight Connected to the Upper-Layer NMS	Enable on the Firewall of the Destination Device
8801	Short message Gateway Interface Protocol (SGIP) 1.2 port.	The port is enabled when the corresponding SMG is used.	The port is enabled when the corresponding SMG is used.	Yes
5090	SMPP3.3/3.4 protocol port.	The port is enabled when the corresponding SMG is used.	The port is enabled when the corresponding SMG is used.	Yes
25	Simple Mail Transfer Protocol (SMTP) port.	The port is enabled when the SMTP Email server is used.	The port is enabled when the SMTP Email server is used.	Yes

NOTE

A random monitoring port on the firewall is temporarily enabled based on the session requirements. That is, the firewall receives responses from the peer end based on the port number and IP address. After the session ends, the random port is disabled. Therefore no dynamic port needs to be enabled on the firewall.

1.3.2 Determining License Capacity

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

Prerequisite

You have imported a license file into eSight.

Context

Table 1-3 describes the license information.

Table 1-3 License information

Item	Attribute	Description	Example
Basic License Information	Validity period	Date when the license file expires	2011-04-14

Item	Attribute	Description	Example
	Reminding days ahead	An alarm reporting that the license file will expire after the specified days is generated, and you need to import a new license file.	15
License Resource Control	Resource Name	Name of the resource for license file management	Client Count
	License Usage	Resource usage for license management	30/2000 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

1.4 Runtime Environment Requirements

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

Table 1-4 lists the runtime environment requirements for the client.

Table 1-4 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 XP, Windows 7 or Windows 2008
Browser	Mozilla Firefox 3.6 or Windows Internet Explorer 8.0 **NOTE** ● If Windows Internet Explorer 8.0 is used, you need to set the browsing mode by performing the following steps: 1. Open Windows Internet Explorer 8.0, and choose **Tools** > **Compatibility View Settings**. 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 NMS only on this client in Windows Internet Explorer 8.0. To modify the security policy, contact the operating system administrator.
Resolution	1024 x 768

1.5 Logging In to and Out of the eSight

This topic describes how to log in to and out of the eSight. The eSight works in Browser/Server mode. You can perform operations on the eSight only after logging in by using the browser.

Prerequisites

- The connection between the current browse and the eSight server is normal, and the eSight server works properly.
- The user account is created.

Background

- The system provides an initial user name **admin** and user password **admin** after it is installed. The user **admin** has all the operation rights of the eSight.
- The user **admin** needs to add users and roles after logging in to the eSight.
- You can choose **System** > **User Settings** to set screen lock period and password after logging in to the eSight.

CAUTION

To ensure security, you need to change the password of the user admin based on the password setting policy on the first access to theeSight.

While you performs return operation, directly use the return back function supported by the eSight system. The return back function supported by the web browser will lead to unpredictable problems.

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://10.10.10.1:8080/. The eSight login page is displayed.

Step 2 Enter the user name and password.

Step 3 Click **Login**.

- If the user name or password you entered is incorrect, the system displays an error message, for example, "Login failure. Incorrect user name or password."
- When the password will expire, you are prompted to change the password within the password expiration warning days.

----End

Logging Out of the eSight

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

Log out of the eSight.

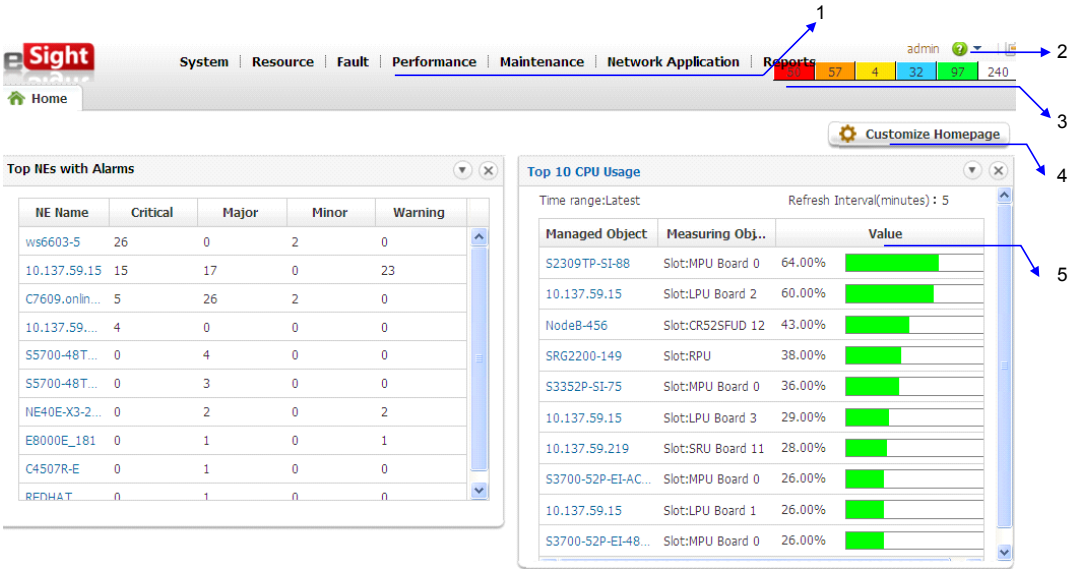
----End

1.6 Main Page

This topic describes eSight main page.

Figure 1-2 shows eSight main page.

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

1.7 Create User Accounts and Configure the Basic Information

This topic describes how to set a password policy to improve access security of the eSight. The password policy settings can include the user password complexity rules and password change interval. A password policy applies to all users once it is configured. Therefore, the password policy must be configured by the security administrator.

Prerequisite

You have permission to setting a password policy.

Context

- After a password policy is modified, the modification takes effect immediately for all users of the eSight. For example, if the minimum length of the user password is changed and if an online user changes the password, the new password used by the user must match the changed minimum length of the password to comply with the password policy.
- A new password policy does not affect the configured password.
- The password policy specifies the password complexity, password change interval, and character restrictions. Using the password policy prevents users from setting a very simple password or using the same password for a long time.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Security Policies** > **Password Policy**.

Step 3 Set a password policy based on the policy plan.

When creating users and roles, you need to set a password based on the configured account policy.

Step 4 Click **Apply**.

----End

1.8 NE Adding

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

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 Set the SNMPv3 parameters on the NE side.

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

1.8.2 Adding NEs to eSight

This topic describes how to create an NE manually. If you want a few different types of NEs to access the eSight, you need to create these NEs one by one.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

The accessed NEs are displayed in the list on the right of the **Resource Management** page.

Step 2 In the Resource Management navigation tree, select the parent object of the NE to be created. Then click **Create Resource**.

Step 3 On the **Select Object Type** page, select **Snmp Network Element**.

The **Configure Parameters** page is displayed.

Step 4 Set NE parameters.

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

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.

Prerequisite

An NE is added to eSight.

Context

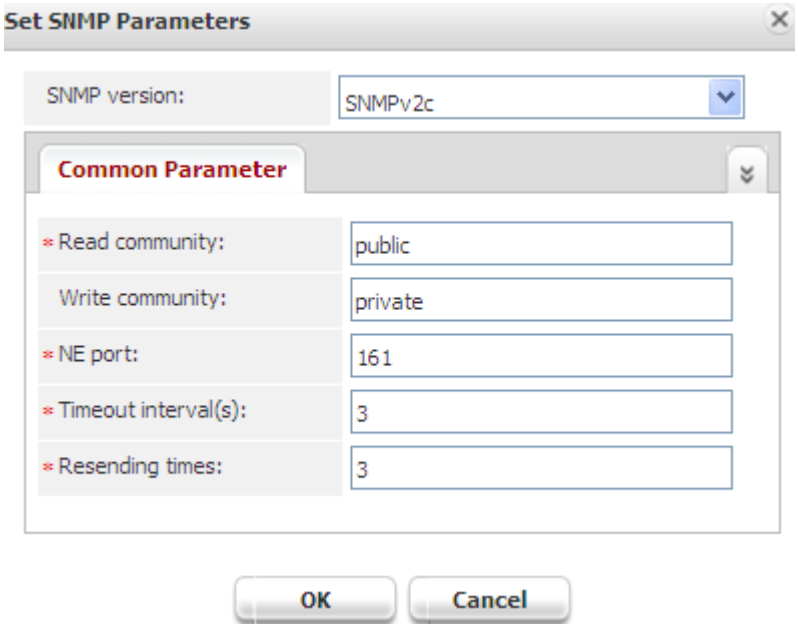
eSight accesses a managed NE over SNMP. When you manually create an SNMP NE or an SNMP NE is automatically created, eSight adapts a specified NE by using the default SNMP profile to determine the SNMP parameters supported by the managed NE. If adaptation is successful, the default profile is the SNMP 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.
- **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.
- **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.
- **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.

Step 4 Click **OK**.

----End

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.

Prerequisite

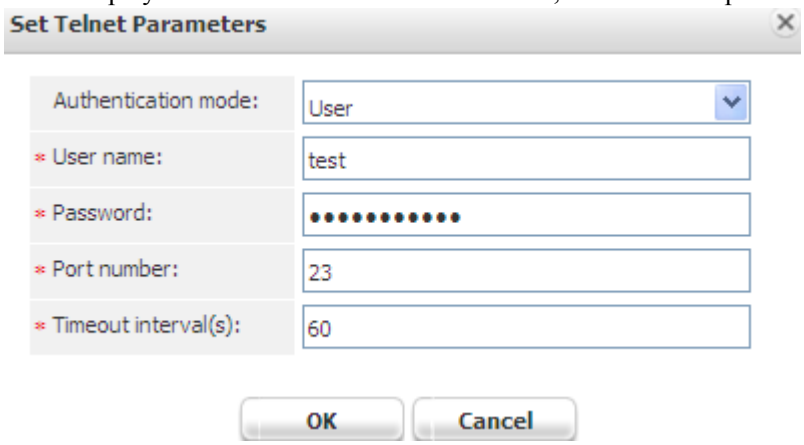
An NE is added to eSight.

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

1.9 Initialize the NEs By Using the SCT

This topic describes how to deploy scripts to configure NEs in batches.

Prerequisite

The scripts that have been successfully verified must exist. For details about how to verify a script, see **9.4.5 Verifying a Script**.

Context

Scripts for multiple NEs can be selected and deployed in batches.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 In the **NE List** navigation tree, right-click the script to be deployed or the NE where the script is to be deployed and choose **Deploy Script** from the shortcut menu.

Step 4 In the **Deploy Script** dialog box, select a script in the **Select Script** area. The details about the script are displayed in the **Preview** area.

If some command lines or parameters need to be modified, modify them and click **Save** before deploying the script.

Step 5 Click **Deploy**.

The scripts for multiple NEs can be selected for deployment.

Step 6 In the confirmation dialog box, click **OK**.

Step 7 The progress of deploying the scripts is displayed on the **Deployment** tab page.

If a script fails to be deployed, perform any of the following operations as needed:

- Retry: The system re-executes the abnormal command.
- Ignore: The system ignores the abnormal command and continues to execute the next command.
- Stop: The system stops deploying scripts.

Step 8 Click **Save Configurations** to save the configurations to NEs.

Step 9 Click **Close**.

----End

1.10 Back Up Device Configuration Files

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

Prerequisite

eSight communicates with NEs normally.

The FTP service is configured and started. For details on how to configure the FTP service, see **10.2 Setting FTP Parameters**.

For the user-defined device, the Telnet parameters on eSight and the NE are set to be the same.

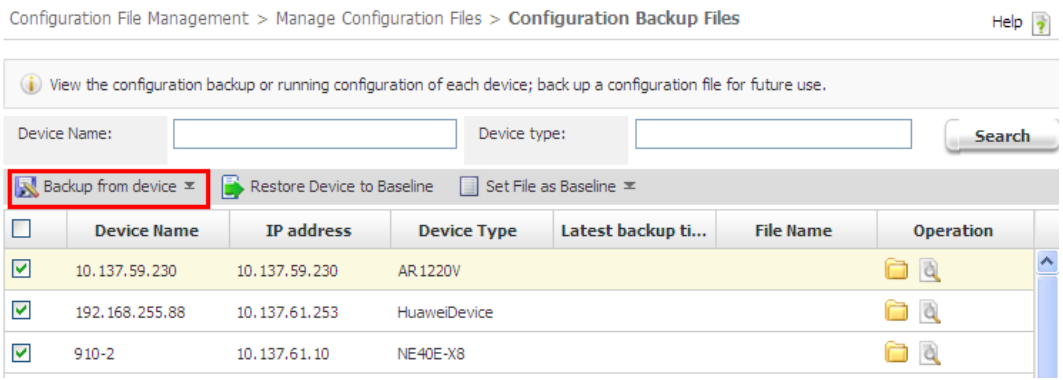
SNMP write permission is set.

Procedure

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

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

Step 3 Select a device and click **Backup from device**.



----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.

1.11 Add a Lower-layer NMS

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

Prerequisite

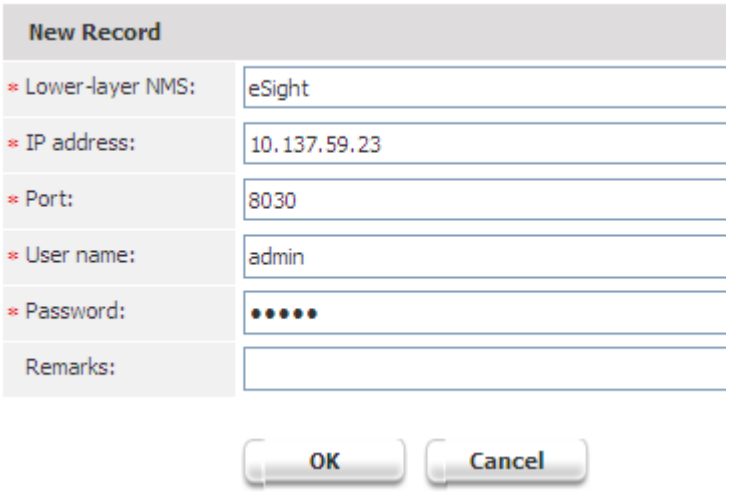
The lower-layer NMS runs properly.

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**, **User name**, and **Password** in the window that is displayed.



Step 3 Click **OK**.

----End

2 Security Management

About This Chapter

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

2.1 Introduction to Security Management

Security management provides the functions of managing user rights and eSight security policies. With these functions, you can set users, user roles, and access control policies.

2.1.1 Security Management

User management is an important component of the eSight security policies. The security mechanism is achieved by user authorization, access control, and user monitoring.

User Authorization

The user with a valid identity can access or operate the resources of the eSight only after the user is authorized.

User authorization involves allocating the operation rights of the eSight to users. Planning roles, object sets, and operation sets before authorization will improve the authorization efficiency. The user **admin** needs to grant rights to new users by creating roles.

Access Control

Access control policies prevent unauthorized users from accessing the network resources. Access control policies are classified into **Login Time Control Policy** and **Login IP Address Control Policy**.

Security Monitoring

Security monitoring involves monitoring user access activities and ensuring that the user behavior falls within security policies.

2.1.2 Security Concepts

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 2-1 Security concepts

Concept	Description
User	The user name and user password are uniquely mapped to the corresponding operation management rights. The default super administrator is **admin**, who can manage all devices and possesses all the operation rights of the eSight.

Concept	Description
Role	A role defines a set of users. Also, a role is a set of permissions that provide a user with the ability to perform a predefined set of functions. Managing user rights based on roles makes rights management more effective. The default super administrator role is **Administrators**.
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.
Login 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.

2.1.3 Default Operation Rights of User Roles

eSight describes the default operation rights of user roles.

Role	Description
Administrators	Have all operation rights.
Security	Have the rights to create and maintain a role or a user, and have the right to manage online users.
Operator	Have the rights to configure and query features. Do not have the right of the security administrator.
Monitor	Have the right to query features.

2.2 Security Policy Settings

Security policies include **Account Policy** and **Password Policy**. You need to plan and configure security policies during installation, and you can modify the configured security policies whenever required.

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. An account policy applies to all users after it is configured. Therefore, the account policy must be configured by the security administrator.

Prerequisite

You have permission to setting an account policy. The eSight provides the default account policy, and you can modify it as required.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Security Policies** > **Account Policy**.

Step 3 Set an account policy based on the policy plan.

When creating users or roles, you need to set the user names or role names based on the configured account policy.

Step 4 Click **Apply**.

----End

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 can include the user password complexity rules and password change interval. A password policy applies to all users once it is configured. Therefore, the password policy must be configured by the security administrator.

Prerequisite

You have permission to setting a password policy.

Context

- After a password policy is modified, the modification takes effect immediately for all users of the eSight. For example, if the minimum length of the user password is changed and if an online user changes the password, the new password used by the user must match the changed minimum length of the password to comply with the password policy.
- A new password policy does not affect the configured password.
- The password policy specifies the password complexity, password change interval, and character restrictions. Using the password policy prevents users from setting a very simple password or using the same password for a long time.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Security Policies** > **Password Policy**.

Step 3 Set a password policy based on the policy plan.

When creating users and roles, you need to set a password based on the configured account policy.

Step 4 Click **Apply**.

----End

2.3 Role Management

When the default role of the eSight cannot meet the user authorization requirements, you can create user-defined roles to assign the management rights of devices for users. A user-defined role is created by Administrators as required.

2.3.1 Create a Role

This topic describes how to create a role. When the default role of the eSight cannot meet the user authorization requirements, you can create user-defined roles to assign the management rights of devices for users.

Prerequisite

- You have permission to create a roles.
- You must learn about the responsibilities and default role rights of the maintenance personnel in the eSight.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Rights Assignment** > **Role**.

You can view the information about the role account.

Step 3 Click **Create**.

Step 4 Set the parameters, and then click **Next**.

When selecting users for the role, you can select the users from the list directly or enter the role name to search for its users. You can also delete the selected users from the list.

Step 5 Click **Add**, set managed objects under one or more managed domains and click **OK**.

1. In the **Managed Domains** area, select a managed domain.

   A red asterisk is displayed in the upper right corner of the managed domains, which indicates that you selected one or more managed objects under the managed domain.
2. In the area on the right, select one or more managed objects.

   The managed object that you selected will not be displayed.

Step 6 Click **Next**.

Step 7 Click **Add**, set operation objects under one or more operation groups and click **OK**.

1. In the **Operation groups** area, select a operation.

   A red asterisk is displayed in the upper right corner of the operation group, which indicates that you selected one or more operations under the operation group.
2. In the area on the right, select managed objects.

   The operation object that you selected will not be displayed.

Step 8 Click **Next**.

Step 9 Check that the configured information is correct and click **Finish**.

----End

2.3.2 Maintaining Role Information

This topic describes how to maintain role information. After a role is created, the user in role of **Administrators** can view the role information and modify the role information such as the role description as required.

Prerequisite

You have permission to maintaining role information.

Context

After a role is created, you can perform the following steps to maintain the role information.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Rights Assignment** > **Role**.

Step 3 In the **Role** window, perform any of the operations described in the following table.

Operation	Method
View	1. Select a role and click the role name. 2. View Users, Managed Objects and Operation Rights, the related information.
Modify	1. Select a role and click  in the **Operation** column. 2. Modify Users, Managed Objects and Operation Rights, the related information. 3. Click **OK**.

Operation	Method
Delete	1. Select a role and click  in the **Operation** column. 2. Confirm the system message. **NOTE** The default system roles cannot be deleted.

----End

2.3.3 Setting a User-Defined Managed Domain

This topic describes how to set a user-defined managed domain.

Context

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

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Advanced** > **User-Defined Managed Domains**.

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

Operation	Method
Create a user-defined managed domain.	1. Click **Create**. 2. Set the parameters. Select members from user-defined managed domains: Click **Add**, select one or more managed objects and click **OK**. 3. Click **OK**.
Modify the information of a user-defined managed domain.	1. Select a managed domain, click  in the **Operation** column of the managed domain list. 2. Modify the related information. Select members from user-defined managed domains: ● Click **Add**, select one or more managed objects and click **OK**. ● select one or more managed objects and click **Delete**. 3. Click **OK**.

Operation	Method
Delete a user-defined managed domain.	1. Select a managed domain, click  in the **Operation** column of the managed domain list. 2. Confirm the system message.

----End

2.4 User Management

User management involves creating the user accounts of the eSight for the maintenance personnel of network devices, and setting the basic information about users and their operation rights. Users are created and configured by the user **admin**.

2.4.1 Create a User

This topic describes how to create a user. You can create user accounts for the maintenance personnel of network devices, and set the basic information about users and their operation rights.

Prerequisite

- You have permission to create a user.
- You learn about the user account policy and 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 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Rights Assignment** > **User**.

Step 3 Click **Create**.

Step 4 Set the basic information about the user, and then click **Next**.

Step 5 Set a role for the user, and then click **Next**.

Step 6 Set an access control policy for the user.

Set an Access Control Policy	Operation
Set the login time control policy	1. Click **Create**. 2. In the **Create Login Time Control Policy** window, set a login time range. 3. Click **OK**. If more than one time policies are defined, you can select only one time policy.
Set a range of IP addresses you access	1. Click **Create**. 2. In the **Create Client IP Address Control Policy** window, set an IP address segment. 3. Select an IP address segment and click **OK**. You can set one or more IP address ranges.

Step 7 Click **Finish**.

----End

2.4.2 Maintaining User Information

This topic describes how to view or modify the user information after a user is created.

Prerequisite

You have permission to maintaining user information.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Rights Assignment** > **User**.

Step 3 In the **User** window, perform the following operations described in the following table.

Operation	Method
View	1. Select a user and click the user name. 2. View the related information.
Modify	1. Select a user and click  in the **Operation** column. 2. Modify the related information. 3. Click **OK**.

Operation	Method
Reset password	1. Select a user and click  in the **Operation** column. 2. Modify the password. 3. Click **OK**. **NOTE** The password of the default system user **admin** cannot be reset.
Delete	1. Select a user and click  in the **Operation** column. 2. Confirm the system message. **NOTE** The default system user **admin** and the current user cannot be deleted.
Enabled/Disabled	1. Click  to enable or disable the account of a user. 2. The **Status** column displays the status of user accounts.

----End

2.5 User Access Control

You can set an access control list (ACL) for a user to allow the user to log in to the server by using a specified IP address within the specified period of time. An ACL must be configured by the user **admin**.

2.5.1 Setting a Login Time Control Policy

This topic describes how to set a login time control policy. The login time control policy allows a user to log in to the server within the specified period of time. A login time control policy must be configured by the user **admin**.

Prerequisite

You have permission to setting a login time control policy.

Context

The default policy allows you to log in at any time.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Access Control Policies** > **Login Time Control Policy**.

Step 3 In the **Login Time Control Policy** window, view the policy information. The following table lists the tasks that you can perform for the login time control policy.

Set a Login Time Control Policy	Operation
Create a login time control policy.	1. Click **Create**. 2. Set the login time control policy. 3. Click **OK**.
Modify the policy.	1. In the time policy table, click  . 2. Modify the policy information. 3. Click **OK**. **NOTE** The default policy cannot be modified.
Delete the policy.	1. In the time policy table, click  . 2. Confirm the system message. **NOTE** The default policy cannot be deleted.

----End

2.5.2 Setting an IP Address Control Policy

This topic describes how to set an IP address control policy. You can set an IP address control policy to allow a user to log in to the server from the client whose IP address is within the specified IP address range. An IP address control policy takes effect for all users after it is configured. An IP address control policy must be configured by the user administrators.

Prerequisite

You have permission to setting an IP address control policy.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Access Control Policies** > **Client IP Address Control Policy**.

Step 3 In the **Login IP Address Control Policy** window, view the system access information. The following table shows the operations that you can do for setting system access information.

Set System Access Information	Operation
Create an IP address control policy.	1. Click **Create**. 2. Set the parameters. 3. Click **OK**.
Modify the policy.	1. In the IP address control list, click  . 2. Modify the policy information. 3. Click **OK**.
Delete the policy.	1. In the IP address control list, click  . 2. Confirm the system message.

----End

2.6 Security Monitoring

The user with Administrators role rights can monitor eSight user sessions and operations, force eSight users to exit, and unlock eSight users.

2.6.1 Monitoring User Sessions

security administrator, By monitoring the user sessions.

Prerequisite

- 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 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Security Monitoring** > **User Session Monitoring**.

Step 3 Click **Refresh**.

Step 4 View online user sessions.

----End

2.6.2 Forcing a User to Log Out

This topic describes how to force a user to log out. The user who possesses the rights of the account administrator group can force the corresponding users to log out when some dangerous operations or invalid sessions are detected during the monitoring or session.

Prerequisite

- Only the security administrator has permission to force users to log out. If you force a user to quit, only the user corresponding to a session is logged out forcibly.
- The logged-in users cannot force themselves to log out.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Security Monitoring** > **User Session Monitoring**.

Step 3 On the row of the user to be logged out of the system, click **Logout**.

Step 4 Confirm the system message.

----End

2.7 Example of Creating User Accounts and Granting Rights

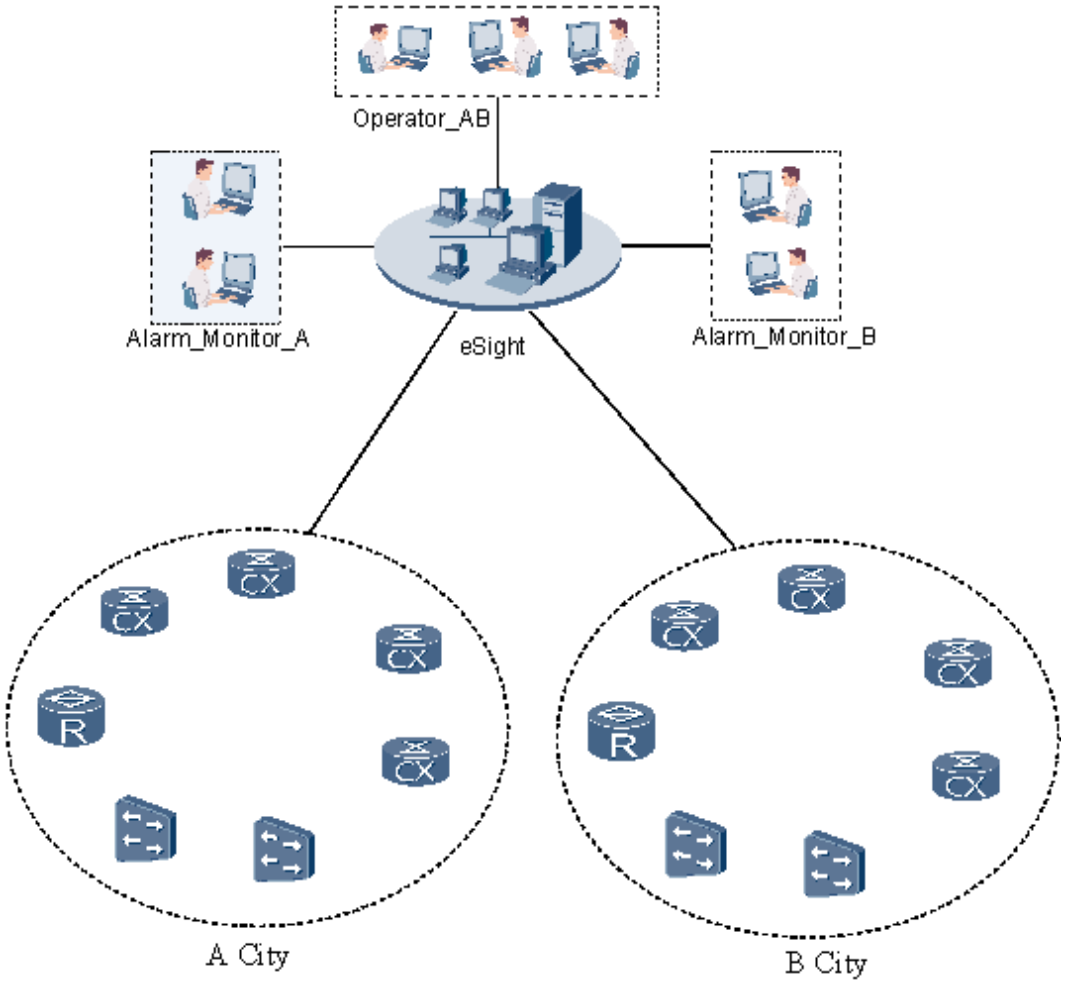
This topic describes how to create user accounts and grant rights in the scenario of management by role and domain.

Application Scenario

NEs at a site are monitored and managed by eSight in a centralized mode. NEs at the site belong to subnets of city A and city B based on the location, and are monitored and maintained by different personnel. To allow different personnel to monitor and maintain the NEs using eSight, grant proper eSight user accounts and rights to the matching personnel.

Figure 2-1 shows the network of the application scenario.

Figure 2-1 Network in the scenario of management by role and domain



Data Plan

Create two subnets based on the location, one for city A and the other for city B.

Create the following roles based on the role responsibility.

Table 2-2 Role plan

Role Name	Responsibility	Managed Objects	Operation Rights
Operator	Responsible for the operation and maintenance of NEs in city A and city B.	NEs in city A and city B	Default operation rights of eSight operators.

Role Name	Responsibility	Managed Objects	Operation Rights
Monitoring personnel of city A	Responsible for monitoring and maintaining alarms on NEs in city A.	NEs in city A	Browse masked alarms. Browse alarm history. Browse events.
Monitoring personnel of city B	Responsible for monitoring and maintaining alarms on NEs in city B.	NEs in city B	Browse masked alarms. Browse alarm history. Browse events.

Create the following users based on the user responsibility.

Table 2-3 User plan

User Name	Responsibility	Role
Operator_AB	Responsible for maintaining NEs in city A and city B.	Operator
Alarm_Monitor_A	Responsible for monitoring alarms on NEs in city A.	Monitoring personnel of city A
Alarm_Monitor_B	Responsible for monitoring alarms on NEs in city B.	Monitoring personnel of city B

Configuration Procedure

The procedure for creating users and granting user rights on eSight is as follows:

1. Create subnets for city A and city B.
   (1) On the main menu, choose **Resource** > **Resource Management**. Choose the parent object, and choose **Root** in the navigation tree.
   (2) Click **Create Resource**, and click **Subnet** under **Subnets and Solutions**.
   (3) Set **Subnet name** to **A City** and click **Apply**.
   (4) Refer to step **1.1** to step **1.3** to create a subnet for city B.
2. Add NEs of city A and city B to matching subnets.
   (1) Click  in the navigation tree. The **Move Node** window is displayed.
   (2) Select NEs of city A under **Source Nodes** on the left and select the **A City** subnet under **Target Nodes** on the left.
   (3) Click **OK**. NEs of city A are added to the **A City** subnet.
   (4) Refer to step **2.1** to step **2.3** to add NEs of city B to city B's subnet.
3. Create monitoring personnel for city A and city B, allocate managed objects and grant operation rights to the monitoring personnel.

(1) On the main menu, choose **System** > **Security Management**. In the navigation tree, choose **Rights Assignment** > **Role**.

(2) Click **Create**, set **Role Name** to ***monitoring personnel of city A***, and click **Next**.

(3) Click **Add**, select NEs of city A in the displayed window, and click **OK**.

(4) Select all NEs of city A and click **Next**.

(5) Click **Add**, refer to to select matching operation rights in the displayed window, and click **OK**.

(6) Select matching operation rights and click **Next**.

(7) Click **Finish**. The role is created.

(8) Refer to step **3.1** to step **3.7** to create monitoring personnel for city B.

NOTE

The **Operator** role is a default role on eSight, whose default managed objects are all NEs on a network and operation rights are granted by default. Therefore, the operator role does not need to be created.

4. Create the **Operator_AB**, **Alarm_Monitor_A**, and **Alarm_Monitor_B** users and set roles for these users. Then each user inherits the managed objects and operation rights from the proper role.

(1) In the navigation tree, choose **Rights Assignment** > **User**.

(2) Click **Create**, set **User Name** to **Operator_AB**, and set **Password** and **Confirm Password**.

(3) Set the user role to **Operator** and click **Next**.

(4) To ensure the security of eSight, perform the following steps:

- Set different available login time based on the shifts.
- Bind IP addresses of area workstations to users.

(5) Click **Finish**.

(6) Refer to step **4.1** to step **4.5** to create the **Alarm_Monitor_A** and **Alarm_Monitor_B** users, and set their roles to monitoring personnel in city A and city B respectively.

After the preceding configurations, the **admin** user can provide these accounts to proper personnel.

3 Resource Management

About This Chapter

eSight provides the functions of uniformly querying and collecting statistics on resources on the network. This helps support service plans and capacity expansion plans of customers.

3.1 Resource Management

You can manage resources in the eSight.

3.1.1 Accessing a Resource

This topic describes the methods of accessing a resource. When one or multiple resources will be managed or monitored on the eSight system, you perform corresponding operations.

3.1.1.1 Creating a Subnet

This topic describes how to create 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.

Context

- You can create subnets under a subnet.
- NEs can be moved to a new subnet through  .
- A subnet consists of a maximum of 10 layers.
- A subnet supports a maximum of 500 NEs.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

Step 2 In the Resource Management navigation tree, select the parent object of the subnet to be created. Then click **Create Resource**.

Step 3 On the **Select Object Type** page, select a subnet type under **Subnets and Solutions**.
The **Configure Parameters** page is displayed.

Step 4 Set subnet parameters.

Step 5 Click **OK**.

NOTE

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

- If the subnet is created successfully, the subnet is displayed on the **Subnets** tab page.
- If the subnet cannot be created, the system prompts the reason for the failure. Click **OK** to set the parameters again.

----End

3.1.1.2 Creating an NE

NEs refer to various types of devices managed by the eSight. The eSight can communicate with the created NEs and manage them. In the system, each type of NE is represented by an icon. NEs described in this topic are actual devices.

?.1. Creating an NE Manually

This topic describes how to create an NE manually. If you want a few different types of NEs to access the eSight, you need to create these NEs one by one.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

The accessed NEs are displayed in the list on the right of the **Resource Management** page.

Step 2 In the Resource Management navigation tree, select the parent object of the NE to be created. Then click **Create Resource**.

Step 3 On the **Select Object Type** page, select **Snmp Network Element**.

The **Configure Parameters** page is displayed.

Step 4 Set NE parameters.

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

?.2. Importing NEs Manually in Batches

This topic describes how to 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.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

Step 2 Click **Batch Import**.

Step 3 Click **Import Hosts and Network Devices**.

Step 4 Click  next to **Template to download** to 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.

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.

----End

?.3. NE Auto-Discovery

This topic describes the NE auto-discovery function. 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.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

Step 2 Click **Auto Discovery**.

Step 3 Click **Network Segment Discovery**.

Step 4 Set network segment discovery parameters and SNMP parameters.

For convenience, you can use the parameters in the saved SNMP 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 **Step 7** is skipped.
- If **Add the discovered objects automatically to the NMS** is not selected, you need to execute the step **Step 7** to add the discovered NEs.

Step 6 Click **Discover**.

The discovered NEs and execution result 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 list.

----End

3.1.2 Managing Resource Information

This topic describes the resource information management functions, including viewing and modifying information about accessed resources. You can delete unnecessary NEs or subnets.

3.1.2.1 Viewing Resource Information

This topic describes how to view resource information including the basic information and protocol information.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

The managed objects are displayed in the list on the right of the **Resource Management** page.

Step 2 **Optional:** Select the search type from **Search by**, set search criteria in **Search criteria**, and click **Search** to search for resources.

Step 3 Click the name of a resource. The information about the resource is displayed.

----End

3.1.2.2 Modifying Resource Information

This topic describes how to modify the attributes about a resource, such as the resource name.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

The managed objects are displayed in the list on the right of the **Resource Management** page.

Step 2 Click  correspond to the target resource.

Step 3 Modify the parameters of the corresponding resource.

Step 4 Click **OK**.

----End

3.1.2.3 Change Devices Frame

When the positions of devices change, you need to adjust the corresponding positions.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

The managed objects are displayed in the list on the right of the **Resource Management** page.

Step 2 On the **Add Monitoring View** page that is displayed, set **View name**, and select managed objects in the **Managed Object** pane. The matching counter instances are displayed in the **Indicator Instances** pane.

Step 3 On the **Add Monitoring View** page that is displayed, Click  , On the **Target Nodes**, adjust the corresponding positions.

Step 4 Click **OK**.

----End

3.1.2.4 Deleting an NE

This topic describes how to delete an NE.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

The managed objects are displayed in the list on the right of the **Resource Management** page.

Step 2 Delete target NEs from the managed object list.

- To delete one target NE, click  in the row where the NE is located.
- To delete multiple target NEs, select them and click **Batch Delete**.

Step 3 In the displayed **Confirm** dialog box, click **Yes**.

The NE is deleted from the list.

----End

3.1.2.5 Deleting a Subnet

This topic describes how to delete a subnet that is no longer managed by the eSight.

Procedure

Step 1 Choose **Resource** > **Resource Management**.

Step 2 Delete target subnets from the managed object list.

- To delete one target subnet, click  in the row where the subnet is located.
- To delete multiple target subnets, select them and click **Batch Delete**.

Step 3 In the displayed **Confirm** dialog box, click **Yes**.

The subnet is deleted from the list.

----End

3.2 Topology Management

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

3.2.1 Familiarizing Yourself with Topology Management

Familiarizing yourself with topology management helps you perform operations related to topology management.

3.2.1.1 Topology Management Functions

This topic describes the topology management functions of the eSight. An understanding of these functions helps you efficiently plan topology and perform operations.

The functions are as follows:

- Displays topology views. You can create topology views as required.
- Identifies different topology objects with different icons, and identifies the status (such as the connection status) of topology objects with small icons.
- Adds or deletes the virtual NEs and links in topology views.
- Modify the position of the NEs and subnets in topology views.
- Displays status of managed objects, such as faulty NEs and connection status of NEs.
- Queries or browses NE alarms using topology views.
- Filters the displayed topology objects based on user permission.
- Expands and collapses the topology navigation tree including expanding all objects and collapsing all objects.
- Sets the topology background. The positions of the icons on the topology background map to the positions of NE nodes.
- Zooms in and zooms out on the topology view, zooms in on an area, restores the topology view to the initial size, and fits the topology view into the screen. These functions help you view the network topology.
- Searches topology objects in the global or partial topology view. This function helps you locate topology objects.
- Supports other functions such as aerial view, printing, and exporting. This function helps you manage the topology view.

3.2.1.2 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.

Subnets

To facilitate management, a large network is divided into several subnets according to a specific rule (for example, by region) in the network management system (NMS). These small networks are called subnets in the eSight.

Network Element

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 including the router, switch, and AR series.
- Virtual NEs: The NEs that cannot be managed by the eSight can be created as virtual NEs. Virtual NEs can be used to create the network topology, and help you in understanding the entire communication network.

Link

Links indicate the connections between NEs in the topology view. The NEs are classified into physical links and virtual links.

- Physical links: Communication between two physical NEs. You can create physical NEs on eSight and allow eSight to discover them automatically.
- 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.

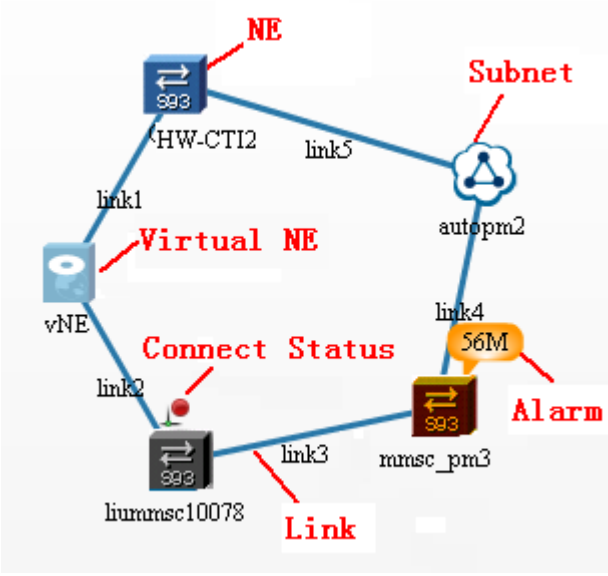
3.2.1.3 Topology Legend

Different icons represent subnets, NEs, links, and their status in the eSight. In this topic, a topology legend is provided.

Topology View

The topology view shows objects and their status.

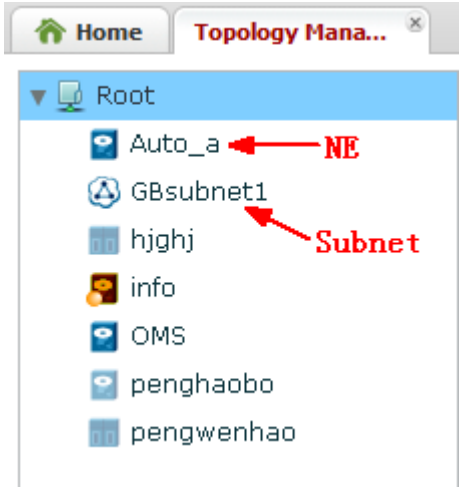
Figure 3-1 Topology view



Topology Tree Legend

A topology view includes subnets and NEs. Links are not displayed in the topology navigation tree.

Figure 3-2 Topology tree legend



3.2.2 Creating a Topology View

The topology view indicates the relationships between topology objects. The NEs and subnets in the topology view are topology objects.

3.2.2.1 Creating Virtual NEs

Virtual NEs are NEs that cannot be managed by the eSight in the entire network. Adding virtual NEs to the topology view helps you understand the entire network.

Context

Virtual NEs cannot be managed.

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 Click  on the toolbar, and click the topology view where a virtual NE is created.

NOTE

You can click  again to cancel the operation of creating a virtual NE.

Step 3 In the displayed **Create Virtual NE** dialog box, set related parameters.

Step 4 Click **OK**.

The created virtual NE is displayed in the topology view.

----End

3.2.2.2 Creating Links

Links indicate physical or logical connections between topology objects. You can create links between any topology objects as required, which indicates the relationships between topology objects.

Context

- Links are displayed in the topology view only.
- Multiple links can be created between two topology objects.
- You can create only links between NEs or subnet rather than links.

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 On the toolbar, click  to create a virtual link.

NOTE

You can click  again or click a blank in topology view to cancel the operation of creating a virtual link.

Step 3 In the topology view, select a start NE and a target NE.

A line is displayed between the two topology objects.

Step 4 In the displayed **Enter Link Name** dialog box, enter a link name.

Step 5 Click **OK**.

A link is created successfully.

----End

3.2.2.3 Adjusting the Positions of NEs

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

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 Adjust the position of an NE in the topology view.

- Move a single NE: In the topology view, click the NE, and drag it to a specified position.
- Move multiple NEs: In the topology 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

3.2.2.4 Adjusting the Positions of Subnets

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

Procedure

Step 1 Choose **Resource** > **Topology Management**.
The **Topology Management** page is displayed.

Step 2 In the topology view, click a subnet, and drag it to the required position.

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

----End

3.2.3 Managing Topology Objects

After creating a topology view, you can manage the topology objects as required.

3.2.3.1 Deleting links

When the network topology changes, you can delete unused links from the topology view.

Procedure

Step 1 Choose **Resource** > **Topology Management**.
The **Topology Management** page is displayed.

Step 2 In the topology view, select a virtual link, click  , and select **Delete Virtual Link**.
The selected link is deleted from the topology view.

----End

3.2.3.2 Deleting Virtual NEs

When the network topology changes, you can delete unused virtual NEs from the topology view.

Procedure

Step 1 Choose **Resource** > **Topology Management**.
The **Topology Management** page is displayed.

Step 2 In the topology view, select a virtual NE, click  , and select **Delete Virtual NE**.
The selected virtual NE is deleted from the topology view.

----End

3.2.3.3 Searching 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**.

The **Topology Management** page is displayed.

Step 2 Set search criteria in front of  .

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

Step 3 Click  .

The system queries the topology objects based on the specified conditions and displays the query results in the **Search Result** dialog.

Step 4 Select a topology object in the **Search Result** dialog, quickly locates the object in the topology view .

----End

3.2.3.4 Setting the Topology Background

You can set the topology background for the NE layout to understand the NE positions.

Context

When you import a background image, the image format can be one of the following:

- *.jpg
- *.jpeg
- *.gif
- *.png
- *.JPG
- *.JPEG
- *.GIF
- *.PNG

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 On the topology toolbar, click  .

Step 3 In the **Set Background** dialog box, choose **Show background image**, and then click  to import the image.

NOTE

If you do not displayed the background image in the topology view, please select **Do not display the background image**.

Step 4 Click **OK**.

The image is displayed as the topology background.

----End

3.2.3.5 Zooming In or Out on the Topology View

You can zoom in to or zoom out of the topology view.

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 You can zoom out on the topology view in the following ways:

- Click  to zoom in to the topology view.
- Click  to zoom out of the topology view.
- Click  to reset the topology view.

----End

3.2.3.6 Saving NE Positions in the Topology View

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

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 Modify the NE positions in the topology view.

Step 3 Click  to save the positions in the topology view.

----End

3.2.3.7 Arranging Topology Objects in the Topology View

You can arrange the topology objects in the topology view as required.

Context

- If you select some topology objects, only 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

Procedure

Step 1 Choose **Resource** > **Topology Management**.
The **Topology Management** page is displayed.

Step 2 In the topology view, select the topology object to be arranged. Click  to select a layout.
The topology objects in the topology view are arranged in the selected layout.

Step 3 Click  to save the new positions.

----End

3.2.3.8 Viewing the Topology View in Full Screen or Aerial View

You can view the topology in full screen or aerial view.

Context

The resolution is not always 1024x768. You can set it as required.

Procedure

Step 1 Choose **Resource** > **Topology Management**.
The **Topology Management** page is displayed.

Step 2 Click  in the lower right corner of the **Topology Management** page.
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 Click  to close the aerial view.

Step 5 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

3.2.3.9 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.

Context

The computer resolution must be 1024 x 768.

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 Choose  > **Show Legends**.

Topology legends define the meanings of topology object colors or status in the topology view.

----End

3.2.3.10 Setting a Device Label

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

Context

The computer resolution must be 1024 x 768.

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 Choose  > **Device Label**.

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

Step 4 Click **OK**.

If you do not select any of the device name, IP address, and system name, the device name is displayed by default.

----End

3.2.3.11 Printing the Topology View

You can print the topology view.

Procedure

Step 1 Choose **Resource** > **Topology Management**.

The **Topology Management** page is displayed.

Step 2 On the toolbar, click  .

Step 3 Set the print parameters.

Step 4 Click **OK**.

----End

3.2.3.12 Exporting the Topology View

You can export the topology view to a local PC.

Procedure

Step 1 Choose **Resource** > **Topology Management**.
The **Topology Management** page is displayed.

Step 2 On the toolbar, click  .

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

Step 4 Click **Save**.
The topology view is saved as a file in the specified path.

----End

3.3 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 3-1** describes operations that can be performed on each type of resources.

Table 3-1 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.

3.4 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.

Prerequisite

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 **Start**. The link discovered by eSight is displayed on the right of the window. Click **OK**.

Table 3-2 Commands for discovering the LLDP link

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.

NOTE

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

For the LLDP link:

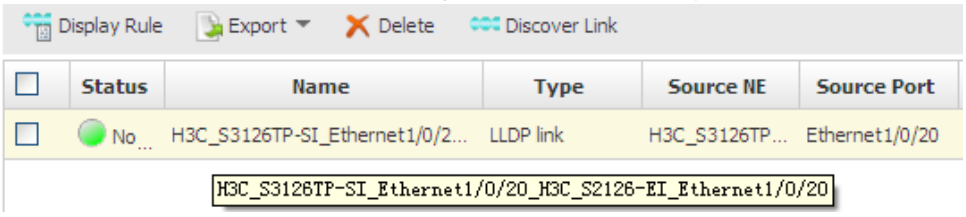
- If the commands listed in Table 3-2 are not set on an NE, set Telnet parameters on eSight and the NE, and then select **Deliver commands**. After the LLDP link is discovered, you can click **Delivery result** to view the command delivery and execution result.
- If the commands listed in Table 3-2 are 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:** Click **Display Rule** to set the display rule of a link.

1. In **Naming Rule**, set the display fields of a link name.

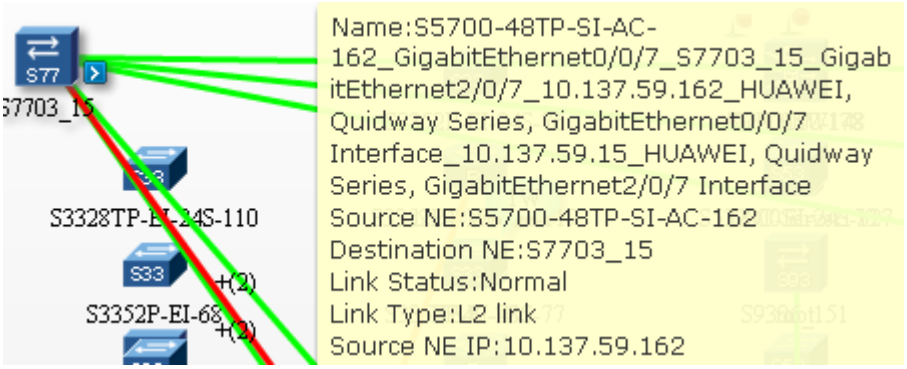
   After the link name is set, in the **Manage Link** window, verify the name under **Name**.



2. 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.



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**.

Step 6 **Optional:** Select a link to be deleted and click **Delete**. 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.

----End

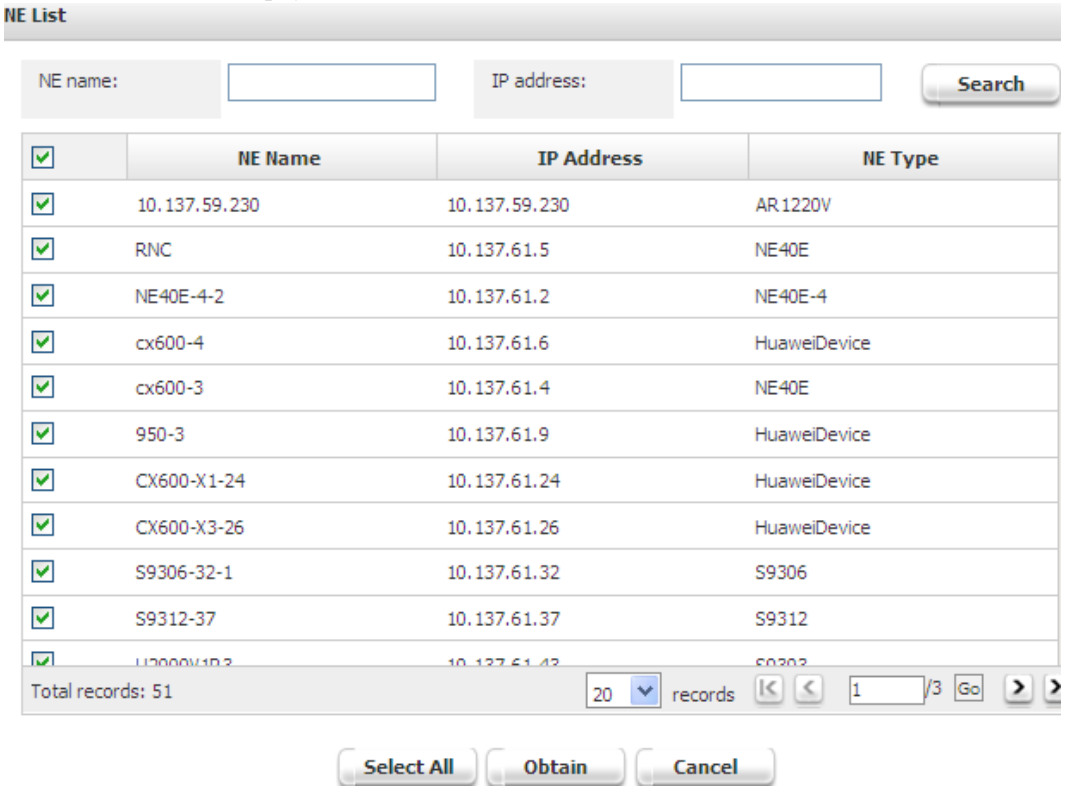
3.5 Electronic Labels Management

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.



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

4 Fault Management

About This Chapter

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

NOTE

To manage NEs' alarms on eSight, you must set the trap packets' destination IP address as the eSight server's IP address.

4.1 Learning About Fault Management

This topic describes the fault management functions and related concepts, such as **Severity**, **Alarm Status**, **Alarm**, and **Events**, helping you to perform fault management properly.

4.1.1 Fault Management Functions

The fault management functions include collecting alarm statistics, displaying alarms, acknowledging alarms, and clearing alarms.

Collecting Alarm Statistics and Displaying Alarms

The eSight receives the alarms generated by the managed NE in real time, collects statistics, and displays alarms in the following three ways.

Table 4-1 Collecting Alarm Statistics and Displaying Alarms

Collecting Alarm Statistics and Displaying Alarms	Description
Alarm board	The alarm board collects statistics of alarms in the alarm list. It also displays alarms by their severity and status, which shows the status of the entire network. The alarm board can act as a monitoring board.
Alarm bar chart	The alarm bar chart displays alarms in charts and numbers based on their severity and status, which presents an overall view of the entire network status. The alarm bar chart can act as a monitoring board.
Alarm query	You can browse current alarms, query historical alarms, and query events in the eSight. The alarm list displays only the alarms to be concerned and handled.

Acknowledging Alarms

You can acknowledge the alarms that have been handled so that these alarms do not need concern. If you want to concern about the handled alarms, you can unacknowledge the alarms and take proper intervention.

Clearing Alarms

You can manually clear the alarms that cannot be cleared automatically or do not exist on the eSight.

Masking Alarms

You can set the rules to mask the alarms. The alarms masked by the eSight are displayed in the list of masked alarms.

Sending Remote Alarm Notifications

When an alarm is generated, the eSight notifies the maintenance personnel by means of Email or short message service (SMS) to help them learn about the alarm information and take proper measures.

4.1.2 Alarm Severities

The alarms are classified: **Critical**, **Major**, **Minor**, and **Warning**. You can take different measures for different severities of alarms.

Table 4-2 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 a problem of relatively low severity that should not impede use of the resource.
Warning	An alarm severity that indicates a condition that can potentially cause a problem with the resource.

4.1.3 Alarm Status

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

Table 4-3 Alarm status

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

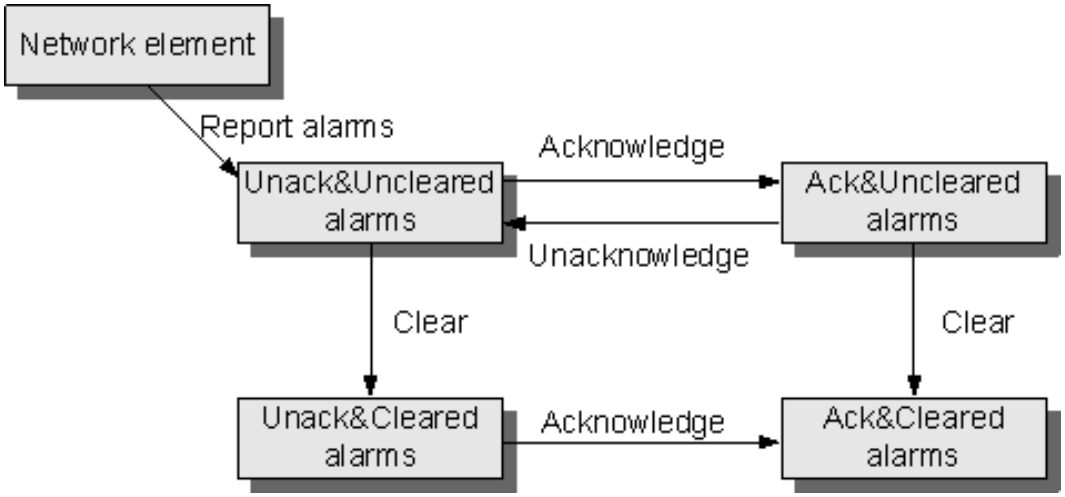
Status Change

Table 4-4 Status Change

Status Change Type	Description
Clearance status change	If the condition that generated the alarm disappears, and the NE or the eSight server becomes normal, the NE or the eSight 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.

The following figure shows the relationship between alarm status.

Figure 4-1 Alarm status relationship



4.1.4 Alarms and Events

This topic describes the similarities and differences between alarms and events in the eSight.

Similarities Between Alarms and Events

Both alarms and events are the presence of anything that takes place on the managed object detected by the eSight.

Differences Between Alarms and Events

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

An event is anything that takes place on the managed object.

The differences are:

- The alarm is a special event. When an fault or exception occurs in the eSight, you must 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.

4.2 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.

4.2.1 Monitoring Alarms in the Topology View

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

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 On the main menu, choose **Resource** > **Topology Management**.

Step 2 In the **Topology Management** window, view the alarm state and NE position based on the displayed tip.

- The tip includes the alarm clearance state, severity, and number of alarms of the highest severity.
- 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.

----End

4.2.2 Monitoring Alarms in the NE Monitoring List

You can view the managed object names, types, alarm severities, and connection status in the monitoring list of the eSight to learn about the running status of the NEs and troubleshoot the fault at the earliest.

Procedure

Step 1 On the main menu, choose **Fault** > **Current Alarms**.

Step 2 Select an alarm and click  .

NOTE

The **Topology Management** window displays the information about the managed NEs in the eSight.

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.

----End

Follow-up Procedure

The **Current Alarms** window displays all alarms generated by this NE. You can acknowledge and clear the alarms.

4.2.3 Monitoring Alarms on the Alarm Board

You can view the alarm board to learn about the number of different severities of alarms or learn about the alarm status from the alarm board or alarm sound.

Context

The alarm board 

is displayed in the upper right corner, and displays the critical alarms, major alarms, minor alarms, warning alarms, clear alarms, and all alarms respectively 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 change with the display times on the alarm board.

4.2.4 Querying Alarms

You can browse current alarms, query the masked alarms, and query historical alarms in the eSight.

4.2.4.1 Browsing Current Alarms

You can set the filter criteria in the current alarm list to view the alarms to be concerned and handled.

Context

- If a new alarm is reported and the alarm meets the merging rule, the alarm can be merged to the alarm list, and the number of alarms increases. The merged alarms are displayed in the current alarm list.

  Default alarm merging rule: If the alarms have the same alarm source, location information, and alarm ID, the alarms are merged to one record.
- In the **Current Alarms** window, you can view the information about each alarm.
- If the current filter criteria are modified, the system searches for alarms based on the modified filter criteria.
- When you browse alarms, you can click to customize the columns to be displayed.

Procedure

Step 1 On the main menu, choose **Fault** > **Current Alarms**.

Step 2 On the **Filter criteria** drop-down menu, select a criterion to query. You can also customize the filter criteria as required. See **4.2.4.5 Customizing Alarm Filter Criteria**.

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

Table 4-5 Operations in Current Alarms window

Operation Name	Operation Method	Description
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. ● 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 the drop-down menu when the window is locked, and click **Search**.	-

Operation Name	Operation Method	Description
Acknowledge	Select one or more alarms and click **Acknowledge**.	● 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**.	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. Select an alarm. Then click in the **Operation** column and choose Shield Alarms**.** 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 mask rule for a performance alarm or clear alarm.
Locate to Topo	Select an alarm and click  .	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 Occurrences**.	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

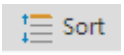
4.2.4.2 Querying Historical Alarms

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

Context

The alarms that are acknowledged and cleared are displayed in the historical alarm list.

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 On the main menu, choose **Fault** > **Historical Alarms**.

Step 2 Set the search information in the search bar and click **Search**.

- **Subnet or NE**: click  . In the **Select Subnet or NE** dialog box, select the required Subnet or NE.

  NOTE

  If you want to re-select alarm sources, click  , The selected alarm sources are cleared.
- **Alarm name**: enter the name of a historical alarm.
- **Time period**: select a start and end dates.
- **Severity**: select the severity of a historical alarm.

Step 3 In the search results window, you can perform the following operations.

Operation Name	Operation Method
Alarm Details	Select an alarm and click **Alarm Name**. The **Alarm Details** dialog box displays the name, cause, and solution for the selected alarm.
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**. Only the historical alarms generated within the selected month are exported.

----End

4.2.4.3 Querying Events

You can query events to view the notification sent from the device to the eSight.

Context

An event is the notification of anything that takes place in the eSight reported by the device.

Procedure

Step 1 On the main menu, choose **Fault** > **Events**.

Step 2 Set the search information in the search bar and click **Search**.

Step 3 In the search results window, you can view the events found.

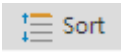
----End

4.2.4.4 Querying Masked Alarms

When you query masked alarms, you can refer to the masking rules of alarms.

Context

When you query masked alarms, you can perform the following settings:

- Click  to customize the information you want to query.
- Click 

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

Procedure

Step 1 On the main menu, choose **Fault** > **Masked Alarms**.

Step 2 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 search results window, select an alarm and click **Alarm Name**.

The **Alarm Details** dialog box displays the name, cause, and solution for the selected alarm.

----End

4.2.4.5 Customizing Alarm Filter Criteria

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

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.

Procedure

Step 1 On the main menu, choose **Fault** > **Current Alarms**.

Step 2 Choose **Filter criteria** > **Set filter criteria**.

Step 3 In the **Set Filter Criteria** dialog box, perform the following operations.

Operation Name	Operation Method
Create	1. Click **Create**. In the right area, set the name, severity, cleared status, event type, and first occurrence time. 2. Click **Save**. In the right area, a message is displayed indicating a success.
Delete	1. In the filter criteria list, select the user-defined filter criterion and click **Delete**. 2. In the **Confirm** dialog box, click **OK**.
Modify	1. In the filter criteria list, select the user-defined filter criterion. In the right area, set the name, alarm severity, cleared status, event type, and first occurrence time. 2. Click **Save**. In the right area, a dialog box is displayed, indicating a success.

Operation Name	Operation Method
Copy	1. In the **Set Filter Criteria** window, select the alarm template in the left navigation tree. 2. Click **Copy**. In the right area, set the alarm severity, cleared status, event type, and first occurrence time. 3. Click **Save**. In the right area, a message is displayed indicating a success.

----End

4.3 Handling Alarms

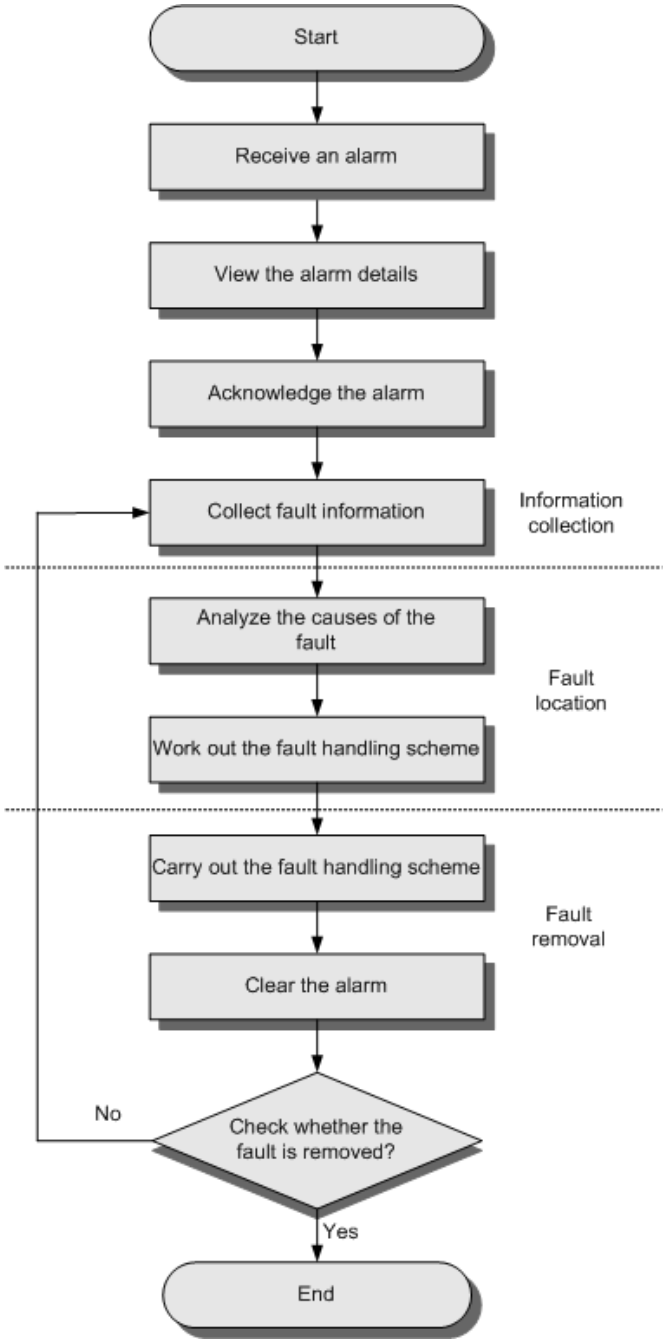
When an alarm occurs, you can handle the alarm to troubleshoot the fault. Handling alarms involves viewing alarm details, acknowledging alarms, identifying alarms, and clearing alarms.

4.3.1 Procedure for Handling Alarms

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

Flow Chart of Handling Alarms

Figure 4-2 Procedure for handling alarms



Procedure Description

Table 4-6 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.
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 in the eSight	After troubleshooting, check if the fault is rectified.

4.3.2 Viewing Alarm Details

You can view the details about current alarms, historical alarms, and masked alarms in the eSight. Alarm details include the alarm name, advice, and location information.

Parameters in the Alarm Details dialog box items

The **Alarm Details** dialog box displays the name, additional information, and solution for the selected alarm.

Table 4-7 Parameters in the Alarm Details dialog box

Parameter	Description
Alarm name	Indicates the name of an alarm. The name reflects the fault symptom of an alarm object.

Parameter	Description
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.
Times occurred	Indicates the number of occurrences of an alarm.
Alarm source	Indicates the NE where an alarm is generated.
Latest 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 serial number of the eSight user that clears an alarm. When an NE automatically clears its alarms, the value of this parameter is empty; when the eSight clears an alarm, the value of the parameter is the serial number of the eSight user that performs the clear operation.
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 SN	Indicates the serial number of a piece of equipment. The equipment SN uniquely identifies an alarm of the equipment.
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.

Parameter	Description
Clear type	Indicates the clearing type of an alarm.
Equipment alarm serial number	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.
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.

4.3.3 Acknowledging Alarms

Acknowledging an alarm indicates that the alarm has been handled and can be ignored.

Context

- If the alarm is acknowledged, **Acknowledge User** displays the user who acknowledged the alarm.
- If the alarm is unacknowledged, **Acknowledge User** displays  .

Procedure

Step 1 On the main menu, choose **Fault** > **Current Alarms**.

Step 2 Select the filter criteria to query the alarms. You can also customize the filter criteria. For details, see **4.2.4.5 Customizing Alarm Filter Criteria**.

Step 3 In the search results window, select one or more alarms and click **Acknowledge**.

Acknowledge User displays the users who acknowledges the alarms.

----End

Follow-up Procedure

If you want to acknowledge the alarm again, choose **More** > **Unacknowledge**.

4.3.4 Clearing Alarms

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.

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 On the main menu, choose **Fault** > **Current Alarms**.

Step 2 Select the filter criteria to query the alarms. You can also customize the filter criteria. For details, see **4.2.4.5 Customizing Alarm Filter Criteria**.

Step 3 In the **Current Alarms** window, select one or more alarms and click **Clear**.

The background color of the alarm is green.

----End

4.3.5 Example of Handling Alarms

This topic uses an example of over high disk usage to describe the procedure for handling alarms, helping you learn about the operations of handling alarms.

Background Information

Administrator A discovers a new alarm in the eSight.

Operation Guide

A performs the following steps according to the handling procedure. (For details about the procedure, see **4.3.1 Procedure for Handling Alarms**.)

1. Receives alarm notification

   A chooses **Fault** > **Current Alarms**. A discovers an alarm of over high disk usage.

2. Views the alarm details

   A clicks the alarm. In the **Alarm Details** dialog box, A views the alarm details.

3. Acknowledges the alarm

   According to the alarm details, it is found that the fault can be rectified and the alarm can be cleared. Therefore, A selects the alarm and clicks **Acknowledge** to acknowledge the alarm.

4. Prepares the troubleshooting scheme

A determines a troubleshooting scheme based on the suggested solution and running status of the eSight.

5. Troubleshoots the fault

   A deletes the redundant files which are not the files built in the eSight, backs up the files to other disks, and deletes the files in the original disk. The disk space of the eSight server is cleared.

6. Checks the troubleshooting result

   A chooses **Fault** > **Historical Alarms**. A finds that alarm of over high disk usage.

4.4 Managing Alarm Data

You can clean up the database by using overflow dump to avoid insufficient space.

4.4.1 Configuring Alarm Overflow Dump

The eSight provides alarm overflow dump to avoid insufficient database tablespace. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the data to a specified folder.

Context

If the tablespace usage exceeds the specified database space threshold, a data overflow occurs.

The eSight checks the alarm management tablespace usage in the database at a specific time of day. If the usage exceeds the threshold, the eSight always dumps the alarms (including historical alarms, masked cleared alarms, and events) reported within the earliest month to the specified path in order according to the reporting time of the alarms, and then deletes the dumped alarms starting with the earliest until the usage is less than the threshold. After dumping, the eSight also checks whether the total size and retention period of the files in the dump directory exceed the specified values. If they exceed the specified values, the eSight deletes the earliest dumped files until the total size and retention period become less than the specified values.

Procedure

Step 1 Choose **System** > **System Configuration**.

Step 2 In the left navigation tree, choose **Database Overflow Dump** > **Alarm Database Dump**.

Step 3 Set alarm dump parameters.

NOTE

Dump path can be an absolute path or a relative path. The relative path is relative to the OMS installation path **%ENT_ROOT%/run/dump** (on Windows). If you specify **Dump path** to **AAA**, the file is saved to **%ENT_ROOT%/run/dump/AAA**.

Step 4 Click **Apply**.

----End

4.5 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.

4.5.1 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.

Context

When you set the Email server, you need to obtain the IP address of the Simple Mail Transfer Protocol (SMTP) server and mailbox 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**: determines whether the current user has permission to send emails.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Remote Notification** > **Email Server**.

Step 3 Set the parameters.

Step 4 Click **Apply**.

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.

----End

4.5.2 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.

Context

When you set the SMS server, you need to obtain the host name, port number, protocol, 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.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Remote Notification** > **SMS Server**.

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

If you want to send long messages or status reply, click **Advanced** to select.

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

Table 4-8 Support long messages

Encoding Protocol	Support Long Messages
SMPP3_3/SMPP3_4	● 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 160 characters. If a message contains more than 160 characters, the system splits the message and sends several short messages to the recipient.
CMPP2_x/ CMPP3_x	
SGIP	

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.

----End

4.5.3 Setting Notification Templates

You can customize an alarm or event notification template. The eSight sends the alarms or events meeting the remote notification rule to users by email or SMS.

Context

- eSight sends the information that users are concerned about based on the customized notification template.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Remote Notification** > **Notification Template**.

Step 3 In the **Notification Template Settings** window, set the alarm or event notification template.

Click  , choose 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 from the **Available Alarm Fields** box. Click  to add the field to the **Selected Alarm Fields** list.

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

- Set the event notification template:

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

NOTE

- In the **Selected Alarm Fields** pane, you can enter a prefix for **Field Name** so that the alarm is added with a prefix and the SMS is sent with the prefix.
- In the **Selected Event Fields** pane, you can enter a prefix for **Field Name** so that the event is added with a prefix and the SMS is sent with the prefix.

----End

4.5.4 Setting Recipient Groups

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

Context

You can add, view, modify, and delete the recipient group.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Remote Notification** > **Notification Recipient Groups**.

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

Operation Name	Operation Method
Create a recipient group	Click **Create**. In the **Create Recipient Group** window, set the recipient group information and click **Save**. ● You can click **Create** to add a member. **Recipient**, **Phone**, and **Email** are mandatory. ● In the **Create Recipient Group** window, you can modify and delete the new recipient group.
View recipient Group	Select a user group and click **Group Name**. In the **View User Group** window, you can view the details about the user group.

Operation Name	Operation Method
Edit a recipient group and users	Select a user group and click  to modify the Group name, Description, and Recipients. For users, you can perform creating, modifying or deleting operations.
Delete a recipient group	Select a user group and click  . In the **Confirm** dialog box, click **OK**.

----End

4.5.5 Setting Notification Rules

You can set the remote alarm notification rule, including notification condition, time, and mode.

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 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Remote Notification** > **Remote Notification Rules**.

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

Operation Name	Operation Method
Create	Click **Create**. You can add a rule by means of the following: ● **By Alarm Severity**: Set **Rule name**, **Severity**, and **Notification recipient groups**. **NOTE** ● When you set the notification receiver, you can click  to add more receivers. ● In the **Group** drop-down list, you can select or add a user group. For details, see **4.5.4 Setting Recipient Groups**. ● **By Alarm**: For details, see **4.5.6 Setting Notification Rules by Alarm**.
Enable	Select one or more rules and click **Enable** to enable the rules.

Operation Name	Operation Method
Disable	Select one or more rules and click **Disable** to disable the rules.
Modify	Select a rule and click  to modify the rule.
Delete	Delete the rule information. Select a notification message and click  . In the **Confirm** dialog box, click **OK**.

----End

4.5.6 Setting Notification Rules by Alarm

You can set the alarm notification rule by selecting the alarm source, alarm, and notification user group.

Context

You must learn about information such as the subnet, alarm source, and event.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Remote Notification** > **Remote Notification Rules**.

Step 3 Click **Create** and select **By Alarm**.

Step 4 Set the **Rule name** and click **Add Alarm Sources**.

Step 5 Select the alarm source from the list and click **OK**.

1. In the **Subnets** area, select a subnet.
   - Select the **Root** node. All the alarm sources are displayed in the **Alarm Sources** area.
   - Select a subnet. All the alarm sources 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 alarm source under the subnet.
2. In the **Alarm Sources** area, select an alarm source.
   - Click **Select All/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.

Step 6 Click **Next**.

Step 7 Click **Add Alarms and Events**.

Step 8 Select an alarm and event from the alarm source, and click **OK**.

1. In the **Device Type** area, select a device type.
   - Select a device type. All the device types under the subnet are displayed in the **Alarm List** area.
   - A red asterisk is displayed in the upper right corner of **Device Type**, which indicates that you selected the alarms or events under **Device Type**.
2. In the **Alarm List** or **Event List** area, select an alarm or event.
   - Click **Select All/Clear All** to select or deselect all the alarm sources under **Alarm Sources**.
   - Select the alarms or events under multiple subnets as required. The alarms or events that you selected will not be displayed under these subnets.
   - 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.

Step 9 Click **Next**.

Step 10 Set the receiver, and click **Finish**.

----End

4.6 Setting Alarm Masking

You can set the rule for masking the alarms that are reported to the eSight but do not need to be handled.

Context

The masking rule is valid only for the alarms reported when the rule is enabled. The time segment contains **Anytime** and **Only during following periods**.

- **Anytime**: The rules in all time periods on the specified date are effective.
- **Only during following periods**: The rules in the specified time period on the specified date are effective.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Basic Settings** > **Mask Rule**.

Step 3 In the **Mask Rule** window, you can perform the following operations.

Operation Name	Operation Method
Create	Click **Create** to add a masking rule. For details, see **4.6.1 Adding Alarm Masking Rules**. **NOTE** If you add a mask rule for the reported alarms in the current alarm window, the rule will take effect for the subsequently reported alarms.

Operation Name	Operation Method
Enable	Select a rule and click **Enable** to enable the rule. If a rule is displayed as **Enabled**, the rule is enabled and the rule takes effect for the subsequently reported alarms.
Disable	Select a rule and click **Disable** to disable the rule. If a rule is displayed as **Disabled**, the rule is disabled.
Delete	Select one or more rules and click  and confirm the system prompt.
Modify	Select a rule and click  and modify the parameters.

----End

4.6.1 Adding Alarm Masking Rules

You can add and enable rules for alarm masking, and ensure that alarms that meet these rules and are received and added to the list of masked rules.

Context

The time segment contains **Anytime** and **Only during following periods**.

- **Anytime**: The rules in all time periods on the specified date are effective.
- **Only during following periods**: The rules in the specified time period on the specified date are effective.

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Basic Settings** > **Mask Rule**.

Step 3 Click **Create**.

Step 4 Set **Rule name**, **Date**, and **Time**, and click **Next**.

Step 5 Click **Add Alarm Sources**, set alarm sources and click **OK**.

1. In the **Subnets** area, select a subnet.
   - Select the **Root** node. All the alarm sources are displayed in the **Alarm Sources** area.
   - Select a subnet. All the alarm sources 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 alarm source under the subnet.
2. In the **Alarm Sources** area, select an alarm source.

- Click **Select All/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.

Step 6 Click **Next**.

Step 7 Click **Add Alarms**, set alarms and click **OK**.

1. In the **Device Type** area, select a device type.
   - Select a device type. All the device types under the subnet are displayed in the **Alarm List** area.
   - A red asterisk is displayed in the upper right corner of **Device Type**, which indicates that you selected the alarms under **Device Type**.
2. In the alarm list area on the right, select an alarm.
   - Click **Select All/Clear All** to select or deselect all the alarms.
   - 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.

Step 8 Click **Finish**.

----End

4.7 Setting 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.

Context

- By default the alarm sound is **Enable**.
- The default settings for different severities of alarms are:
  - **Critical**: **Critical.mp3**
  - **Major**: **Major.mp3**
  - **Minor**: **Minor.mp3**
  - **Warning**: **Warning.mp3**

Procedure

Step 1 On the main menu, choose **Fault** > **Alarm Settings**.

Step 2 In the navigation tree on the left, choose **Basic Settings** > **Alarm Sound**.

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

- Select **Severity** and click **Disable** to disable the alarm sound for the selected alarm.
- Select **Severity** and click **Enable** to Enable the alarm sound for the selected alarm.
- Click **Play** to listen to the alarm sound.

- Click **Operation**. In the **Set alarm sound** window, select **Alarm sound** and **Play count**, and click **Save**.

NOTE

Click **Default Setting** to restore the alarm sound to the default setting.

----End

5 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.

5.1 Basic Concepts

This topic describes the basic concepts that you must be familiar with before conducting performance management.

5.1.1 Performance Event and Performance Indicator

In the network running process, some internal and external factors may affect the transmission quality, resulting in signal attenuation, which is displayed as different performance events.

Performance Event

Different from an alarm, when a performance event is reported, the service is still running but the transmission quality has deteriorated. The deterioration is compromised temporarily by a device's built-in error correction mechanism. If the transmission quality continues to deteriorate, it may exceed the performance threshold and an threshold alarm may be generated.

By performance management, network maintenance personnel can detect performance deterioration in advance and solve the potential fault before it occurs.

Performance Indicator

Performance indicators are used to monitor resource usage, for example, CPU usage and memory usage. During performance monitoring, the Performance indicators are collected and calculated. You can set the performance threshold to specify the condition for generating an alarm and determine the alarm severity.

5.1.2 Performance Threshold

A performance alarm is generated only when the value of a Performance indicator exceeds the specified threshold.

The performance threshold specifies the requirement on devices to ensure the proper running of the network. You can check whether a device is running properly based on the performance threshold. When the value of a Performance indicator exceeds the specified threshold, the measurement object generates a Quality of Service (QoS) alarm, which must be processed. When the value of this Performance indicator is smaller than the specified threshold, the QoS alarm is cleared.

Normally when you set the performance threshold, reserve a certain performance margin for detecting potential faults in advance.

5.1.3 Latest and Historical Performance Data

Network maintenance personnel query the latest and historical performance data to analyze the network or service running status.

Latest Performance Data

Latest performance data refers to the performance data that is monitored in real time and can be browsed in the performance monitoring view. Latest performance data updates dynamically in the performance monitoring view. When browsing the latest performance data in the

performance monitoring view, you can select multiple NEs to compare their performance on a certain performance counter, or select multiple performance counters to view the overall performance about an NE.

Historical Performance Data

Historical performance data refers to the performance data that is obtained about an NE in the past period of time. The search criteria include object type, object instance, measurement unit, measurement object, and time segment. Historical performance data can be displayed in tables or graphs.

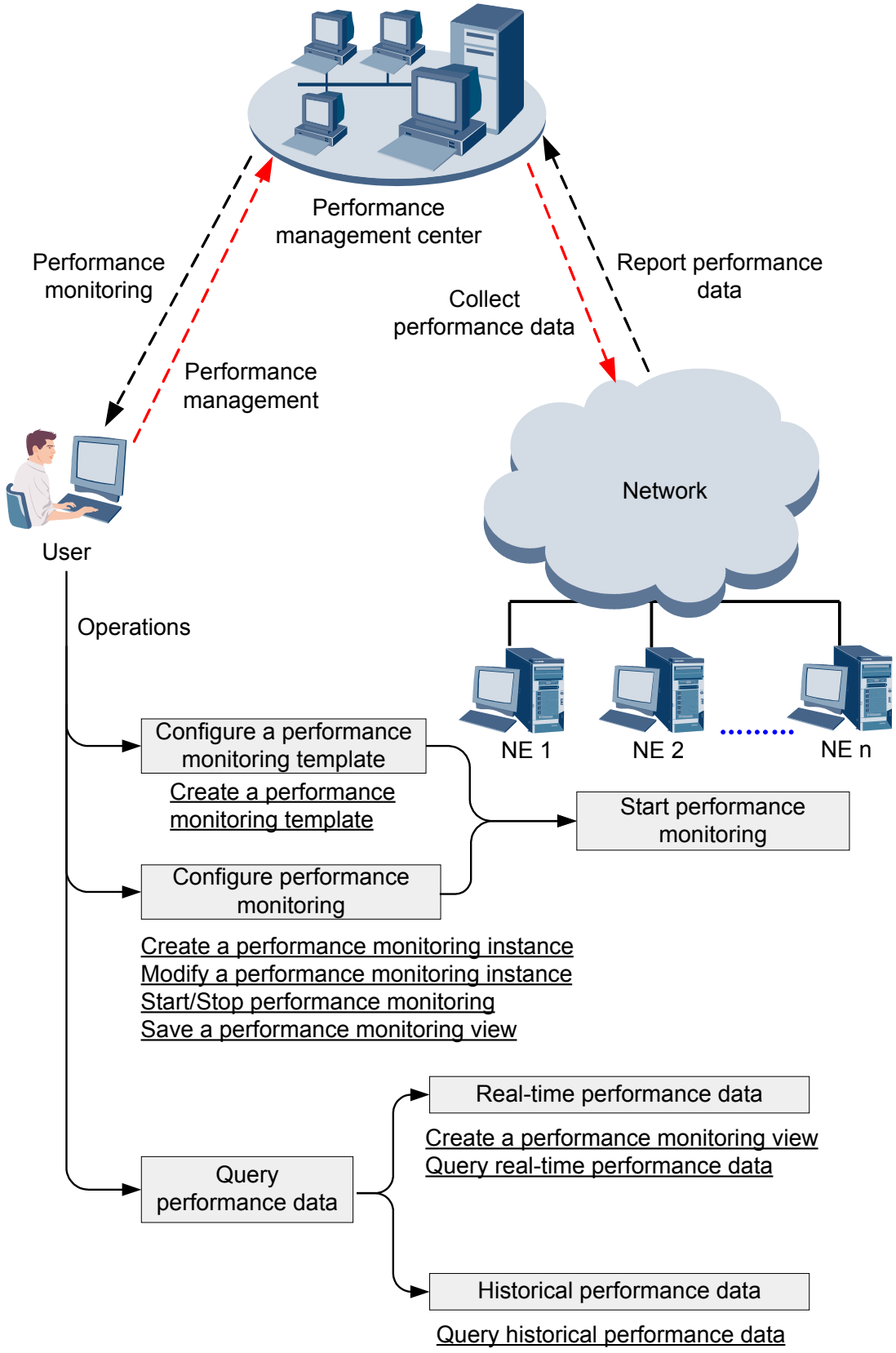
5.2 Performance Monitoring Process

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 5-1 shows the performance monitoring process. The two sides connected to the eSight are users and NEs. Users enable performance monitoring and view performance data in the eSight. NEs report performance data to the eSight.

Figure 5-1 Performance monitoring process



Process of Monitoring NE Performance on the User Side

The process of monitoring NE performance on the user side is as follows:

1. **Configure a performance monitoring template**: NEs of the same type share attributes. Users can preset monitoring parameters in a performance monitoring template. The eSight automatically delivers the template to managed NEs to provide the default performance and alarm management. Then NEs automatically execute performance monitoring tasks based on the template, collect performance data, and generate alarms.
2. **Configure performance monitoring**: Create a performance monitoring instance on a monitoring object, and enable/disable the performance monitoring instance to collect performance data. You can modify performance counters and attributes for a monitoring object, and monitor the data collection and alarm status in real time for all performance monitoring instances.
3. **Querying Latest Performance Data**: Performance data reported by NEs is stored in the eSight performance database. You can monitor the latest performance data in a performance monitoring view in real time, and query historical performance data based on the specified time segment. Performance data can be displayed in tables (default display mode) and graphs (advanced display mode). For details, see **Querying Latest Performance Data** and **Querying Historical Performance Data**.

Process of Reporting Performance Data on the NE Side

The process of reporting performance data on the NE side is as follows:

After receiving a performance monitoring task from a performance monitoring template or instance in the eSight, an NE starts to collect performance data, and reports performance data and alarms to the eSight periodically. The PRESTAT module in the eSight processes the original performance data before generating reports and reporting results to the superior NMS as required, and stores the processing result in the performance database.

5.3 Setting Performance Monitoring

By monitoring and collecting NE or network performance data, network maintenance personnel can detect and rectify potential faults in advance.

5.3.1 Configuring a Performance Monitoring Template

A performance monitoring template automatically collects KPI data on NEs. After an NE of the same type as NEs specified in the template is created, the NE automatically inherits the performance monitoring template, executes the performance monitoring task, collects performance data, and generates alarms.

Context

NEs of the same type share the same attributes. After you set the preceding attributes for a performance monitoring template, when a new NE of the same type is connected to the eSight, the eSight automatically delivers the template to the NE and provides the default performance alarm management for the NE. Settings in a performance monitoring template can be used for NEs in batches, which improves the efficiency in creating and delivering performance monitoring tasks.

Procedure

Step 1 Choose **Performance** > **Template Configuration**.

Step 2 Select an NE type in the navigation tree. Then all the performance counters for this NE type are displayed in collapsed mode in the right pane.

Step 3 Click  to expand the performance counters.

Step 4 Click  . On the **Change Thresholds** page that is displayed, set the threshold for generating an alarm, and click **OK**.

NOTE

When **Number of repetitions** is set to **3**, a device reports an alarm only after the performance counter value exceeds the threshold in three consecutive collection periods.

Step 5 Set collection thresholds, Click **Monitoring**.

Step 6 Click **Apply** to deliver the performance monitoring template (including the performance monitoring task) to NEs.

----End

5.3.2 Creating a Performance Monitoring Task

To start a performance monitoring task for collecting performance data, you must first create a performance monitoring task.

Procedure

Step 1 Choose **Performance** > **Monitoring Configuration**.

Step 2 Click **Create**.

Step 3 Click **Select Managed Objects**, On the **Select Managed Objects** page that is displayed, choose a subnet in the navigation tree. All managed objects are displayed for this subnet in the **Managed Objects** pane.

Step 4 Click  to expand managed objects, select the required managed objects, and click **OK**.

Step 5 Click **Select Indicators**. On the **Select Indicators** page that is displayed, choose a object type in the navigation tree. All counters are displayed for this object type in the **Indicators** pane.

Step 6 Click  to expand indicators pane, select the required managed objects, and click **OK**.

Step 7 **Optional:** To define the performance data collection period and performance threshold, click **Modify Properties**.

1. Deselect **Enable Template** for the required performance counter.

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.

2. Change the performance data collection period. Click  to change the performance threshold for reporting an alarm. Then click **OK**.

   NOTE

   If **Number of repetitions** is set to **3**, a device reports an alarm only after it is generated in three consecutive performance data collection periods.

3. Click **OK**.

Step 8 In **Measurement Objects**, click  . In the **Select the measurement objects for the indicators** window, enter or select measurement objects. Click **OK**.

NOTE

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.

Step 9 Click **OK** and view the performance monitoring instance creation result for this performance counter in **Result**.

Step 10 Click **Finish** to return to the **Monitoring Configuration** page.

----End

5.3.3 Setting A Performance Monitoring Task

After creating a performance indicator monitoring task successfully, you can modify, delete, start, stop, and view it.

Prerequisite

A performance monitoring task has been created.

Procedure

Step 1 Choose **Performance** > **Monitoring Configuration**.

Step 2 Set the search criteria and click **Search**. The performance monitoring tasks that meet the search criteria are displayed.

Step 3 Select multiple monitoring objects in the performance monitoring list, and click **Modify** to modify multiple performance monitoring tasks in batches.

Step 4 On the **Modify Properties** page that is displayed, select a performance counter to be modified, set the items such as whether to enable the template, performance data collection period, and performance threshold for reporting an alarm, and then click **OK**.

Step 5 Select multiple monitoring objects in the performance monitoring list, and click **Start** to start multiple performance monitoring tasks.

NOTE

- You can start a performance monitoring task only when the value of **Collection Status** is **Stopped**. If **Collection Status** is **Abnormal**, stop the collection task and check that the communication is normal first.
- You can stop or delete performance monitoring instances in batches.

----End

5.3.4 Adding a Performance Monitoring View

A performance monitoring view provides real-time graphical monitoring for Key Performance Indicators (KPIs). In a performance monitoring view, you can monitor multiple objects for one performance counter or monitor multiple performance counters for one object.

Prerequisite

- One or more performance monitoring instances exist.
- 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

Step 1 **Optional:** Create a performance monitoring view on the main page.

1. Choose **Performance** > **Monitoring View**.
2. Click **Add Monitoring View**.
3. On the **Add Monitoring View** page that is displayed, set **View name**, and select managed objects in the **Managed Object** pane. The matching counter instances are displayed in the **Indicator Instances** pane.
4. Select counters to be added to the performance monitoring view, and click **OK**.

Step 2 **Optional:** Save the performance monitoring view in the performance monitoring list.

1. Choose **Performance** > **Monitoring Configuration**.
2. Set the search criteria and click **Search**. The performance monitoring tasks that meet the search criteria are displayed.
3. Select multiple monitoring objects in the performance monitoring list, and click **Save as Monitoring View**.
4. On the **Add Monitoring View** page that is displayed, set the view name, and click **OK**.

----End

Follow-up Procedure

Choose **Performance** > **Monitoring View**. Select a required monitoring view. Click  . On the **Modify Monitoring View** page, change the view name and add/delete performance counters.

5.4 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.

5.4.1 Querying Latest Performance Data

You can query performance data monitored in the latest one week that is displayed in a performance monitoring view and view data changes in graphics.

Prerequisite

A performance monitoring view has been added for the performance counters to be queried.

Procedure

Step 1 Choose **Performance** > **Monitoring View**.

Step 2 Click  to display the proper performance monitoring view.

----End

5.4.2 Querying Historical Performance Data

You can query historical performance data in a specified period to get familiar with the network or service running status.

Procedure

Step 1 Choose **Performance** > **Historical Data**.

Step 2 Click **Select Managed Object**. On the **Select Managed Object** dialog box that is displayed, select the object type to be queried, and click **OK**. All managed objects of the selected object type are displayed in the **Managed Object** column.

Step 3 Select managed objects in batches, and click **OK**. The managed object sets associated with the selected object type are displayed in **Managed Objects**.

Step 4 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 5 Click the **Data Graph** tab and select a measurement counter.

Step 6 Click **Select Instances**.

Step 7 On the page that is displayed, select multiple instances that are related to the measurement counter, and click **OK**. The performance data is displayed in graphics for the measurement counter.

NOTE

The performance data of the measurement counter is displayed in different colors for different instances in the graph.

----End

Follow-up Procedure

Click **Export All Data** to save the collected performance data to a local .csv file.

5.4.3 Viewing NE Performance Overview

In the NE manager, you can view the real-time KPI data about NEs, which is displayed in graphics.

Prerequisite

The NE to be viewed supports performance management.

Procedure

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

Step 2 Choose an NE in the navigation tree, and click the NE name in the **Name** column in the right pane.

Step 3 Click  to view the NE basic information and KPI data.

Step 4 **Optional:** Click **Configure**. In the **Configure** dialog box, select KPIs to be displayed in graphics of **KPI**, and click **OK**.

TIP

- Click and select **Indicator Details**. The KPI data graph is automatically displayed on the **KPI Indicator Details** tab page. You can view the KPI data at different data collection time points.
- If a KPI contains multiple measurement objects, click  , select **Measurement Object**, and add/delete measurement objects to be displayed in a data graph on the page that is displayed.

----End

6 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.

6.1 Report Functions

The report system provides flexible and easy-to-use application services such as developing reports based on design documents and generating, forwarding, and managing reports based on the Web. The report system provides the functions such as monitoring, analyzing, optimizing, and formulating 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:

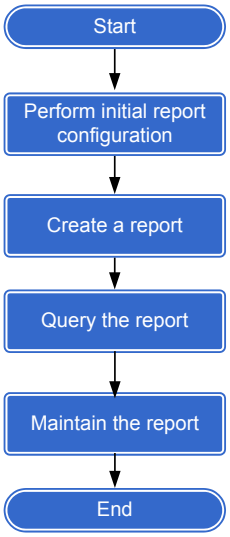
- Store reports to the report storage area.
- Store only periodical reports to the report folder of the report storage area.
- Configure the report storage area.
- Print reports in the report storage area in the report system.

6.2 Configuration Process

This topic describes the process of configuring the report system.

Figure 6-1 shows the process of configuring the report system.

Figure 6-1 Process of configuring the report system



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.
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

6.3 Setting the Report System Parameters

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

6.3.1 Configuring the Report System

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

Procedure

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

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

6.3.2 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.

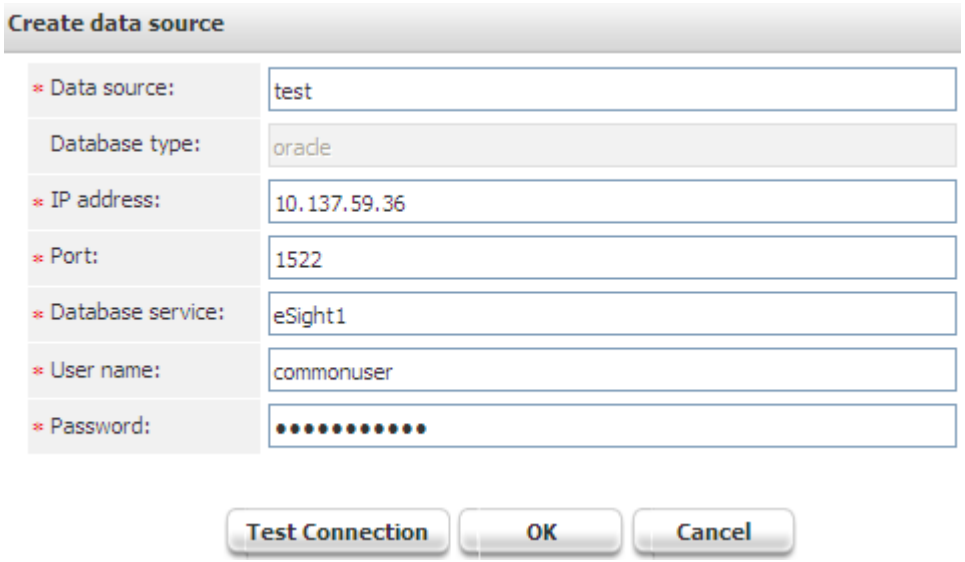
Context

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**.

6.4 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.

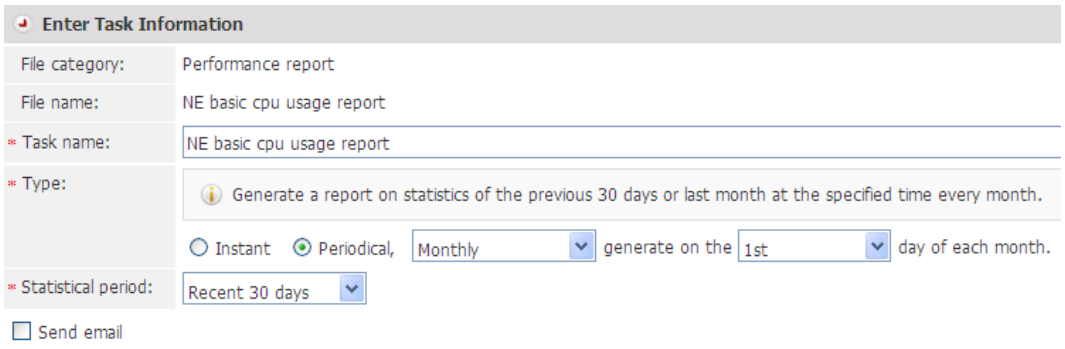
TIP

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.



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.
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

6.5 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.

NE CPU Usage Report

Execution Time :2011-08-05 06:18:40

Statistic Range :2011-08-01 19:12:59 - 2011-08-31 19:13:01

Device Name	Device Regoin	Device Type	Device IP	Instance
10.137.59.230	ROOT	AR1220V	10.137.59.230	Slot:Board 2
10.137.59.230	ROOT	AR1220V	10.137.59.230	Slot:SRU Board 0
cisco_10.137.134.192	ROOT	Catalyst4507RE	10.137.134.192	CPU:1
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:0
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:2
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:3
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:5
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:6

----End

6.6 Maintaining the Report System

Periodically maintain the report system as required.

6.6.1 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

6.6.2 Managing Report Storage Space

When the report storage area is full, you should periodically clear the reports in the storage area to release the space.

Procedure

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

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

6.6.3 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.
- For a periodical report task, click to disable the task.
- For an instant report task, click to execute the task immediately.

----End

7 NE Explorer

About This Chapter

eSight provides the functions such as managing basic device information, viewing device panels, managing device interface information, and viewing IP addresses.

7.1 NE Explorer Function

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.
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.

7.2 Querying an NE

This topic describes how to monitor an NE by querying the basic information, panels, and alarm and performance of the NE.

7.2.1 Querying Basic Information

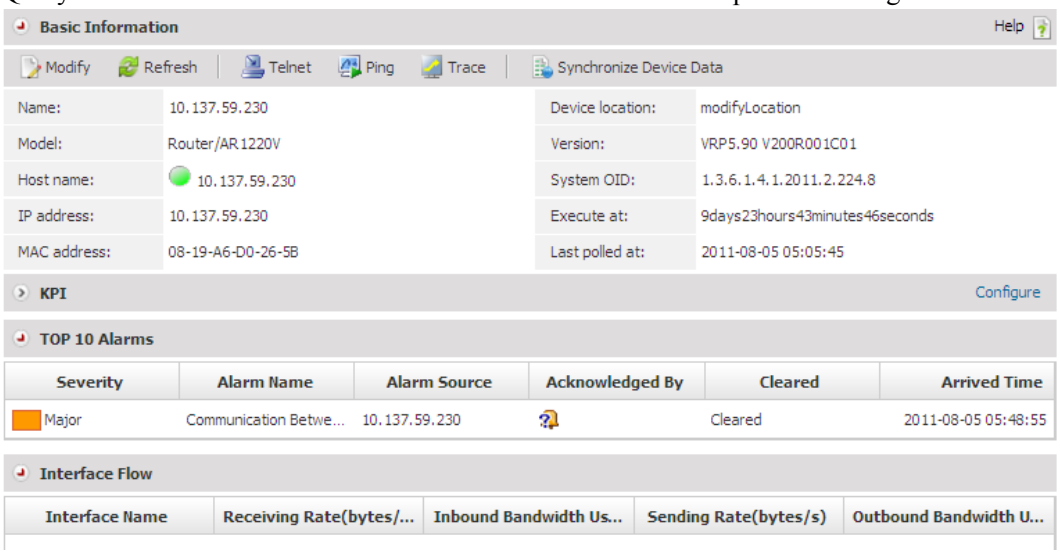
This topic describes how to query the basic information of an NE.

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**.

Step 3 Query the basic information of the NE in the **Basic Information** pane on the right.



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**.
- 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 **7.3.2.1 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.

Step 4 Click **KPI** to view the key performance information of the NE.

Step 5 Click **TOP 10 Alarms** to view the top 10 alarms of the NE.

Step 6 Click **Interface Flow** to view the interface traffic volume of the NE.

----End

7.2.2 Viewing the Device Panel

This topic describes how to view the information of the slot, board, subcard, and port where an NE resides 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.

----End

7.2.3 Querying the Alarm List

This topic describes how to view the NE alarm list.

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 7-1 Operations in Current Alarms window

Operation Name	Operation Method	Description
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. ● 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**.	-
Acknowledge	Select one or more alarms and click **Acknowledge**.	● If the alarm is acknowledged, **Acknowledge User** displays the user who acknowledges the alarm. ● If the alarm is unacknowledged, **Acknowledge User** displays  .

Operation Name	Operation Method	Description
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 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**.	● 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 .	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**.	-

----End

7.2.4 Querying Performance Status

This topic describes how to query performance status.

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

7.2.5 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**.

Step 3 Click **Synchronize**. After the synchronization, in the displayed **Progress** window, click **View Details** to 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

7.3 Configuring an NE

NE configuration includes the NE configuration method, protocol parameters, interfaces, and restoration of the NE configuration file.

7.3.1 Configuring Web NMS of NE

eSight integrates NE Web NMS to enable NE configuration.

Prerequisite

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

7.3.2 Setting Protocol Parameters

To implement normal communication between eSight and an NE, you should set the protocol parameters of eSight.

7.3.2.1 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.

Prerequisite

The Telnet parameters on eSight and NE are the same.

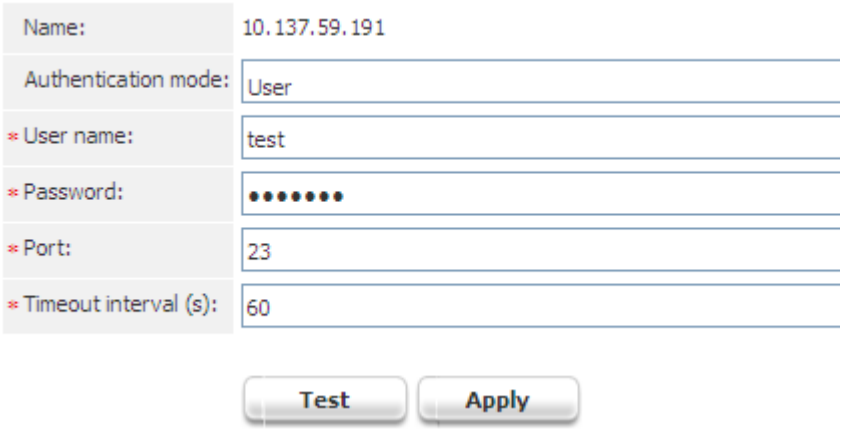
A device is added to eSight.

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

7.3.2.2 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.

Prerequisite

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

A device is added to eSight.

Context

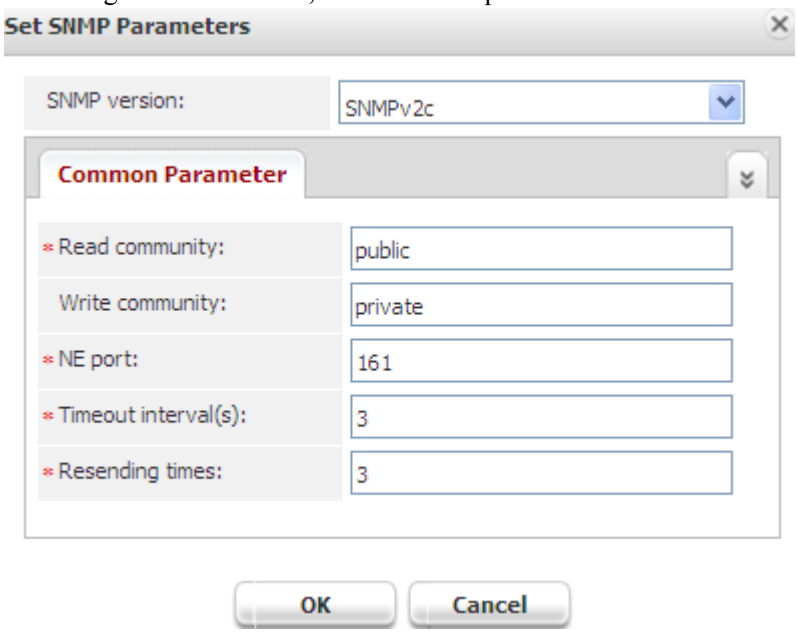
eSight accesses a managed NE over SNMP. When you manually create an SNMP NE or an SNMP NE is automatically created, eSight adapts a specified NE by using the default SNMP profile to determine the SNMP parameters supported by the managed NE. If adaptation is successful, the default profile is the SNMP 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.
- **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.
- **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.
- **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.

Step 4 Click **Test**. After the test, click **Apply**.

----End

7.3.3 Managing Interfaces

To manage a device, a user must know the basic information and state of the interfaces on the device.

7.3.3.1 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.

7.3.3.2 Configuring Interfaces

This topic describes how to activate, deactivate an interface, and modify the alias of the interface.

Prerequisite

SNMP write permission is set.

Procedure

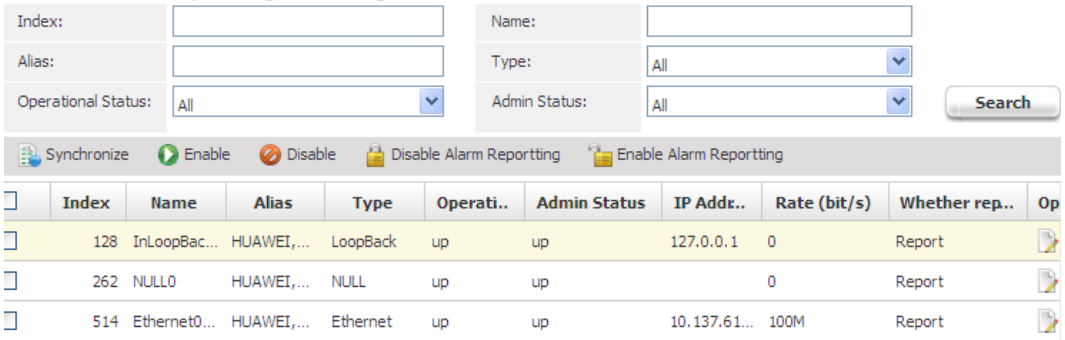
Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

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.

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

7.3.3.3 Querying Interface Parameters

eSight supports query of information on an 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** > **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

7.3.4 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.

Prerequisite

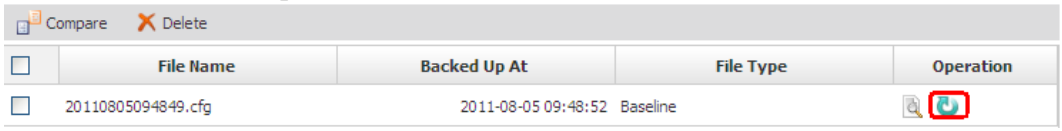
SNMP write permission is set.

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 **10.4.2 Backing Up NE Configuration Files Manually**.

8 Service Management

About This Chapter

eSight provides the function of managing Wireless Local Area Network (WLAN) and the IP Security (IPSec) Virtual Private Network (VPN) services.

8.1 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.

8.1.1 What Is IPSec VPN

IPSec VPN is a layer 3 tunnel encryption protocol developed by the Internet Engineering Task Force (IETF) to ensure the security and confidentiality of data transmitted over the Internet. IPSec VPN provides security services for IP packets at the IP layer. The IPSec protocol defines how to add fields to IP packets to ensure integrity, confidentiality, and correctness of IP packets, and how to encrypt IP packets. IPSec VPN protects data transmitted between two hosts, between two security gateways, or between a host and a security gateway.

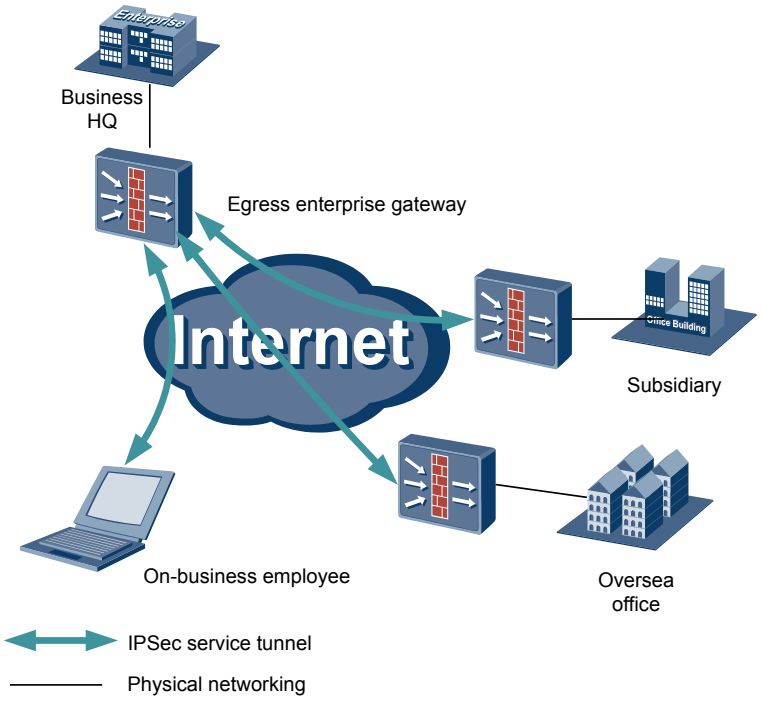
8.1.1.1 IPSec VPN Application

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 8-1**. 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 8-1 Typical application scenario of IPSec VPN



8.1.1.2 Related Concepts of IPSec VPN

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

Data Flow

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

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

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

Security Association (SA)

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

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

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

SA Negotiation Mode

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

- Internet Security Association and Key Management Protocol (ISAKMP) negotiation

  The IKE automatic negotiation mode, that is, ISAKMP negotiation mode, is quite simple. You only need to configure the security policy information about which the IKE negotiated. ISAKMP establishes and maintains SAs in automatic negotiation mode.

  NOTE

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

- Manual negotiation

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

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

Data Protection Mode

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

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

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

8.1.2 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

8.1.3 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.

Prerequisite

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

8.1.4 Viewing the Topology Structure of the IPSec Service

When querying the topology structure of the network domain, a user can view the tunnels of nodes in the network domain and tunnel status information in the topology view.

Procedure

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

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

8.1.5 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

8.2 WLAN Service Management

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

8.2.1 What Is 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.

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.

8.2.2 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.

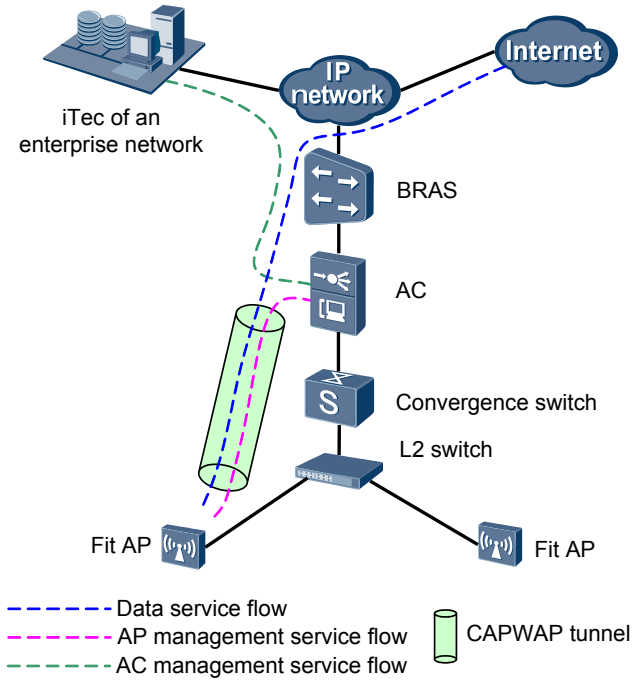
In the direct connection network scheme, each AP establishes a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel with an AC. Management services must be encapsulated in CAPWAP tunnels. Data services can be encapsulated in CAPWAP tunnels.

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 8-2**. All the data services and AP management services are encapsulated in CAPWAP tunnels. Different Virtual Local Area Networks (VLANs) distinguish different services.

  Figure 8-2 Data services encapsulated in CAPWAP tunnels

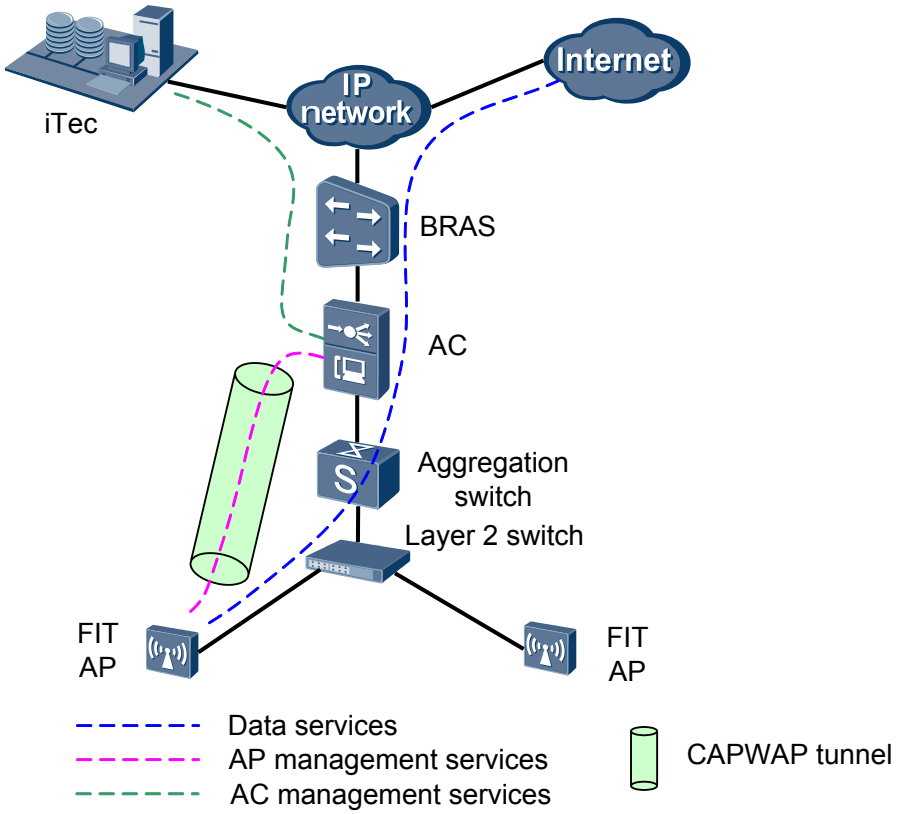


  In this mode, you only need to configure management VLANs on switches in advance. You do not need to configure data VLANs. The AP management VLANs connect APs to ACs.

- 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 8-3**. No data service is encapsulated in CAPWAP tunnels. Data services are forwarded from the AC to the upper-layer device. The AP management services are encapsulated by CAPWAP tunnels. Different VLANs distinguish different services.

  Figure 8-3 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

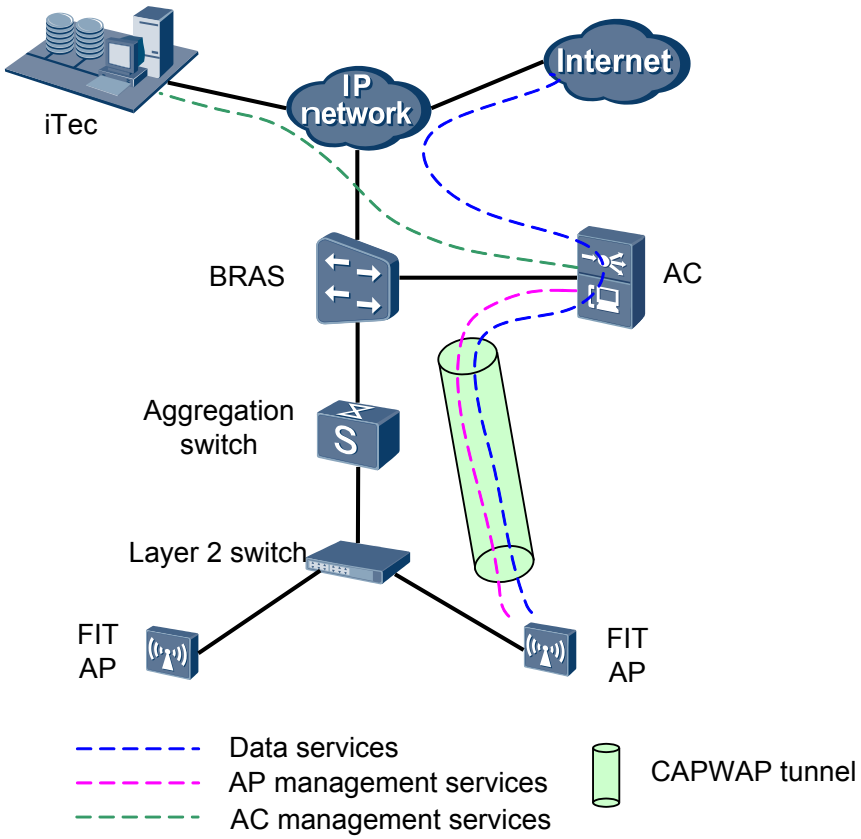
In a hung beside network, ACs are hung beside the BRAS to manage the WLAN service of APs. In the hung beside network mode, ACs that are hung beside the BRAS manages all the APs that are deployed within the management area of the BRAS, and AC deployment is quite centralized. The hung beside network mode 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 8-4**. All the data services and AP management services are encapsulated in CAPWAP tunnels. Different VLANs distinguish different services.

  Figure 8-4 Data services encapsulated in CAPWAP tunnels

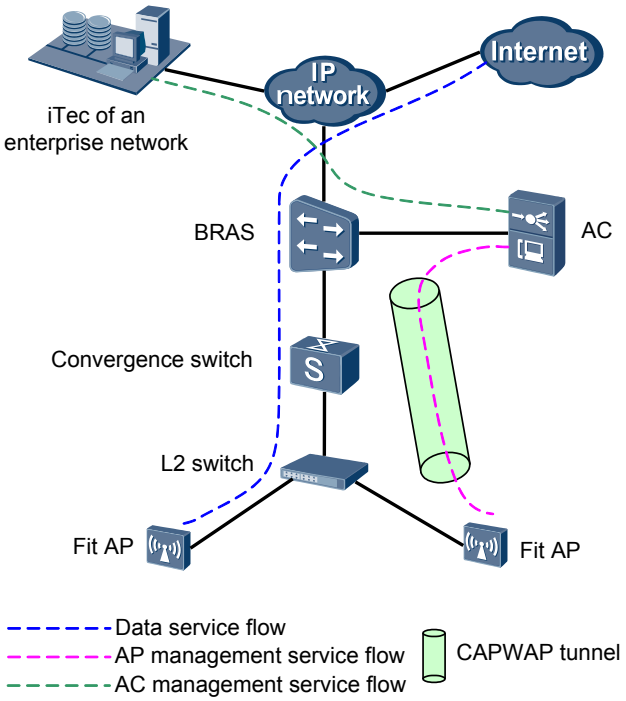


  In this mode, you only need to configure management VLANs on switches in advance. You do not need to configure data VLANs. The AP management VLANs connect APs to ACs.

- 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 8-5** shows the networking diagram.

Figure 8-5 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 8-1** compares the direct connection network with the hung beside network.

Table 8-1 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.

8.2.3 WLAN Operation

This topic describes how to manage the WLAN service.

8.2.3.1 Setting Basic AC Information

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

Prerequisite

SNMP write permission is set.

Procedure

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

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

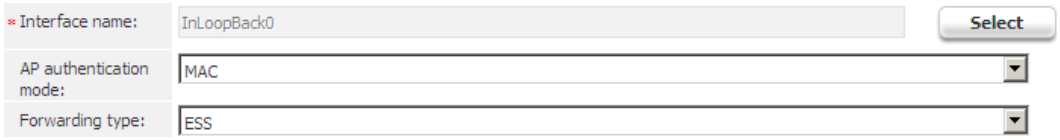
Step 3 In the pane on the right, click **Add**. In the displayed **Create AC** window, click **Select**. In the window that is displayed, select an AC and click **OK** to create an AC.

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.

8.2.3.2 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.

Prerequisite

A VLAN is configured.

The basic functions of the AC are configured.

The AP is connected to an AC.

The AC is set to report alarms to the eSight server.

SNMP write permission is set.

Context

The process of connecting an AP to a WLAN is as follow:

- If an AP is added in offline mode, this AP can be directly connected to a WLAN.
- If an AP is not added in offline mode, but **AP authentication mode** is set to **No authentication**, or AP MAC or SN is in the set **Whitelist**, the AP is automatically added and connected to the WLAN.
- If an AP does not exist in the whitelist or AP list, and **AP authentication mode** is not set to **No authentication**, the AP is in the unauthorized AP list. You can identify the AP in the unauthorized AP list to determine whether to add the AP to the WLAN.

Procedure

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

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

8.2.3.3 Configuring a Profile

Configure an AP profile, a radio profile, and an ESS profile and bind the profiles to an AP to complete AP service configuration.

?.1. 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.

Prerequisite

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.

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

NOTE

Click  to modify AP profile parameters.

----End

?.2. 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.

Prerequisite

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

?.3. 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.

Prerequisite

SNMP write permission is set.

A maximum of 32 ESS profiles can be created on eSight.

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

8.2.3.4 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.

Prerequisite

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 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

8.2.3.5 Binding Profiles to an AP

Bind the related AP profile, radio profile, and ESS profile to an AP to complete AP service provision.

Prerequisite

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

8.2.3.6 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 on the left, 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 8-2 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.
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	
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

8.2.3.7 Browsing STAs

A user browses information on all wireless terminal on the live network.

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

8.2.3.8 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

8.2.3.9 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.

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 Smart Configuration Tool

About This Chapter

This topic describes the system functions and the related operations of the iManager U2000 Smart Configuration Tool.

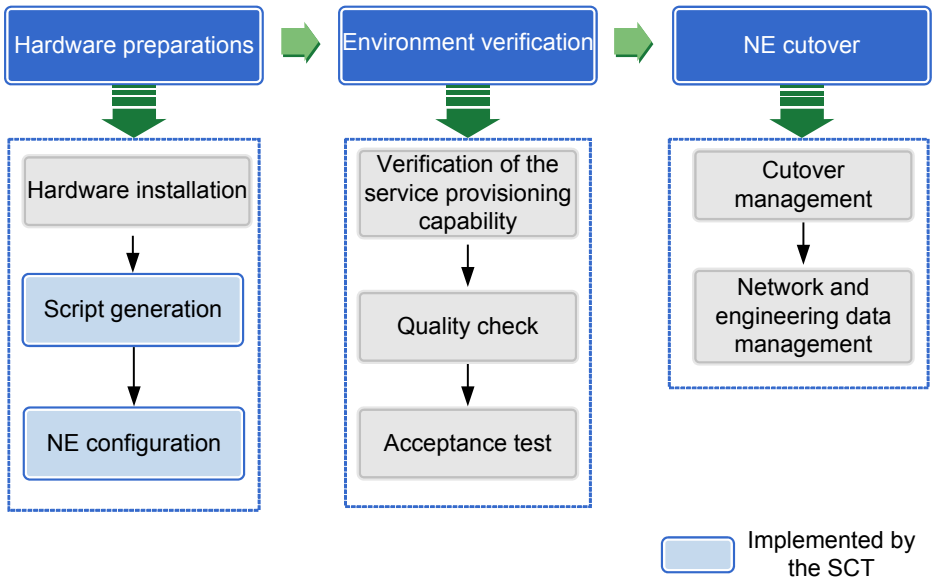
9.1 SCT Overview

This topic describes the functions of the iManager eSight SCT.

9.1.1 Introduction to the SCT

Generating and deploying scripts are necessary for network environment setup. Manual script generation based on sample scripts and network planning tables takes a long time and is very prone to errors. The SCT can use configuration templates and planning tables to generate scripts in one-touch mode and deploy the scripts to NEs in batches, which improves the efficiency of making scripts.

- The SCT is used to make scripts and configure NEs during deployment. With the graphical Command Line Interfaces (CLIs) provided by the SCT, you can enter command keywords to query the required configuration command or set the relevant parameters to create a script.
- The SCT supports template management. You can use a template to quickly generate a script that is used for batch configuration of NEs.



SCT: Smart Configuration Tool

Use any of the following methods to generate a script:

- Create a template according to Low Level Design (LLD) documents and import a network planning table to generate scripts in batches.
- Use an existing script to generate a template and apply the template to NEs of the same type to generate an NE script.
- Use a universal template to generate a script.
- Enter commands to create a script.

9.1.2 System Functions

This topic describes the functions of the SCT.

Offline Script Verification

The SCT allows you to modify scripts in offline mode. The SCT automatically verifies generated scripts and displays verification results in different colors to ensure that all configurations are compliant with command line standards.

Quick Template Generation

Scripts can be used to generate templates in one-touch mode, facilitating the similar configuration in subsequent operations.

Planning Table-based Script Generation in One-Touch Mode

Templates can be exported in batches to generate a planning table. After you set parameters in the planning table and import the planning table, the SCT automatically generates a script based on the planning information.

Batch Configuration

Scripts can be quickly deployed to multiple NEs to implement batch NE configuration.

Universal Template

The SCT provides universal templates that are applicable to different configuration situations. Select the required template and set parameters in the template to generate scripts.

9.2 Client Window Overview

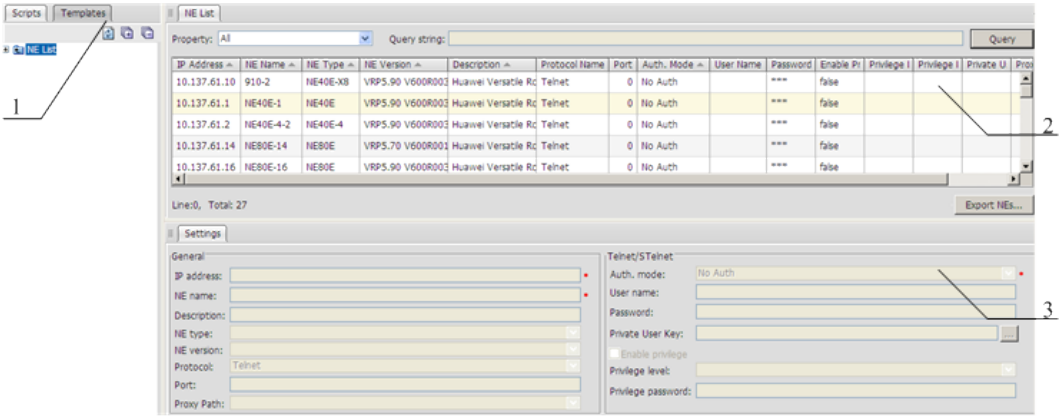
This topic describes the main client window on the iManager eSight SCT, helping to find navigation paths quickly and increase operation efficiency.

9.2.1 Main Client Window

This topic describes the elements in the main client window on the SCT and the functions of these elements.

Main Client Window

Figure 9-1 Elements in the main client window



(1) **Scripts** and **Templates** tab pages (2) Configuration area

(3) **General** area

Element Description

1. **Scripts** and **Templates** tab pages
   - The **Scripts** tab page displays the **Devices** navigation tree. Scripts can be created for each NE in the navigation tee. The NEs can be classified into different folders for easy search and management.
   - The **Templates** tab page displays the **Templates** navigation tree. This tree contains both universal templates and customized templates. The templates can be classified into different folders for easy search and management.
2. Configuration area
   - Select a script from the **Devices** navigation tree and modify the script information in the configuration area. You can also right-click a script and choose **Save Configurations**, **Deploy Script**, **Apply Template**, or **Configure Terminal** from the shortcut menu to perform the relevant operation.
   - Select a template from the **templates** navigation tree and modify the template information in the configuration area.

   NOTE

   If you select a folder or main node from the navigation tree, the configuration area only allows you to view the script, NE, or template information about the folder or main node.
3. **General** area

   If you select a record in the configuration area, general information about the record is displayed in the **General** area.

   NOTE

   If you select a script or template from the navigation tree, no general information is displayed.

9.2.2 Shortcut Icons

This topic describes the functions of shortcut icons used for the configuration of scripts or templates.

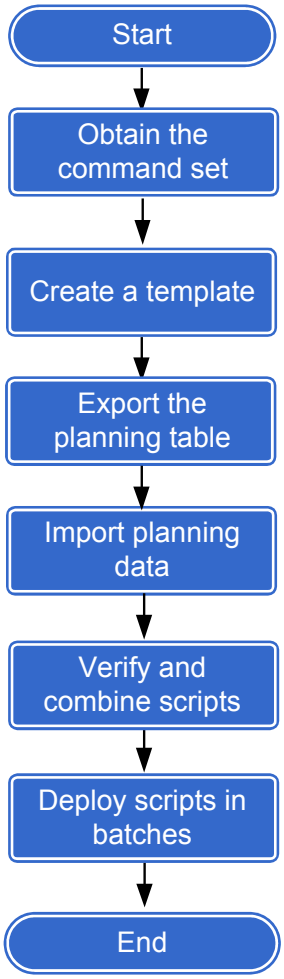
Icon	Name	Function
Shortcut icons for script configuration		
	Modify	Locks a script and synchronizes the script information. If you click this shortcut icon when modifying a script, only the current client can be used to modify the script and other clients are locked. This prevents concurrent operations by multiple clients.
	Save	Saves script information. A script can be verified, deployed, or converted to a template only after the script is saved. In a saved script, the information is displayed in colors. If an incorrect command is entered, the entire line of the command is displayed in red.
	Find/Replace	Finds and replaces script information matching the specified keyword.
	Previous Error	Locates the previous incorrect command line in the current script.
	Next Error	Locates the next incorrect command line in the current script.
	Deploy	Deploys a script to an NE.
	Verify Script	Verifies whether the script information is syntactically correct and displays the verification result. The commands with **Verification Result** being **Failure** are displayed in red. For the incomplete commands with **Verification Result** being **Fuzzy match**, reference commands are displayed for the user to enter a complete commands.
	Generate Template	Converts script information to a template to facilitate the similar configuration in subsequent operations.
	Query	Queries the commands related to a command keyword entered in the query box. **NOTE** ● A maximum of 200 commands (the first 200 commands) related to the specified command keyword can be displayed. ● When querying commands, you can enter only a command keyword, not command parameters.
Shortcut icons for template configuration		
	Modify	Locks a template and synchronizes the template information. If you click this shortcut icon when modifying a template, only the current client can be used to modify the script and other clients are locked. This prevents concurrent operations by multiple clients.
	Copy	Copies a command or view selected from the current template or another template.

Icon	Name	Function
	Paste	Pastes the copied command or view to a new location.
	Up	Moves the selected command/view and its sub nodes upwards.
	Down	Moves the selected command/view and its sub nodes downwards.
	Insert	Inserts a command into a template.
	Delete	Deletes the selected command from a template.
	Modify Description	Updates the description about a command.
	Modify Command	Modifies the command.
	Apply	Applies the current template to an NE for script generation.
	Save	Saves template information.
	Save as	Saves the current settings as a new template.
	Expand	Expands all commands.
	Collapse	Collapses all commands.
	Switch	Switches between the display of **Command** and **Command Description**.

9.3 Configuration Process

This topic describes the process of using the SCT to configure NEs in typical scenarios.

Figure 9-2 Flowchart of configuring NEs



No.	Task	Description
1	**Obtaining command sets**	This task is to obtain command sets. Script verification and template generation can be performed only after the associated NE command sets have been obtained.
2	**Creating a template**	This task is to create a template. A lot of NEs need to be configured during network configuration. You can create a template for NEs of the same type and apply the template to these NEs. This improves script generation efficiency.
3	**Exporting the planning table**	This task is to export the network planning table by using a template.
4	**Importing planning data**	This task is to import planning data. The SCT can automatically generate scripts for every NE.

No.	Task	Description
5	Verifying and combining scripts	This task is to verify script syntax in offline mode according to the relevant command sets, and combine multiple scripts into one script.
6	Deploying scripts in batches	This task is to implement batch NE configuration by deploying scripts.

9.4 SCT Operation Tasks

This topic describes how to configure NEs in typical scenarios where the SCT is used.

9.4.1 Obtaining Command Sets

This topic describes how to obtain command sets. After the associated NE command sets have been obtained, perform operations such as script verification and template generation.

Context

- Check whether the NE type and version are empty in the NE list. If the NE type and version are not empty, the command sets of the NE have been obtained by the SCT and you do not need to click **Obtain Command Set**.
- If no command set is obtained, check whether the Telnet/STelnet parameters of the NE are correct by clicking **Test** in the **General** area in the NE list. If the test failed, reset the Telnet/STelnet parameters for the NE. Command sets can be obtained only after the test succeeds.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 In the **NE List** navigation tree, select the NE whose command set needs to be obtained, right-click, and then choose **Obtain Command Set** from the shortcut menu.

A progress bar is displayed indicating the progress of obtaining the command set.

Step 4 **Optional:** Click **Run in Background**.

Step 5 After obtaining the command set successfully, click **Close**.

The values of **NE type** and **NE version** for the NE are changed.

----End

9.4.2 Creating a Template

This topic describes how to create a template. A lot of NEs need to be configured during network configuration. You can create a template for NEs of the same type and apply the template to these NEs. This improves script generation efficiency.

Use any of the following methods to generate a template:

- Importing an existing template: Import an existing template to the SCT.
- Generating a template using existing scripts: Use sample scripts in the Low Level Design (LLD) document or existing scripts to generate a template.
- Manually creating a template: If neither the LLD document nor existing scripts are available, manually create a template. This method requires a good grasp of NE configuration commands.

9.4.2.1 Importing a Template

This topic describes how to import a template. The template can be either a customized one or a universal one provided by the SCT.

Prerequisite

The template to be imported must be available.

Procedure

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

Step 2 Click the **Templates** tab.

Step 3 **Optional:** In the **Templates** navigation tree, right-click the **Templates** node and choose **Create Folder** from the shortcut menu.

Step 4 **Optional:** In the **Create folder** dialog box, enter a folder name, and click **OK**.

Step 5 Select the **Templates** node or the new folder, right-click, and choose **Import Template** from the shortcut menu.

Step 6 In the dialog box that is displayed, click **Browse**, and then select the template to be imported.

Step 7 Click **Import**. The imported template is displayed in the navigation tree.

----End

9.4.2.2 Generating a Template by Using Existing Scripts

This topic describes how to generate a template by using sample scripts in the Low Level Design (LLD) document or using existing scripts. Compared with the method of manually creating a template, generating a template by using sample scripts in the LLD document is more precise and efficient.

Prerequisite

Inheritable scripts must be obtained.

Context

Existing scripts are classified into the following types:

- Sample scripts in the LLD document
- Saved scripts that have been used

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 Choose **NE List** from the navigation tree. Select the NE to be configured, right-click, and choose **Create Script** from the shortcut menu.

Step 4 In the **Create Script** dialog box, set **Script Name** and **Description**. Click **OK**. The created script is automatically displayed under the relevant NE node.

Step 5 Click **Modify**. Then, copy sample scripts in the LLD document or saved scripts to the blank area in the right-hand pane and modify them as needed.

NOTE

If a script contains a large number of commands, click **Find/Replace** to modify the script.

Step 6 Click **Save**.

Step 7 Click **Verify Script**.

Step 8 In the **Verification Result** dialog box, view the verification result for each command.

- If the verification result of a command is **Error**, take the following operations:

  Click **Close**. In the text box for command query, enter the command and press **Enter** to check whether the NE supports the command. Then, modify the command in the **Script Configuration** area.

  NOTE

  Enter only the keyword of the command to be queried. Do not enter any command parameter.

- If the verification result of a command is **Ambiguous Match**, take the following operations:

  Click **Close**. In the text box for command query, enter the command and press **Enter**. The value range for the parameter in the command is displayed. Based on this range, modify the command in the **Script Configuration** area.

Step 9 Click **Generate Template**.

Step 10 In the **Generate Template** dialog box, modify the parameters in commands as needed.

Step 11 Click **OK**.

Step 12 In the dialog box that is displayed, set **Template Name**, **Template description**, and **Application scenario**.

Step 13 Click **OK**. A message is displayed indicating that the operation is successful.

Step 14 Click **OK**.

----End

9.4.2.3 Creating a Template

This topic describes how to create a template. NE configurations can be saved as a template so that you can use this template to configure NEs in batches.

Procedure

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

Step 2 Click the **Templates** tab.

Step 3 **Optional:** In the **Templates** navigation tree, right-click the **Templates** node and choose **Create Folder** from the shortcut menu.

Step 4 **Optional:** In the **Create folder** dialog box, enter a folder name, and click **OK**.

Step 5 In the **Templates** navigation tree, right-click the **Templates** node and choose **Create template** from the shortcut menu.

Step 6 In the **Create Template** dialog box, select a path for saving the template, set **NE type** and **NE version** related to the template, and enter basic template information. Then, click **OK**.

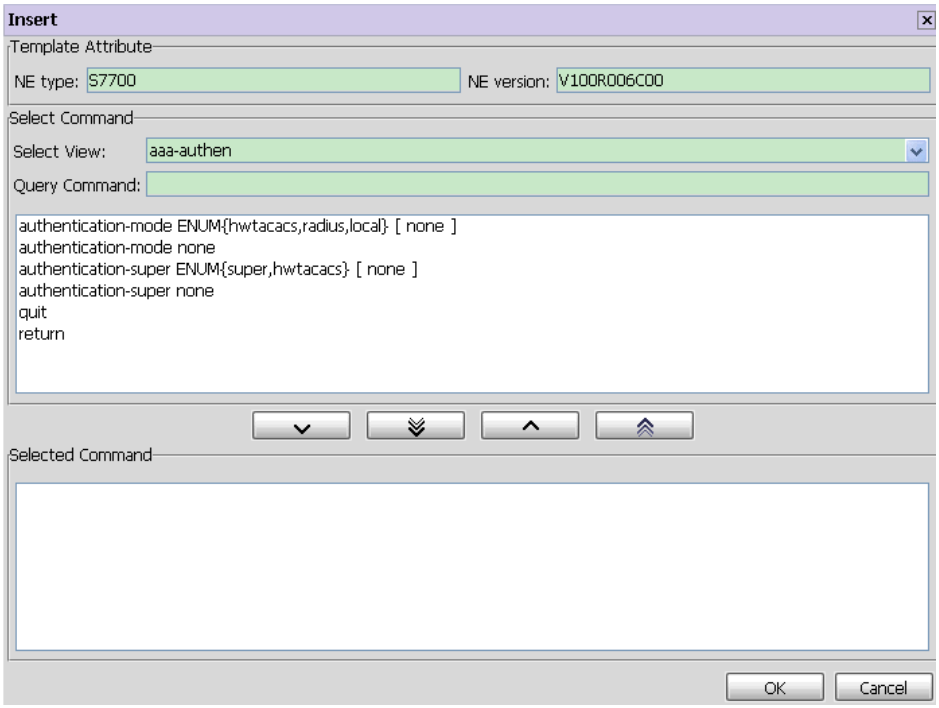
NOTE

If **NE type** or **NE version** is not set, no command can be inserted to the template.

Step 7 In the **Insert** dialog box, select a value from the **Select View** drop-down list.

Step 8 In the **Query Command** field, enter the keyword of the command to be queried.

All commands containing this keyword are displayed in the query result area.



Step 9 Click to add the required commands to the list of selected commands. Then, click **OK**.

The created template is displayed in the navigation tree, and details about the template are displayed in the **Template Configuration** area.

Step 10 In the **Template Configuration** area, modify the created template.

- Double-click a command or parameter to modify the related description.
- Double-click the **Parameter Value** column to enter or change parameter values.
- Click shortcut icons to perform command-related operations, such as inserting or deleting commands, or changing the command description. For detailed description of shortcut icons, see **9.2.2 Shortcut Icons**.

- Click in the **Command** column. In the dialog box that is displayed, modify the command view.

----End

9.4.3 Exporting the Planning Table

This topic describes how to export the network data planning table by using a template. After entering required information according to fields in the planning table, use the SCT to import configurations and generate scripts.

Procedure

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

Step 2 Click the **Templates** tab.

Step 3 Choose **Template List** from the navigation tree. Select a node at any level under the **Template List** node, right-click, and then choose **Export Planning Table** from the shortcut menu.

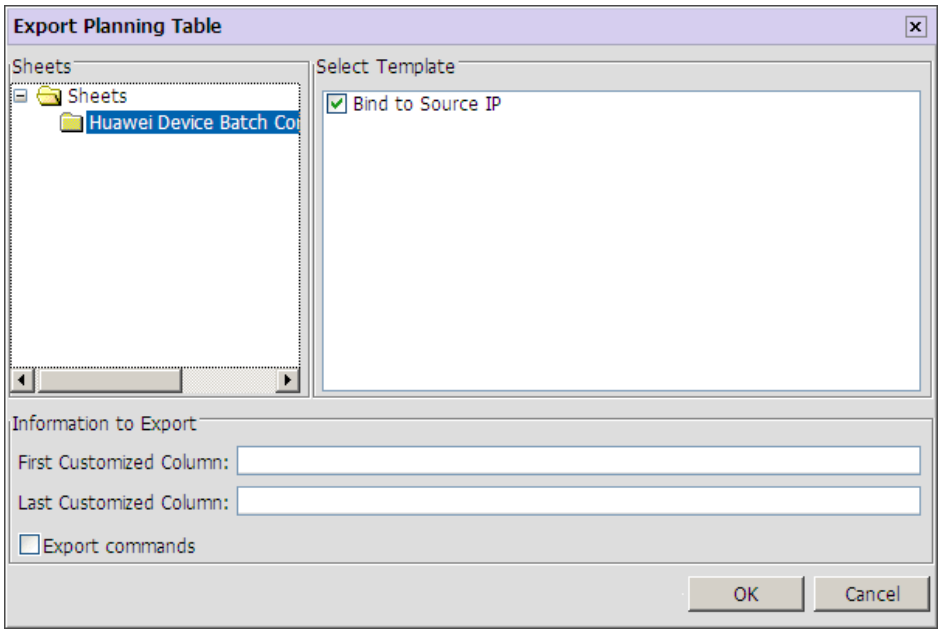
NOTE

If the selected node is a folder node, all templates in the folder will be exported to an .xls file.

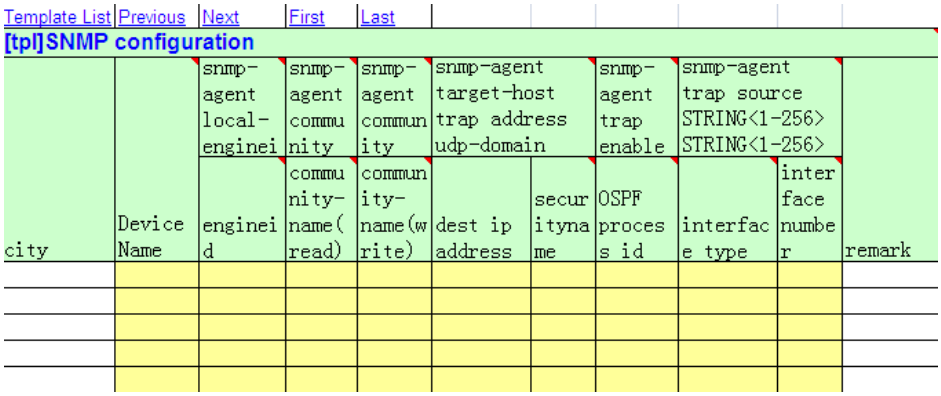
Step 4 Choose **Export Planning Table**.

Step 5 In the dialog box that is displayed, select the template to be exported and enter desired information.

- **First Customized Column** indicates the leftmost column in the exported table. You can add customized information and separate the information by comma.
- **Last Customized Column** indicates the rightmost column in the exported table. You can add customized information and separate the information by comma.
- If the **Export commands** check box is selected, complete command lines are displayed in the exported planning table. If the **Export commands** check box is not selected, only parameters are displayed in the exported planning table.



Step 6 Click **OK**. In the dialog box that is displayed, click **OK**. The following table is displayed.


Template List | Previous | Next | First | Last

[tpl]SNMP configuration

city	Device Name	snmp-agent local-enginei d	snmp-agent community community-name(read)	snmp-agent community community-name(write)	snmp-agent target-host trap address udp-domain dest ip address	snmp-agent target-host trap address udp-domain securityname	snmp-agent trap enable OSPF process id	snmp-agent trap source STRING<1-256> interface type	snmp-agent trap source STRING<1-256> interface number	remark

NOTE

- Commands in bald specify that the commands are used for accessing a view.
- During fill-in of parameters, you can add rows, but not columns.
- If a command needs to be applied to the same NE for several times, add multiple rows so that multiple commands can be generated in the script.
- During fill-in of parameters, refer to the parameter range in comments of the table.
- Parameters highlighted in yellow are mandatory and those highlighted in white are optional.
- If a mandatory parameter is not filled in, the generated scripts do not contain the command line associated with the parameter.
- Click **Template List**, **Previous**, **Next**, **First**, or **Last** in the first row of each table to switch to the related table.

Step 7 Enter detailed information. Then, choose **File** > **Save As** from the main menu to save the network data planning table to a local disk.

----End

9.4.4 Importing Planning Data

This topic describes how to import planning data. With this function, the SCT can automatically generate scripts for each NE.

Prerequisite

- A template must be created or imported.
- All the required information must be entered for the exported planning table.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 Choose **NE List** from the navigation tree. Right-click **NE List** and choose **Import Planning Table** from the shortcut menu.

Step 4 In the dialog box that is displayed, click **Browse** to select the network data planning table.

If the **Replace same-name script** check box is selected, scripts with the same name are replaced.

If the **Replace same-name script** check box is not selected, scripts generated subsequently will be named based on the previous script name. For example, if a script named **Interface Configuration(1)** already exists, after a planning table is imported, the script name is **Interface Configuration(2)**.

Step 5 Click **Import**. The associated scripts are automatically generated under each NE node according to the network data planning table and template.

----End

9.4.5 Verifying a Script

This topic describes how to verify the script for an NE in offline mode to check the script syntax according to the related command set.

Prerequisite

- Created scripts must exist. For details about how to create a script, see **9.5.4.1 Creating a Script Manually**.
- **NE version** and **NE type** must be set correctly for the specified NE.
- The command set for the NE whose script needs to be verified must exist on the SCT or have been imported into the SCT.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 In the **NE List** navigation tree, select the script to be verified, right-click, and then choose **Verify Script** from the shortcut menu.

Alternatively, click in the **Script Configuration** area to verify the script.

Step 4 In the **Verification Result** dialog box, view the verification result for each command.

- If the verification result of a command is **Error**, take the following operations:

  Click **Close**. In the text box for command query, enter the command and press **Enter** to check whether the NE supports the command. Then, modify the command in the **Script Configuration** area.

  NOTE

  Enter only the keyword of the command to be queried. Do not enter any command parameter.

- If the verification result of a command is **Ambiguous Match**, take the following operations:

  Click **Close**. In the text box for command query, enter the command and press **Enter**. The value range for the parameter in the command is displayed. Based on this range, modify the command in the **Script Configuration** area.

----End

9.4.6 Combining Scripts

This topic describes how to combine multiple NE scripts into one script.

Prerequisite

- All NE scripts must be generated.
- All NE scripts must be correct.

Context

This function supports the combining of multiple scripts for a single NE or all NEs.

Procedure

- Scenario 1: To combine multiple scripts for a single NE, perform the following operations:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Scripts** tab.
  3. Choose **NE List** from the navigation tree. Then, select the NE whose scripts need to be combined. All scripts for the NE are displayed in the **Script List** area in the right-hand pane.
  4. Select a script, right-click, and choose **Select All** from the shortcut menu.
  5. Right-click all the selected scripts and choose **Combine Script** from the shortcut menu.
  6. In the dialog box that is displayed, view the progress of combining scripts. When the progress bar reaches 100%, click **Close**.
- Scenario 2: To combine multiple scripts for all NEs, perform the following operations:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Scripts** tab.
  3. Choose **NE List** from the navigation tree. Select an NE under the **NE List** node. Then, select **All** from the **Attribute** drop-down list.
  4. Click **Query**. The scripts for all NEs are displayed.
  5. Select a script, right-click, and choose **Select All** from the shortcut menu.
  6. Right-click all the selected scripts and choose **Combine Script** from the shortcut menu.
  7. In the dialog box that is displayed, view the progress of combining scripts. When the progress bar reaches 100%, click **Close**.

----End

9.4.7 Deploying Scripts

This topic describes how to deploy scripts to configure NEs in batches.

Prerequisite

The scripts that have been successfully verified must exist. For details about how to verify a script, see **9.4.5 Verifying a Script**.

Context

Scripts for multiple NEs can be selected and deployed in batches.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 In the **NE List** navigation tree, right-click the script to be deployed or the NE where the script is to be deployed and choose **Deploy Script** from the shortcut menu.

Step 4 In the **Deploy Script** dialog box, select a script in the **Select Script** area. The details about the script are displayed in the **Preview** area.

If some command lines or parameters need to be modified, modify them and click **Save** before deploying the script.

Step 5 Click **Deploy**.

The scripts for multiple NEs can be selected for deployment.

Step 6 In the confirmation dialog box, click **OK**.

Step 7 The progress of deploying the scripts is displayed on the **Deployment** tab page.

If a script fails to be deployed, perform any of the following operations as needed:

- Retry: The system re-executes the abnormal command.
- Ignore: The system ignores the abnormal command and continues to execute the next command.
- Stop: The system stops deploying scripts.

Step 8 Click **Save Configurations** to save the configurations to NEs.

Step 9 Click **Close**.

----End

9.5 Common Maintenance Operations

This topic describes common maintenance operations on templates and scripts.

9.5.1 Configuring a Single NE

This topic describes how to configure a single NE.

Context

NOTE

In the main topology of the eSight client, right-click an NE and choose **Configuration Terminal** from the shortcut menu to configure the single NE.

The **Configuration Terminal** provides the following functions:

- Enters common command lines to configure NEs.
- Enters a command keyword in the query box to view the commands matching the keyword.
- Queries historical commands.

Historical commands are the ones that have been entered. This function helps to view information about the commands that have been executed for the specified NE.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 In the **NE List** navigation tree, right-click an NE and choose **Configuration Terminal** from the shortcut menu.

Step 4 Use either of the following methods to configure the NE:

- On the **Configuration Information** tab page, enter a configuration command and deploy it.
  1. On the **Configuration Information** tab page, enter a command keyword. Then, click  or press **Enter** to query the commands matching the keyword.
  2. Select the command to be configured and enter the parameter value.
  3. Click **Deploy**.

     The configuration results are displayed on the **Terminal Window** tab page.
- Enter configuration information on the **Terminal Window** tab page.

  The effect of NE configuration on the **Terminal Window** tab page is the same as the effect of NE configuration using Telnet.

Step 5 **Optional:** Click the **History Command** tab to view historical commands.

CAUTION

Historical commands cannot be dumped or saved. If the **Configuration Terminal** for a specified NE is closed, the relevant historical commands are deleted.

----End

9.5.2 Exporting NE Information into a File

This topic describes how to export NE information into a file in .xls format.

Context

The information about some NEs or all NEs can be exported as needed.

Procedure

- To export information about some NEs into a file, perform the following operations:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Scripts** tab.
  3. Choose **NE List** from the navigation tree.
  4. Hold down **Ctrl** and select the desired NEs in the right-hand **NE List** area.
  5. Right-click the selected NEs and choose **Export NE** from the shortcut menu.

6. In the dialog box that is displayed, click the **Save File** option button and click **OK**.

   NOTE

   - If the FireFox is used, the exported file is saved to **C:\Documents and Settings\osuser\My Documents\Downloads** by default. **osuser** indicates the user name for logging in to the OS. To change the path, do as follows:
     1. Choose **Tools** > **Options** from the main menu of the FireFox.
     2. In the **Downloads** area, click **Browse** and set the path.
   - If the Internet Explorer is used, the **Save As** dialog box is displayed. Select the path for saving the exported file.

- To export information about all NEs into a file, perform the following operations:
  1. Log in to the eSight client.
  2. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  3. Click the **Scripts** tab.
  4. Choose **NE List** from the navigation tree.
  5. Click **Export All NEs** in the right-hand **NE List** area.
  6. In the dialog box that is displayed, click the **Save File** option button and click **OK**.

     NOTE

     - If the FireFox is used, the exported file is saved to **C:\Documents and Settings\osuser\My Documents\Downloads** by default. **osuser** indicates the user name for logging in to the OS. To change the path, do as follows:
       1. Choose **Tools** > **Options** from the main menu of the FireFox.
       2. In the **Downloads** area, click **Browse** and set the path.
     - If the Internet Explorer is used, the **Save As** dialog box is displayed. Select the path for saving the exported file.

----End

9.5.3 Maintaining Templates

This topic describes how to maintain templates.

9.5.3.1 Modifying a Template

This topic describes how to modify commands and parameters in a template.

Context

Both predefined templates and customized templates can be modified.

Procedure

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

Step 2 Click the **Templates** tab.

Step 3 Choose the template to be modified from the navigation tree. All commands and parameters of the template are displayed in the right pane.

Step 4 Click **Modify**.

- Double-click a command or view to modify the related description.

NOTE

- The lines prefixed with asterisks (*) indicate mandatory parameters.
- If the descriptions of two parameters in a template are the same, the parameters are combined into one in the exported template.
- If a command contains parameters of the enumerated type and the enumerated parameter values are incomplete, modify the command to add values. For example, in the **authentication-mode aaa** command, **aaa** indicates that the authentication mode is AAA. The other two authentication modes are **password** and **none**. If you change **aaa** into **ENUM{aaa,none,password}** in the command, any authentication mode can be selected as needed when you set parameters.

- Double-click the **Parameter Value** column to enter or change parameter values.
- Click in the **Command** column. In the dialog box that is displayed, modify the command view.
- Set the command that contains no parameter in the template to be optional.
  1. Select the command that contains no parameter, and then click **Modify Command**. In the dialog box that is displayed, add square brackets for the selected command.

     NOTE

     Leave a space between the command and each square bracket.
  2. Click **OK**. A check box is displayed to the right of the command. If the check box is selected, it indicates that the command needs to be executed. If the check box is not selected, it indicates that the command will not be executed.
- Copy and paste commands.
  1. Select the commands to be copied or the view in which commands need to be copied, and then click to copy the commands.

     NOTE

     Items in either the current template or another template can be copied.
  2. Click to paste a copied item.
     - If a view or a parameter of the view is copied, the item will be pasted to the last node related to the view.
     - If a command or a parameter of the command is copied, the item will be pasted below the command.
     - To paste a copied item to a blank template, the root node must also be copied.
- Move the selected command upwards or downwards in the template.
  1. Click to move the command upwards.
  2. Click to move the command downwards.
- Delete a command or view.

  Select the command or view to be deleted, and click ✕.

  NOTE

  If you delete a selected view, all the commands related to the view are deleted.

Step 5 Click **Save**.

----End

9.5.3.2 Applying a Template

This topic describes how to apply a template to quickly generate a script.

Prerequisite

The network planning table must have been obtained to generate scripts for multiple NEs.

Context

Both custom templates and universal templates can be used to generate scripts.

Procedure

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

Step 2 Click the **Templates** tab.

Step 3 In the **Template List** navigation tree, right-click a template and choose **Apply Template** from the shortcut menu.

Step 4 In the **Apply Template** dialog box, select an NE in the **Select NE** area and click **Next**.

You can select multiple templates and apply them to an NE or select one template and apply it to multiple NEs.

Step 5 On the **Set Parameter** tab page, set command parameters and click **Finish**.

NOTE

- In a command, the parameter marked with an asterisk (*) must be set. If such a parameter is not set, the generated script does not contain the command.
- If multiple templates are selected, you must set the parameters for each template.

----End

Follow-up Procedure

1. Click the **Scripts** tab.
2. Choose the NE to which the template is applied from the **NE List** navigation tree. The created script is displayed under the NE node. The name of the script is the same as the name of the applied template.

9.5.3.3 Exporting Templates

This topic describes how to export templates. The tool supports the exporting and backup of all templates for follow-up template modification or for reference.

Context

You can choose to export some templates or all templates as required.

Procedure

- To export some templates, do as follows:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Templates** tab.
  3. Choose **Template List** from the navigation tree. All templates are displayed in the right pane.

4. Hold down **Ctrl** while selecting the templates to be exported. Right-click these templates and choose **Export Template** from the shortcut menu.
5. In the dialog box that is displayed, click the **Save File** option button, and click **OK**.

   NOTE

   - If the FireFox is used, the exported file is saved to **C:\Documents and Settings\osuser\My Documents\Downloads** by default. **osuser** indicates the user name for logging in to the OS. To change the path, do as follows:
     1. Choose **Tools** > **Options** from the main menu of the FireFox.
     2. In the **Downloads** area, click **Browse** and set the path.
   - If the Internet Explorer is used, the **Save As** dialog box is displayed. Select the path for saving the exported file.

- To export all templates, do as follows:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Templates** tab.
  3. Choose **Template List** from the navigation tree. All templates are displayed in the right pane.
  4. Select a template.
  5. Click **Export All Templates**.
  6. In the dialog box that is displayed, click the **Save File** option button, and click **OK**.

     NOTE

     - If the FireFox is used, the exported file is saved to **C:\Documents and Settings\osuser\My Documents\Downloads** by default. **osuser** indicates the user name for logging in to the OS. To change the path, do as follows:
       1. Choose **Tools** > **Options** from the main menu of the FireFox.
       2. In the **Downloads** area, click **Browse** and set the path.
     - If the Internet Explorer is used, the **Save As** dialog box is displayed. Select the path for saving the exported file.

----End

9.5.3.4 Importing a Template

This topic describes how to import a template. The template can be either a customized one or a universal one provided by the SCT.

Prerequisite

The template to be imported must be available.

Procedure

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

Step 2 Click the **Templates** tab.

Step 3 **Optional:** In the **Templates** navigation tree, right-click the **Templates** node and choose **Create Folder** from the shortcut menu.

Step 4 **Optional:** In the **Create folder** dialog box, enter a folder name, and click **OK**.

Step 5 Select the **Templates** node or the new folder, right-click, and choose **Import Template** from the shortcut menu.

Step 6 In the dialog box that is displayed, click **Browse**, and then select the template to be imported.

Step 7 Click **Import**. The imported template is displayed in the navigation tree.

----End

9.5.4 Maintaining Scripts

This topic describes how to maintain scripts.

9.5.4.1 Creating a Script Manually

This topic describes how to create a script that contains NE configurations. A script can be created manually or by using a template.

Prerequisite

NEs must be added to the SCT. For details about how to add NEs, see Synchronizing NE Configurations to the eSight.

Context

You can create a script in any of the following methods. This topic focuses on the method of creating a script manually.

- Create a script manually.

  Enter commands to create a script manually.

  NOTE

  If a large number of commands are required for script creation, creating several scripts is recommended, with each script containing no more than 200 commands. This is to ensure the efficiency of script verification and deployment.

- Create a script by using a template.

  The template to be used can be either universal or customized. For details, see **9.5.3.2 Applying a Template**.

- Create a script by importing the planning table.

  You can use existing templates to generate a planning table. After you set parameters in the planning table and import the planning table, the SCT automatically generates a script based on planning information. For details, see **9.4.4 Importing Planning Data**.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 In the **NE List** navigation tree, select the NE for which the script needs to be created, right-click, and then choose **Create Script** from the shortcut menu.

Step 4 In the **Create Script** dialog box, set **Script Name** and **Description**, and click **OK**.

The created script is displayed under the NE node.

Step 5 In the **Script Configuration** area, click to modify the script.

Step 6 Enter commands in the blank area.

After entering a command keyword in the query box, click or press **Enter** to query commands related to the command keyword.

Step 7 Click to save the commands.

All commands are displayed in colors and view commands are displayed in bold.

NOTE

If characters in the script are displayed in black after you click to save the commands, it indicates that the type and version of the NE have not been set. In this case, you must obtain the command set. For details, see **9.4.1 Obtaining Command Sets**.

Step 8 **Optional:** Incorrect commands are displayed in red. Modify the incorrect commands, and click to save the new configurations.

TIP

If incorrect commands are displayed after the script has been saved, see **9.4.5 Verifying a Script** to correct them.

----End

9.5.4.2 Modifying a Script

This topic describes how to modify a script of an NE.

Prerequisite

The script must exist on the NE.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 Choose **NE List** from the navigation tree. Then, select the script to be modified under an NE node.

Step 4 Click in the right pane to modify the script.

Step 5 Modify the commands in the script as required.

Step 6 Click **Save**.

----End

9.5.4.3 Exporting Scripts

This topic describes how to export scripts. You can use the tool to export NE scripts. The exported scripts can be used for follow-up script verification or fault location, and provide reference for the configuration of other NEs.

Context

You can choose to export some scripts or all scripts as required.

Procedure

- To export some scripts, do as follows:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Scripts** tab.
  3. Choose **NE List** from the navigation tree. Then, click the NE whose scripts need to be exported. All scripts of the NE are displayed in the right pane.
  4. Hold down **Ctrl** while selecting the scripts to be exported. Right-click these scripts and choose **Export Script** from the shortcut menu.
  5. In the dialog box that is displayed, click the **Save File** option button, and click **OK**.

     NOTE

     - If the FireFox is used, the exported file is saved to **C:\Documents and Settings\osuser\My Documents\Downloads** by default. **osuser** indicates the user name for logging in to the OS. To change the path, do as follows:
       1. Choose **Tools** > **Options** from the main menu of the FireFox.
       2. In the **Downloads** area, click **Browse** and set the path.
     - If the Internet Explorer is used, the **Save As** dialog box is displayed. Select the path for saving the exported file.
- To export scripts of all NEs, do as follows:
  1. Choose **Maintenance** > **Smart Configuration Tool** from the main menu.
  2. Click the **Scripts** tab.
  3. Choose **NE List** from the navigation tree. Then, select any of the NEs whose scripts need to be exported. All scripts of the NE are displayed in the right pane.
  4. **Optional:** Select **All** from the **Attribute** drop-down list. Then, click **Query**.
  5. Click **Export All Scripts**.
  6. In the dialog box that is displayed, click the **Save File** option button, and click **OK**.

     NOTE

     - If the FireFox is used, the exported file is saved to **C:\Documents and Settings\osuser\My Documents\Downloads** by default. **osuser** indicates the user name for logging in to the OS. To change the path, do as follows:
       1. Choose **Tools** > **Options** from the main menu of the FireFox.
       2. In the **Downloads** area, click **Browse** and set the path.
     - If the Internet Explorer is used, the **Save As** dialog box is displayed. Select the path for saving the exported file.

----End

9.5.4.4 Importing Scripts

This topic describes how to import scripts. You can use the tool to import the scripts of other NEs to the target NE. If the methods of configuring different NEs are similar, this function greatly improves the efficiency of making scripts.

Context

You can import scripts for one NE or multiple NEs as needed. The SCT supports the import of scripts in .zip or .txt format.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 Choose **NE List** from the navigation tree. All NEs are displayed in the right pane.

Step 4 Select one or more NEs for which scripts need to be imported, right-click, and then choose **Import Script** from the shortcut menu.

Step 5 In the dialog box that is displayed, click **Browse** to choose the scripts to be imported.

Step 6 Click **Import**. Associated scripts are displayed on each NE node.

----End

9.5.4.5 Deploying a Script in a Scheduled Manner

This topic describes how to create a scheduled task to deploy a script. A script can be deployed only once, or on a daily, weekly, or monthly basis.

Prerequisite

An NE must be created or imported.

Procedure

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

Step 2 Click the **Scripts** tab.

Step 3 Select the **NE List** node, right-click, and then choose **Scheduled Deployment** from the shortcut menu.

Step 4 In the dialog box that is displayed, click **Add**.

Step 5 In the **Create Deployment Task** dialog box, click  or  to add the required NE to the list of selected NEs.

Step 6 Click **Next**.

Step 7 Specify the script to be deployed in a scheduled manner. Then, click **Next**.

NOTE

The script will be automatically deployed in a scheduled manner. Do not enter any MML command.

Step 8 Set the following parameters for the scheduled task:

- Name for Scheduled Task
- Log Subfolder
- Vendor

- Remarks
- Period
- Deployment Date, Deployment Frequency, and Start Time

Step 9 Click **Finish**.

Step 10 A record about the scheduled task is displayed in the **Manage Scheduled Deployment Task** dialog box.

----End

Follow-up Procedure

After creating scheduled tasks, perform the following operations as required:

- Modify a scheduled task.
  1. In the **Manage Scheduled Deployment Task** dialog box, select the scheduled task to be modified, right-click, and then choose **Modify Task** from the shortcut menu.
  2. After modifying the task, click **Finish**.
- Download logs related to a scheduled task.
  1. In the **Manage Scheduled Deployment Task** dialog box, select the scheduled task whose logs need to be downloaded, right-click, and then choose **Download Log** from the shortcut menu.
  2. In the dialog box that is displayed, select the time range for generating logs. Then, click **OK**.
  3. In the dialog box that is displayed, click **Save File**, and click **OK**.
- Delete logs related to a scheduled task.
  1. In the **Manage Scheduled Deployment Task** dialog box, select the scheduled task whose logs need to be deleted, right-click, and then choose **Clear Log** from the shortcut menu.
  2. In the dialog box that is displayed, select the time range for generating logs. Then, click **OK**.
  3. In the dialog box that is displayed, click **OK**. Logs related to the scheduled task are deleted from the server.

10 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.

10.1 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.

Configuration File Backup

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.

Configuration File Restore

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.

10.2 Setting FTP Parameters

Before backing up or restoring a device configuration file, ensure that FTP parameters are set correctly. If they are set incorrectly, you cannot transfer files between NEs and eSight properly.

Context

NOTE

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.

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

10.3 Setting the Maximum Number of Backup NE Configuration Files

You must set the maximum number of backup NE configuration files to avoid excessive space usage.

Context

When the number of backup NE configuration files reaches the maximum, eSight deletes the earliest backup NE configuration files by default.

Procedure

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

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

Step 3 Set **Max. backup files** and click **Apply**.

----End

10.4 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.

10.4.1 Backing Up NE Configuration Files Automatically

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

10.4.1.1 Creating a Backup Task

You can create a backup task for a type of NEs.

Prerequisite

eSight communicates with NEs normally.

The FTP service is configured and started. For details on how to configure the FTP service, see **10.2 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.

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

10.4.1.2 Enabling a Backup Task

When a configuration file backup task is disabled, you must enable the backup task for execution.

Prerequisite

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

10.4.1.3 Maintaining a Backup Task

You can browse and maintain a backup task as required.

Prerequisite

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

10.4.2 Backing Up NE Configuration Files Manually

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

Prerequisite

eSight communicates with NEs normally.

The FTP service is configured and started. For details on how to configure the FTP service, see **10.2 Setting FTP Parameters**.

For the user-defined device, the Telnet parameters on eSight and the NE are set to be the same.

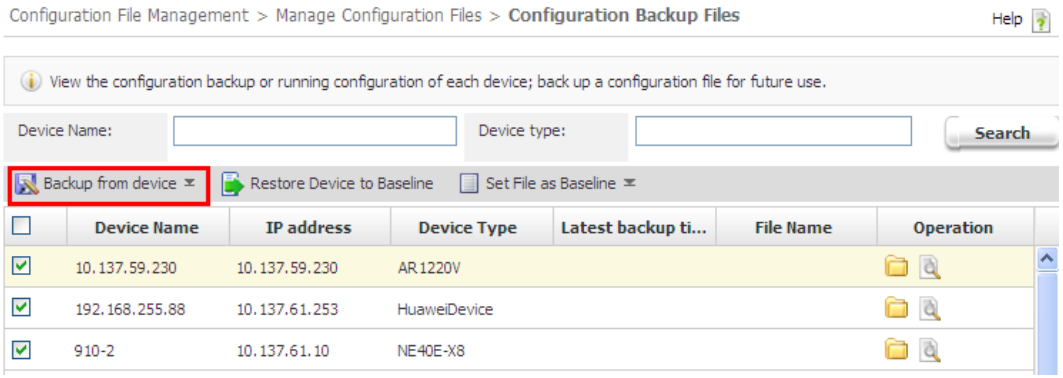
SNMP write permission is set.

Procedure

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

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

Step 3 Select a device and click **Backup from device**.



----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.

10.5 Managing NE Configuration Files

This topic describes common operations for managing NE configuration files.

10.5.1 Viewing an NE Configuration File

This topic describes how to view a backup NE configuration file and a configuration file that is in use.

Prerequisite

A backup file is in .cfg format.

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 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

10.5.2 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

10.5.3 Comparing NE Configuration Files

You can know differences between NE configuration files by comparing them.

Prerequisite

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

----End

10.5.4 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.

Prerequisite

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

10.5.5 Restoring NE Configuration Files

When an NE is faulty, you can upload an NE configuration file to the NE to restore NE configuration data.

Prerequisite

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

----End

11 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.

11.1 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 third-party devices on panels. You can perform the operations such as activating an interface, deactivating an interface, and querying alarm information on panels.

Alarm Management

eSight parses standard alarms reported by user-defined devices by default. You need to customize private alarm parameters for private alarms reported by user-defined devices by using the provided customization tool. eSight parses private alarms based on the private alarm parameters.

Resource Management

eSight supports operations based on the standard MIB. eSight also provides the functions such as managing interfaces, querying and modifying basic information about devices, and querying

IP address table (IPv4), IP routing table, and entity data based on the RFC1213. You can customize basic information about the device manufacturer, logo, and device model.

11.2 User-defined Devices' Functions

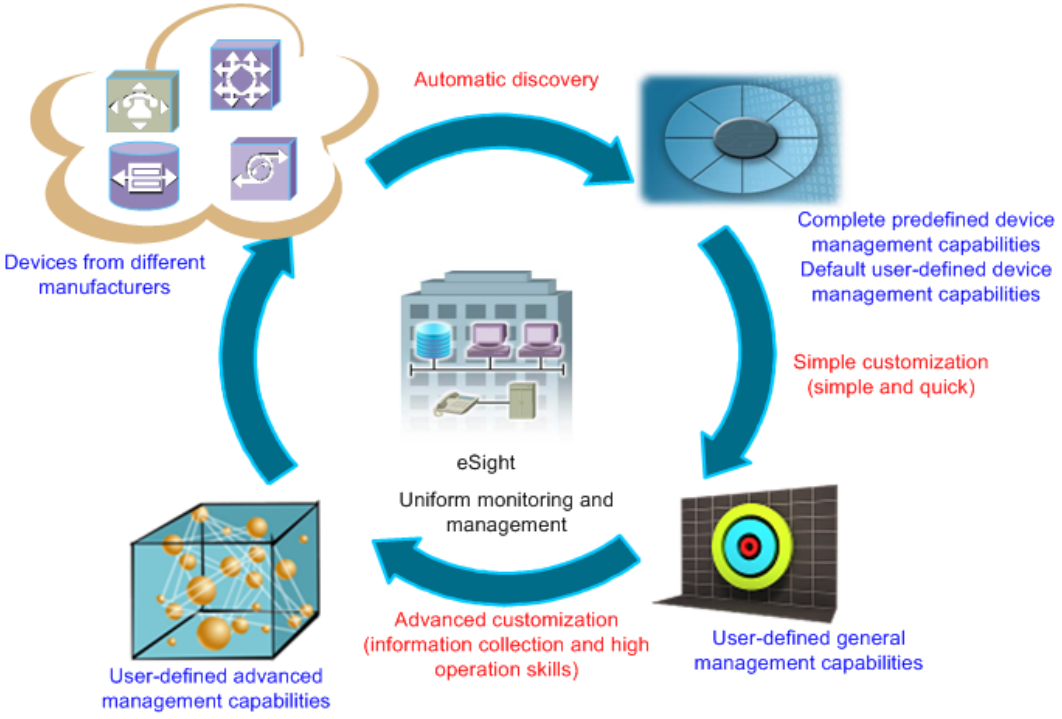
eSight provides a management platform, allowing you to add devices supporting SNMP to eSight. eSight provides complete management capabilities for pre-integrated devices. You can customize user-defined devices (devices of the **Huawei Device**, **H3C Device**, **Cisco Device**, and **Unknown** types) 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.

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
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. (The displayed operation result may differ from the actual result.)

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 Customizing the	● Manufacturer name (Only **Unknown** is available.) ● NE type ● NE category	Unknown
Interface manager			Unknown
Telnet parameters			Unknown

Customization Item	Description	Information to Collect	Application Scope
Topology icon	Manufacturer Name and Device Type.		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 **11.5.1 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
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 **11.5.2 Customizing Performance Indicators**.	● 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.

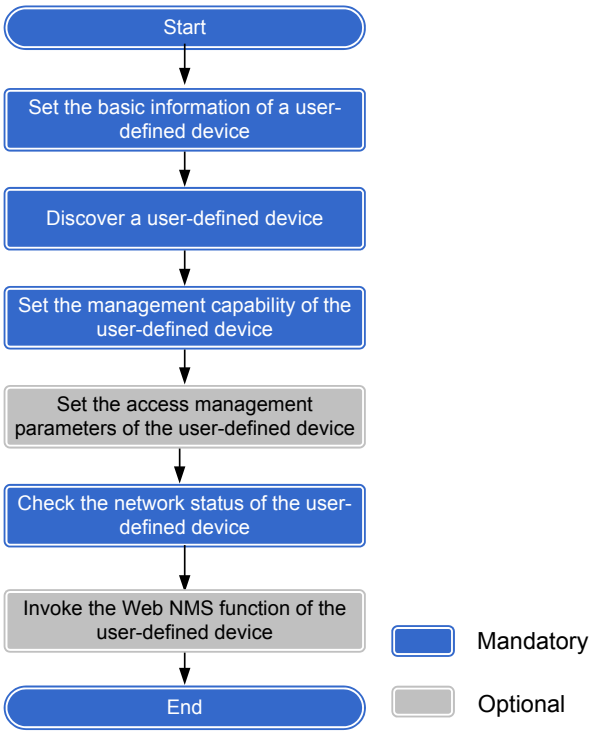
Customization Item	Description	Information to Collect	Application Scope
Configuration backup files	Devices only of the **Unknown** type need customization. After customizing a device, you can back up and restore the device's configuration file. (The displayed operation result may differ from the actual result.) Workload: 0.2 person/day For details, see **11.5.3 Customizing a Device Configuration File**.	● Backup command ● Restore command ● Restart command **NOTE** Obtain the preceding information from the manufacturer.	Unknown
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 **11.5.4 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

11.3 User-defined Device Management Process

This topic describes the user-defined device management process.

Figure 11-1 shows the user-defined device management process.

Figure 11-1 User-defined device management process



Operation	Remarks
1. **11.4 Setting the Basic Information of User-Defined Devices**	Configure manufacturer and type information about user-defined devices.
2.**3.1.1.2 Creating an NE**	Upload user-defined devices to eSight so that eSight can manage the devices.
3.**11.5 Setting the Management Capability of User-defined Devices**	Customize the alarm parameters, performance counters, configuration files, and NE panels of user-defined devices as required.
4. (Optional) **7.3.2 Setting Protocol Parameters**	Ensure that the SNMP parameter settings and Telnet parameter settings on user-defined devices are the same as those on eSight so that eSight can manage the user-defined devices.
5. **11.6 Checking the Network Status of User-Defined Devices**	Check the network status of user-defined devices periodically to obtain the status of communication between eSight and user-defined devices in real time.
6. (Optional) **11.7 Invoking the Web NMS of User-Defined Devices**	Invoke the Web management page of each user-defined device to perform related configuration operations.

11.4 Setting the Basic Information of User-Defined Devices

This topic describes the manufacturer and type information on the user-defined devices.

11.4.1 Customizing Basic Vendor Information

Set the vendor information on the customized devices so that you can easily distribute a customized device to a vendor.

Procedure

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

Step 2 In the navigation tree on the left, choose **Basic NE Information** > **Vendor Information** and click **Create**.

Step 3 Set the basic vendor information on the user-defined devices and click **OK**.

Step 4 **Optional:** In **Vendor Information**, view the vendor information on the customized device and click  to modify related information as required.

----End

11.4.2 Customizing Device Type Information

After customizing the manufacturer information on the user-defined devices, you must set the device type.

Procedure

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

Step 2 In the navigation tree on the left, choose **Basic NE Information** > **NE Type Information** and click **Create**.

Step 3 Set the device type information and click **OK**.

Step 4 **Optional:** In **NE Type Information**, view the type information on the user-defined device and click  to modify related information as required.

----End

11.5 Setting the Management Capability of User-defined Devices

Set the alarms, performance indicators, configuration files, and performance panels of user-defined devices as required.

11.5.1 Customizing SNMP Alarm Parameters

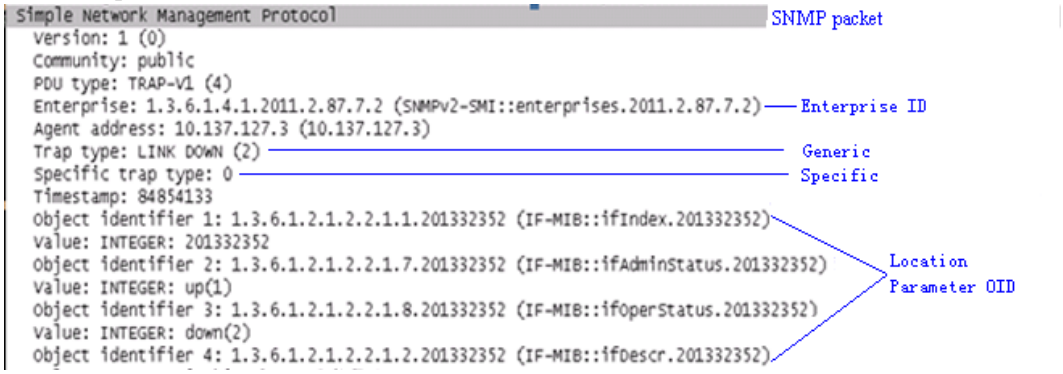
You can customize SNMP alarm parameters on eSight so that third-party devices will report SNMP alarms to eSight.

Context

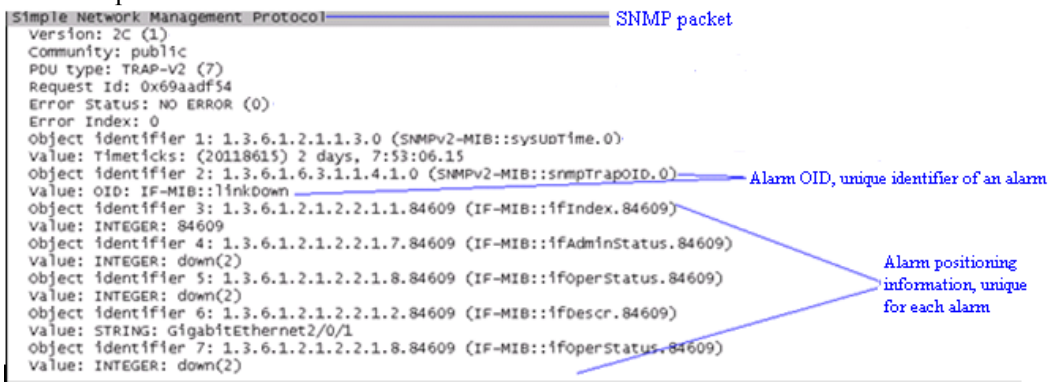
You must obtain alarms' trap IDs and MIB node information for locating alarm parameters from the manufacturer.

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:

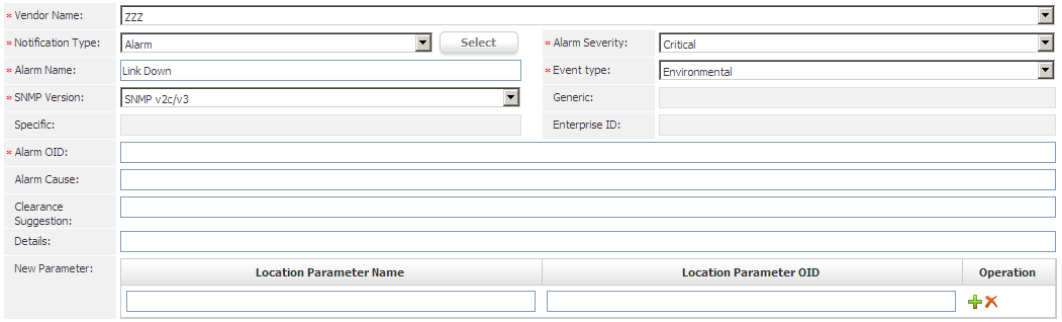


Procedure

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**.

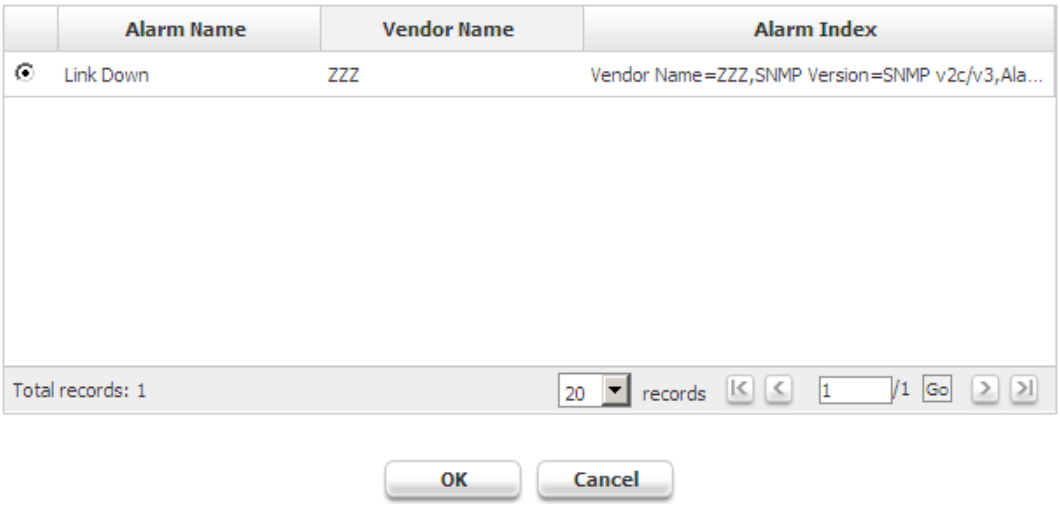
Step 3 Click **Create**, set user-defined alarm parameters on the **Create Alarm Type** tab page, and click **OK**.



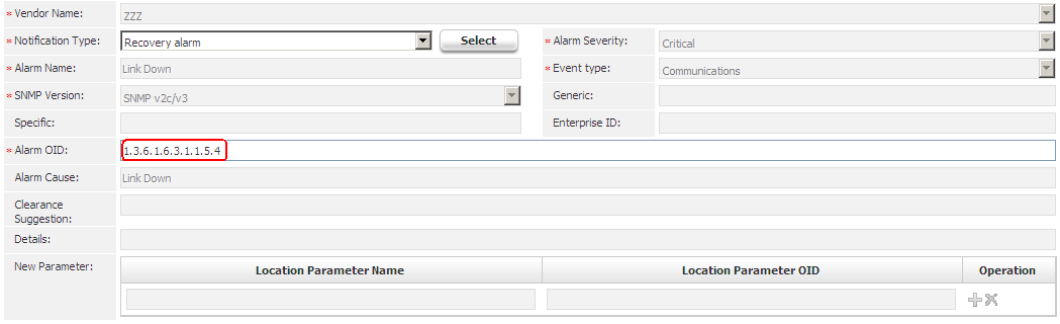
Parameter		Description
SNMP Version		SNMP versions supported by eSight, including SNMPv1, SNMPv2c, and SNMPv3. ● Set the alarm OID for devices supporting SNMPv2c or SNMPv3. ● For devices supporting SNMPv1, set **Generic**, **Specific**, and **Enterprise ID**.
Generic		The combination of **Generic**, **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 clear alarms.

1. Click **Create**. On the **Create Alarm Type** tab page, set **Notification Type** to **Recovery Alarm**.
2. Click **Select**, select an alarm, and click **OK**.



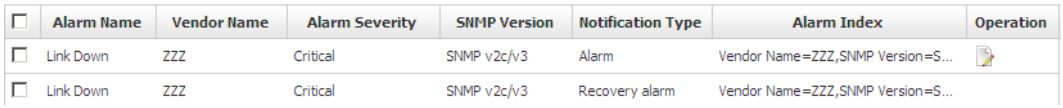
3. Set the alarm OID for clear alarms only. Then click **OK**.



----End

Follow-up Procedure

In the **Alarm Type** window, you can view user-defined alarm information.



11.5.2 Customizing Performance Indicators

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

Context

- User-defined device performance indicator group: contains performance indicators of devices, for example, device temperature. The monitoring object is each device.
- User-defined interface performance indicator group: contains performance indicators of interfaces, for example, interface traffic. The monitoring object is interface.
- Group of performance indicators without specified monitoring objects: indicates private performance indicators of devices from different manufacturers. After customizing a performance indicator, you must specify the monitoring object for it.

You must obtain the user-defined performance indicator MIB information from manufacturers.

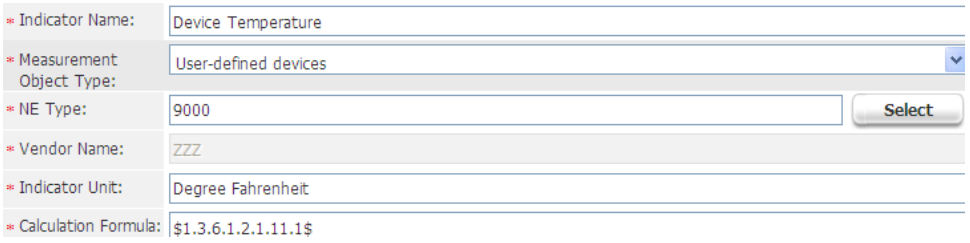
Procedure

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 indicators whose monitoring objects are unspecified.

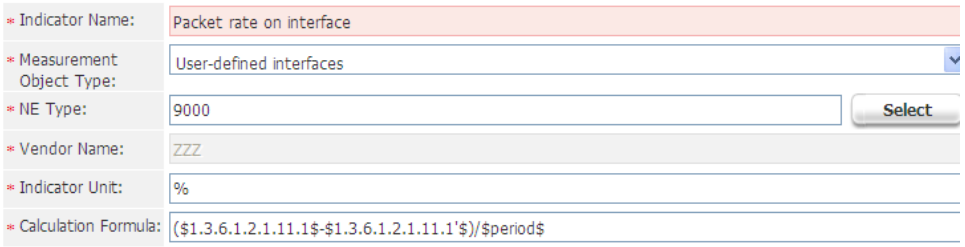
1. Create user-defined device indicators. Click **Create**, set device performance indicator parameters on the **Create Performance Indicator** tab page, and click **OK**.



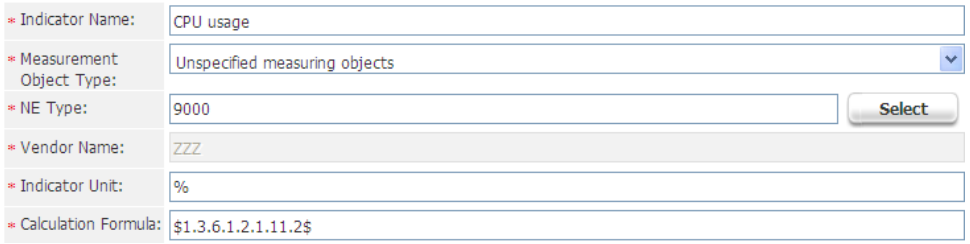
NOTE

Set **Calculation Formula** of a device performance indicator to *MIB ID* followed by **.0**.

2. Create user-defined interface indicators. Click **Create**, set interface performance indicator parameters on the **Create Performance Indicator** tab page, and click **OK**.

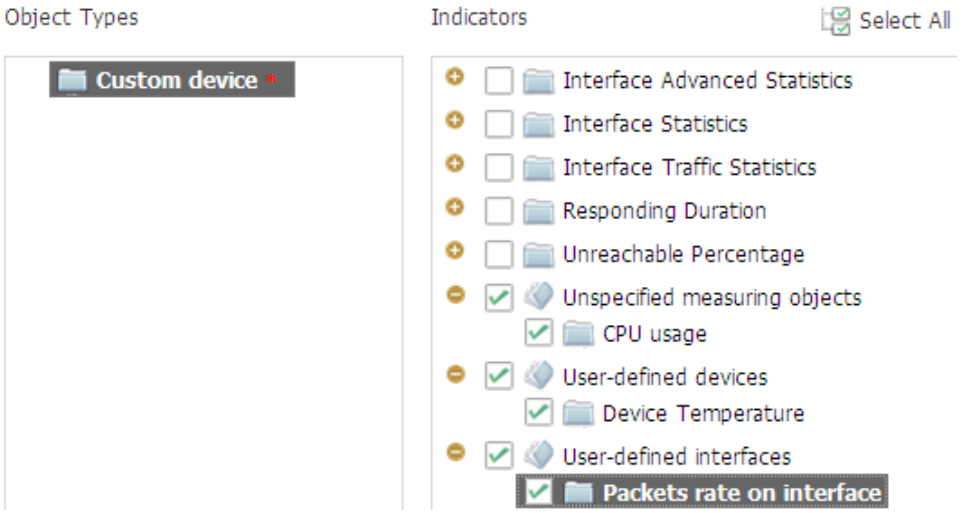


3. Create object indicators whose monitoring objects are unspecified. Click **Create**, set object performance indicator parameters on the **Create Performance Indicator** tab page, and click **OK**.

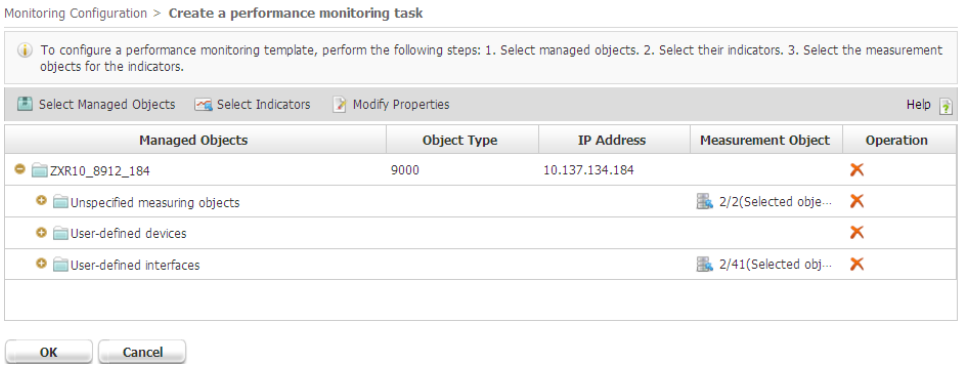


Step 4 Create a performance monitoring instance.

1. On the main menu, choose **Performance** > **Monitoring Configuration**, and click **Create**.
2. Click **Select Managed Objects** and select a user-defined device.
3. Click **Select Indicators**, select user-defined device performance indicators, and click **OK**.

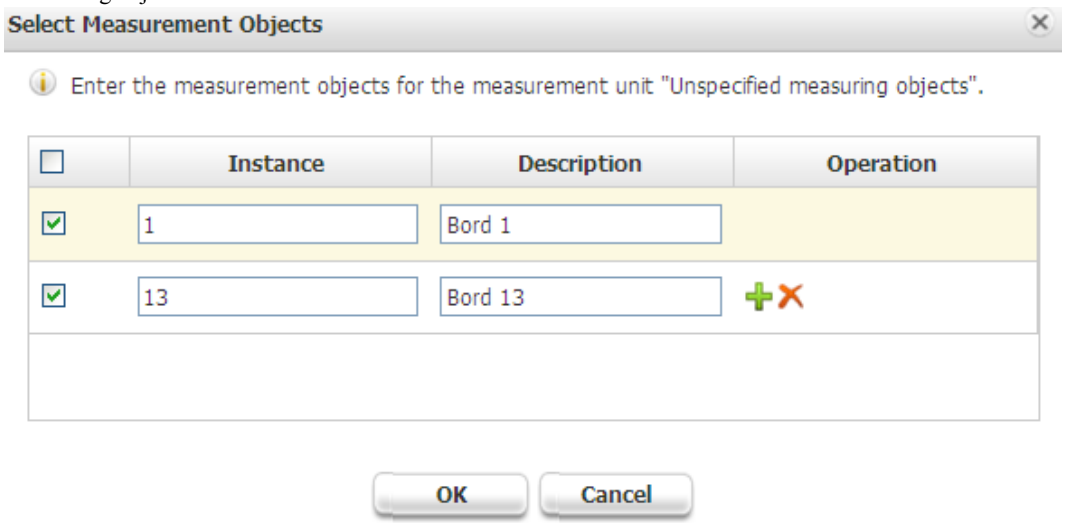


4. Click on the right of **Unspecified measuring objects** and **User-defined interfaces**, set a measurement object, and click **OK**.



NOTE

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

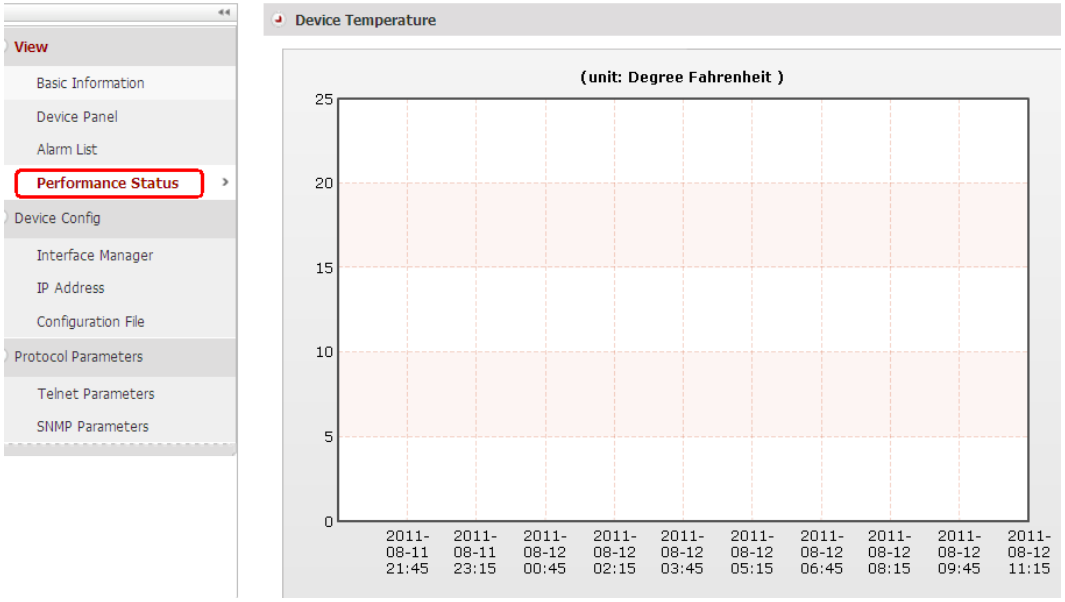


5. Click **OK**. In the **Operation Results** dialog box displaying the operation success message, click **Complete**.

----End

Follow-up Procedure

You can view the user-defined performance status in the NE manager.



11.5.3 Customizing a Device Configuration File

You must customize restart commands and commands for backing up and restoring configuration files for devices from different manufacturers as required.

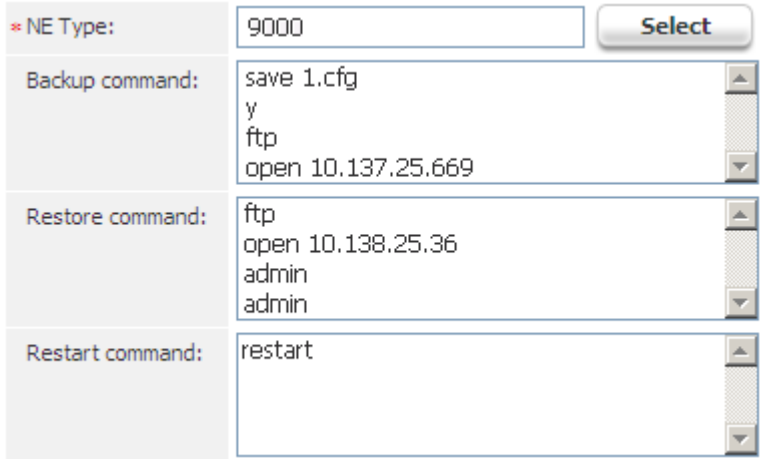
Procedure

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 then 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.

----End

11.5.4 Customizing the Device Panel

You can upload a device panel photo or draw a device panel on eSight to customize the device panel. This topic describes how to upload a device panel photo to customize the device panel.

Context

- When customizing the device panel in the NE manager, you do not need to collect devices' **vendortype** or start indexes.
- Devices of the **Unknown** type have default device panels and do not support customization.

Procedure

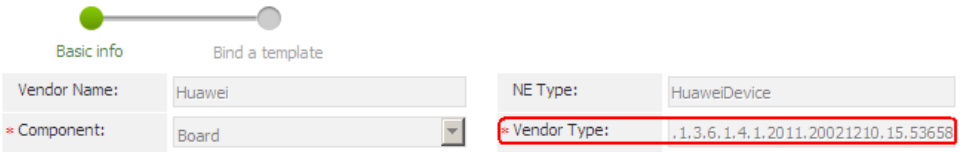
Step 1 Choose **Resource** > **Resource Management** from the main menu. On the NE list, click **Name** of an NE and click **Manage**. The NE manager is displayed.

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

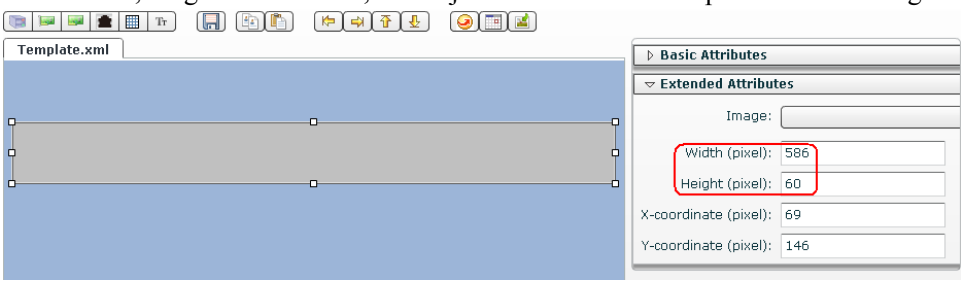
Step 3 Customize a shelf.

1. Right-click a shelf and choose **Customize Template**.

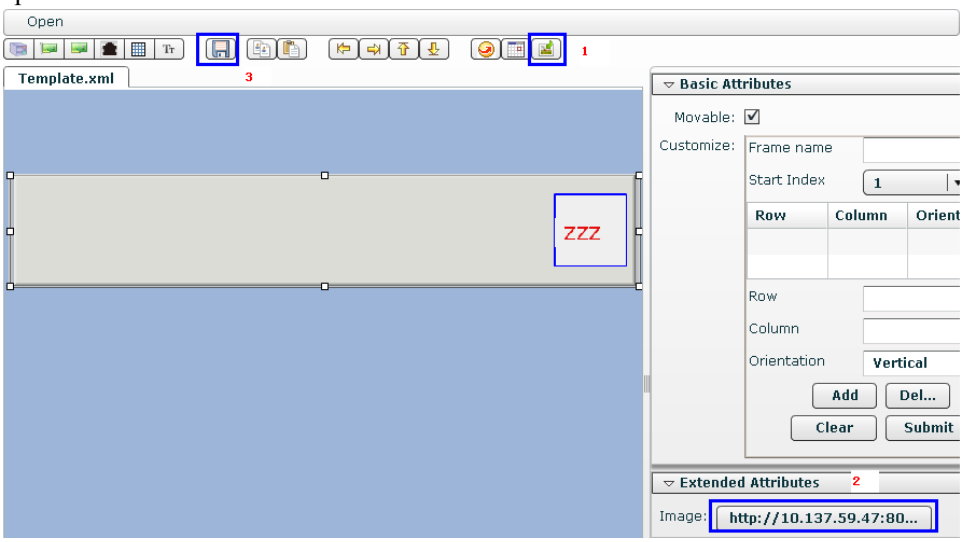
2. Click **Next**. (eSight automatically matches the shelf type with the shelf model.)



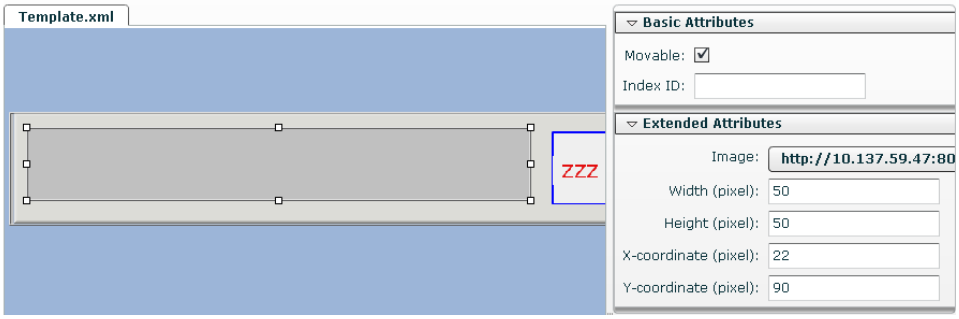
3. Click **Create Template**. On the menu bar in the **Template Customize** window, select the slot icon, drag it to the editor, and adjust the slot size to adapt to the shelf image.



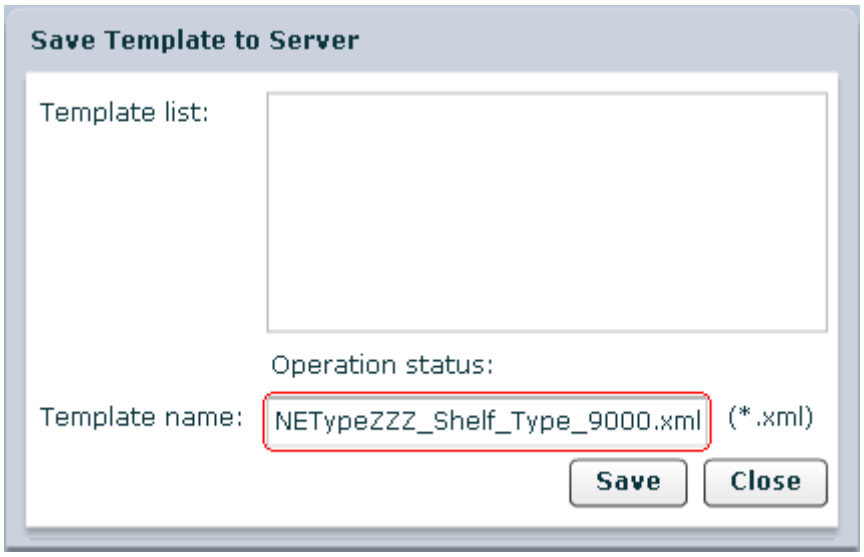
4. Select the shelf icon and drag it to the slot created in **Step 3.3**.
5. Click to upload the shelf image. In **Extended Attributes**, select the image that you uploaded.



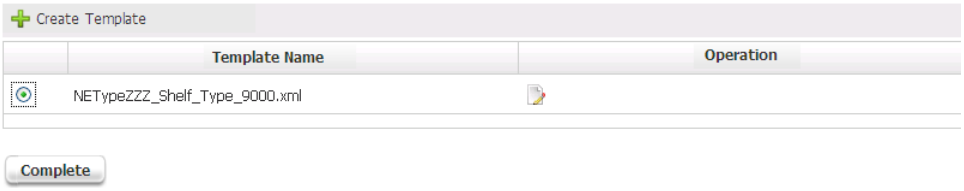
6. Set the slots on the shelf as required. Each board maps a slot. Drag the slot icon on the menu bar to the shelf. Set the slot size and **Index ID**.



7. Click , enter the shelf template name in the dialog box that is displayed, and click **Save**.



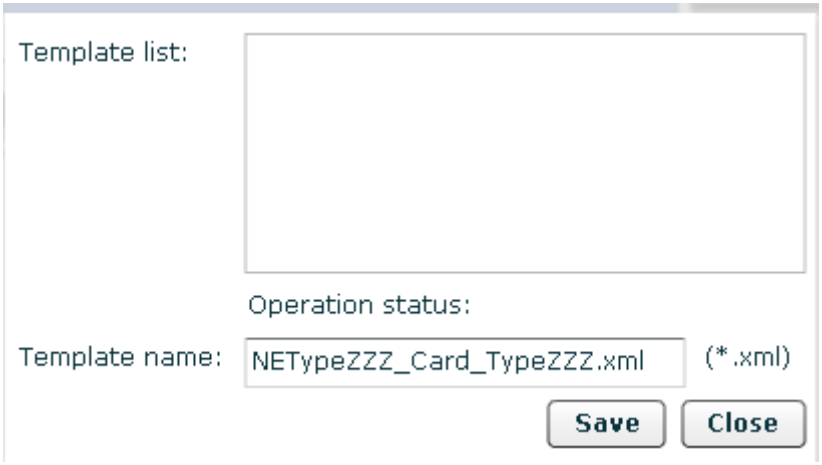
8. Click **Back** at the upper right corner, select the saved shelf template, and click **Complete**.



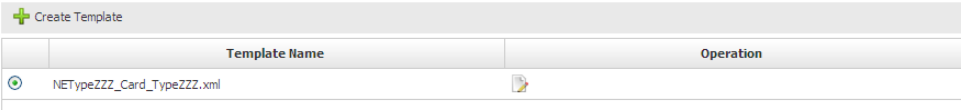
Step 4 Customize a board.

1. On the device panel tab page in the NE manager, right-click a board, and choose **Customize Template**.
2. Click **Next**. (eSight automatically matches the board type with the board model.)
3. Click **Create Template**. On the menu bar in the **Template Customize** window, select the slot icon, drag it to the editor, and adjust the slot size to adapt to the board image.
4. Select the board icon and drag it to the slot created in **Step 4.3**.
5. Click to upload the shelf image. In **Extended Attributes**, select the image that you uploaded and set the number of ports.

   To enable the order of ports on the board to be the same as that on the physical device, drag to the board, set the slot size and **Index ID**, and then rearrange the ports on the board.
6. Click , enter the board template name in the dialog box that is displayed, and click **Save**.



7. Click **Back** at the upper right corner, select the saved board template and click **Complete**.

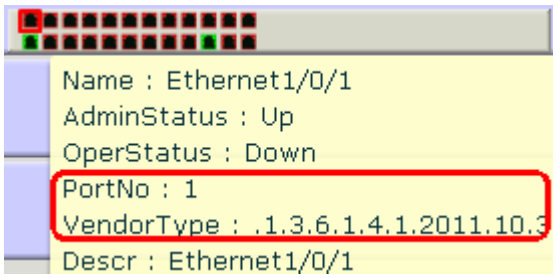


Step 5 Customize a port template.

1. On the device panel tab page in the NE manager, right-click a port, and choose **Customize Template**.

   NOTE

   Move the cursor to the port, the tooltip **Vendor Type** is displayed. You must set different port templates for ports with different **Vendor Type** values.



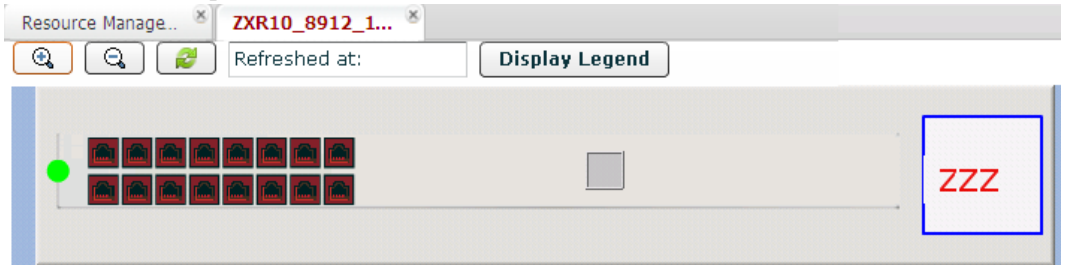
2. Click **Next**. (eSight automatically matches the port type with the port model.)
3. Click **Create Template**. On the menu bar in the **Template Customize** window, select the slot icon, drag it to the editor, and adjust the slot size to adapt to the port image.
4. Select the port icon and drag it to the slot created in **Step 5.3**.
5. Click to upload the port image. In **Extended Attributes**, select the image that you uploaded.

6. Click , enter the port template name in the dialog box that is displayed, and click **Save**.
7. Click **Back** at the upper right corner, select the saved port template, and click **Complete**.

----End

Follow-up Procedure

To verify the device panel customization, click **View** > **Device Panel** in the NE manager to refresh the device panel.



11.6 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.

11.6.1 Performing a Ping Test

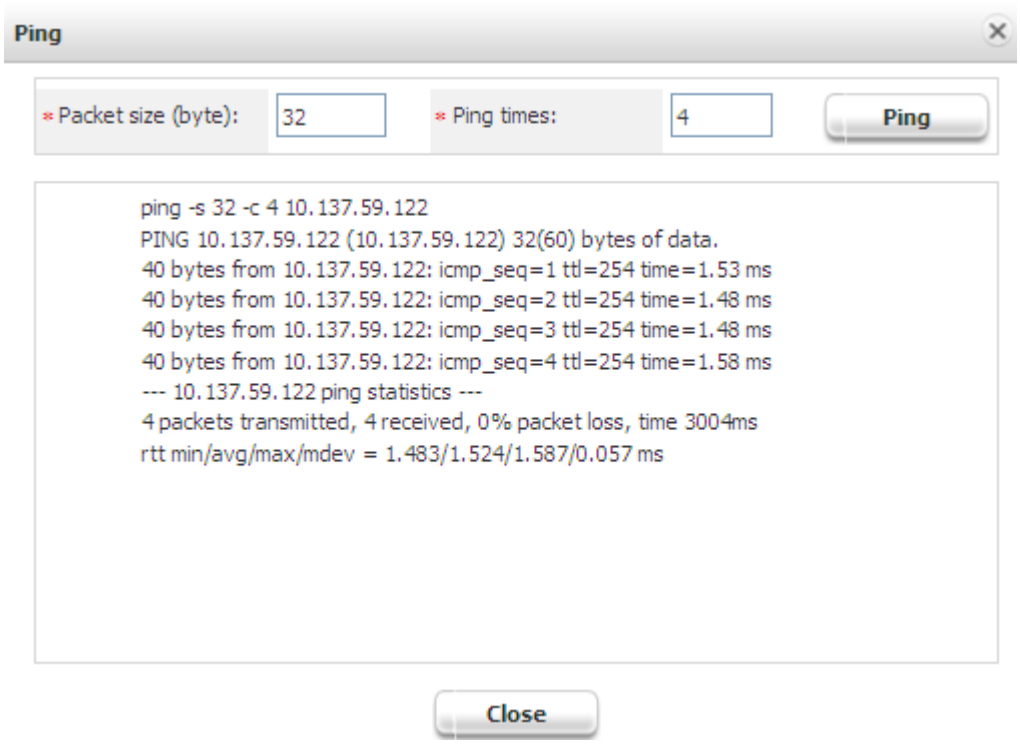
Perform a Ping test on a user-defined device in the NE manager to check the communication status of eSight and the device.

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

11.6.2 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

11.6.3 Query Basic Interface Information

eSight supports query of information on an 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** > **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

11.6.4 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, click **View Details** to 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

11.7 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.

Prerequisite

The type of devices is customized.

The user-defined device supports the Web NMS and the Web NMS has been configured when you customize the NE type on eSight.

Context

NOTE

Huawei frame-type switches and routers do not support the Web NMS function and services of the devices must be configured by using the smart configuration tool.

Procedure

Step 1 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

12 System Management

About This Chapter

12.1 System Configuration
After the eSight is installed, you need to configure it for proper running.

12.2 Log Management
A log records the operations and major events of the eSight. You can query the log information using the log management function.

12.3 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.

12.4 License Management
You have permission for the eSight only after obtaining a license. The license controls the resources and functions of the eSight.

12.5 Backing Up and Restoring the Database
To ensure eSight database security, you must back up and restore the database in time.

12.1 System Configuration

After the eSight is installed, you need to configure it for proper running.

12.1.1 Configuring Log Overflow Dump

The eSight provides log overflow dump to avoid insufficient database tablespace. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the data to a specified folder.

Context

If the tablespace usage exceeds the specified database space threshold, a data overflow occurs.

The eSight checks the log tablespace usage in the database at a specific time of day. If the usage exceeds the threshold, the eSight always dumps the logs (including security logs, operation logs, and system logs) recorded within the earliest month to the specified path in order according to the recording time of the logs, and then deletes the dumped logs starting from the earliest until the usage is less than the threshold. After dumping, the eSight also checks whether the total size and retention period of the files in the dump directory exceed the specified values. If they exceed the specified values, the eSight deletes the earliest dumped files until the total size and retention period become less than the specified values.

Procedure

Step 1 Choose **System** > **System Configuration**.

Step 2 In the left navigation tree, choose **Database Overflow Dump** > **Log Database Dump**.

Step 3 Set log dump parameters.

NOTE

Dump path can be an absolute path or a relative path. The relative path is relative to the OMS installation path **%ENT_ROOT%/run/dump** (on Windows). If you specify **Dump path** to **AAA**, the file is saved to **%ENT_ROOT%/run/dump/AAA**.

Step 4 Click **Apply**.

----End

12.1.2 Configuring Alarm Overflow Dump

The eSight provides alarm overflow dump to avoid insufficient database tablespace. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the data to a specified folder.

Context

If the tablespace usage exceeds the specified database space threshold, a data overflow occurs.

The eSight checks the alarm management tablespace usage in the database at a specific time of day. If the usage exceeds the threshold, the eSight always dumps the alarms (including historical alarms, masked cleared alarms, and events) reported within the earliest month to the specified

path in order according to the reporting time of the alarms, and then deletes the dumped alarms starting with the earliest until the usage is less than the threshold. After dumping, the eSight also checks whether the total size and retention period of the files in the dump directory exceed the specified values. If they exceed the specified values, the eSight deletes the earliest dumped files until the total size and retention period become less than the specified values.

Procedure

Step 1 Choose **System** > **System Configuration**.

Step 2 In the left navigation tree, choose **Database Overflow Dump** > **Alarm Database Dump**.

Step 3 Set alarm dump parameters.

NOTE

Dump path can be an absolute path or a relative path. The relative path is relative to the OMS installation path **%ENT_ROOT%/run/dump** (on Windows). If you specify **Dump path** to **AAA**, the file is saved to **%ENT_ROOT%/run/dump/AAA**.

Step 4 Click **Apply**.

----End

12.1.3 Configuring Performance Overflow Dump

The eSight provides performance overflow dump to avoid insufficient tablespace of the database. If the eSight detects that the tablespace usage exceeds the specified database space threshold, the eSight automatically dumps the data to a specified folder.

Context

If the tablespace usage exceeds the specified database space threshold, a data overflow occurs.

The eSight checks the performance management tablespace usage in the database at a specific time of day. If the usage exceeds the threshold, the eSight always dumps the performance data collected within the earliest month to the specified path in order according to the collecting time of the data, and then deletes the dumped data starting from the earliest until the usage is less than the threshold. After dumping, the eSight also checks whether the total size and retention period of the files in the dump directory exceed the specified values. If they exceed the specified values, the eSight deletes the earliest dumped files until the total size and retention period become less than the specified values.

Procedure

Step 1 Choose **System** > **System Configuration**.

Step 2 In the left navigation tree, choose **Database Overflow Dump** > **Performance Database Dump**.

Step 3 Set performance dump parameters.

NOTE

Dump path can be an absolute path or a relative path. The relative path is relative to the OMS installation path **%ENT_ROOT%/run/dump** (on Windows). If you specify **Dump path** to **AAA**, the file is saved to **%ENT_ROOT%/run/dump/AAA**.

Step 4 Click **Apply**.

----End

12.2 Log Management

A log records the operations and major events of the eSight. You can query the log information using the log management function.

12.2.1 Logs

Logs of the eSight include operation logs, system logs, and security 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.

12.2.2 Querying Security Logs

You can query security logs to understand the information about eSight-related security operations.

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**.

Step 2 In the left navigation tree, choose **Query Logs** > **Security Logs**.

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

After clicking **Details**, you can query detailed information about the log.

----End

12.2.3 Querying System Logs

You can query system logs to understand the information about eSight operations.

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.
- You can view the operation logs of all users after login.

Procedure

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

Step 2 In the left navigation tree, choose **Query Logs** > **System Logs**.

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

After clicking **Details**, you can query detailed information about the log.

----End

12.2.4 Querying Operation Logs

You can query operation logs to understand the information about eSight user operations.

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.
- The user logs is succeed, queried all user operation logs.

Procedure

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

Step 2 In the left navigation tree, choose **Query Logs** > **Operation Logs**.

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

After clicking **Details**, you can query detailed information about the log.

If it is a batch operation, you can also click **Operation Log Details** to query the information of all the operation results.

----End

12.3 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.

12.3.1 Lower-Layer NMS Management

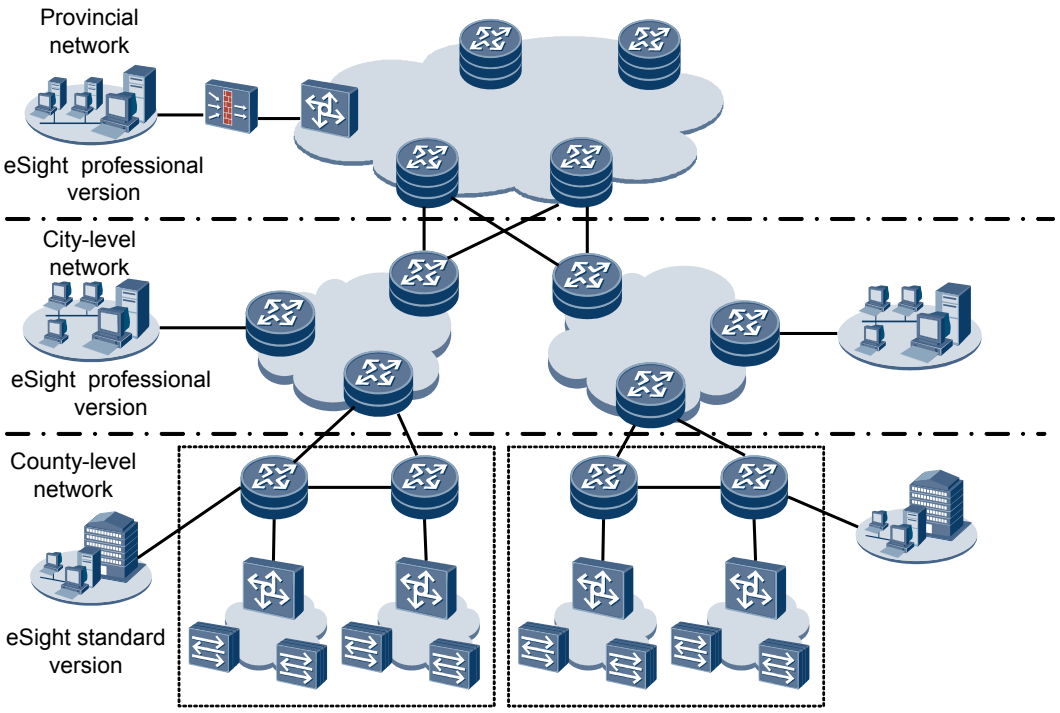
The hierarchical network management mechanism of eSight enables users to divide management areas and construct a layer-based management system based on the geographical area and organization structure. Upper-layer NMSs have higher rights than lower-layer NMSs. Upper-layer NMSs have rights to manage lower-layer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

12.3.1.1 Lower-Layer NMS Application

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

See **Figure 12-1**. 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 12-1 Lower-Layer NMS application



12.3.1.2 Lower-Layer NMS Function

This topic describes the basic functions of the hierarchical network management.

You can display a lower-layer NMS page on the upper-layer NMS page to view the alarms, topology, performance, and reports of the lower-layer NMS. You can implement all functions of a lower-layer NMS on the lower-layer NMS page. Upper-layer NMSs monitor only the connection status of lower-layer NMSs and can log in to lower-layer NMSs in SSO mode.

eSight provides the following functions for upper-layer NMSs to monitor lower-layer NMSs:

- Adding a lower-layer NMS

  You can add a lower-layer NMS so that the upper-layer NMS can monitor the lower-layer NMS.

- Displaying a lower-layer NMS page

  You can display a lower-layer NMS page on the upper-layer NMS page to view the alarms, topology, performance, and reports of the lower-layer NMS.

- Viewing the lower-layer NMS list

  You can view the list of lower-layer NMSs that are managed by an upper-layer NMS.

- Deleting a lower-layer NMS

  You can delete a lower-layer NMS as required.

12.3.2 Managing a Lower-Layer NMS

This topic describes how to manage a lower-layer NMS.

12.3.2.1 Adding a Lower-Layer NMS

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

Prerequisite

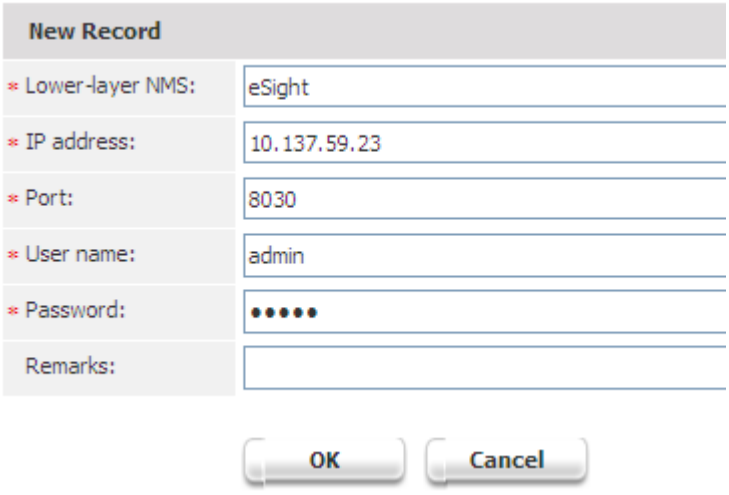
The lower-layer NMS runs properly.

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**, **User name**, and **Password** in the window that is displayed.



Step 3 Click **OK**.

----End

12.3.2.2 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**.

Step 3 Query the lower-layer NMS status.

Step 4 **Optional:** Click  to modify lower-layer NMS parameters. Click **OK**.

Step 5 **Optional:** Click **Lower-layer NMS** of a lower-layer NMS to access and manage it.

----End

12.3.2.3 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 all lower-layer NMSs.

NOTE

You do not need to specify a lower-layer NMS. By default, eSight tests the connectivity of all lower-layer NMSs.

----End

12.4 License Management

You have permission for the eSight only after obtaining a license. The license controls the resources and functions of the eSight.

12.4.1 Querying the License Information of the eSight

You can query the information about the current license.

Prerequisite

You have imported a license file into the eSight.

Context

Table 12-1 describes the license information.

Table 12-1 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 the 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.

If the current license will be expired, you need to import a new valid license in time. See **12.4.2 Importing a License File**.

----End

12.4.2 Importing a License File

If the eSight has no license or the original license expires, you need to import a license file to the eSight.

Prerequisite

You have purchased a license from Huawei.

Procedure

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

The information about the current license file is displayed.

Step 2 Click **Import License**.

Step 3 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

12.5 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 database backup and restoration tool on eSight server.

- In a Windows operating system, choose **Start** > **All Programs** > **eSight** > **tools** > **Launch Database Backup And Recovery Tool**.
- In a Linux operating system, execute the **run.sh** file in the **eSight\backuptool\bin** directory.

Step 2 Connect to the URL for logging in to the database backup and restoration tool by means of the client explorer.

URL example: http://10.135.23.61:8130/backup

Step 3 Click **Set backup path** to set the path for saving backup files, and click **OK**.

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 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.

13.1 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 13-1 List of maintenance items

Maintenance Period	Routine Maintenance Task
Daily	**13.3.1 Browsing Current Alarms**
	13.3.2 Querying Security Logs
Weekly	**13.4.1 Checking the Disk Status of the eSight Server**
	13.4.2 Checking the Disk Space of the eSight Server
	13.4.3 Checking the Logs of the Oracle Database
	13.4.4 Checking the Running Status of Anti-Virus Software
Monthly	**13.5.1 Maintaining User Information**
	13.5.2 Changing the Password of the Current User
Quarterly	**13.6.1 Checking the Equipment Room Environment**
	13.6.2 Checking the Power Supply of the eSight Server
	13.6.3 Checking Hardware and Peripherals of the eSight Server

13.2 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.

13.3 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.

13.3.1 Browsing Current Alarms

You can set the filter criteria in the current alarm list to view the alarms to be concerned and handled.

Context

- If a new alarm is reported and the alarm meets the merging rule, the alarm can be merged to the alarm list, and the number of alarms increases. The merged alarms are displayed in the current alarm list.

  Default alarm merging rule: If the alarms have the same alarm source, location information, and alarm ID, the alarms are merged to one record.
- In the **Current Alarms** window, you can view the information about each alarm.
- If the current filter criteria are modified, the system searches for alarms based on the modified filter criteria.
- When you browse alarms, you can click  to customize the columns to be displayed.

Procedure

Step 1 On the main menu, choose **Fault** > **Current Alarms**.

Step 2 On the **Filter criteria** drop-down menu, select a criterion to query. You can also customize the filter criteria as required. See **4.2.4.5 Customizing Alarm Filter Criteria**.

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

Table 13-2 Operations in Current Alarms window

Operation Name	Operation Method	Description
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. ● 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 the drop-down menu when the window is locked, and click **Search**.	-
Acknowledge	Select one or more alarms and click **Acknowledge**.	● If the alarm is acknowledged, **Acknowledge User** displays the user who acknowledges the alarm. ● If the alarm is unacknowledged, **Acknowledge User** displays  .

Operation Name	Operation Method	Description
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. Select an alarm. Then click in the **Operation** column and choose Shield Alarms**.** 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 mask rule for a performance alarm or clear alarm.
Locate to Topo	Select an alarm and click .	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 Occurrences**.	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

13.3.2 Querying Security Logs

You can query security logs to understand the information about eSight-related security operations.

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**.

Step 2 In the left navigation tree, choose **Query Logs** > **Security Logs**.

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

After clicking **Details**, you can query detailed information about the log.

----End

13.4 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.

13.4.1 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) and Single-Server System (Solaris):
  1. Log in to the OS as the **t2000nmsuser** user.
  2. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     Password: *password_of_user_root*
  3. Run the following commands to view the physical status of the disk on the current server:

     # **iostat -E**

The following information is displayed:

```
sd1       Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: HITACHI  Product: H101414SCSUN146G Revision: SA25 Serial No:
0848E3PKSA
Size: 146.80GB <146800115712 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
```

- Perform the following steps in a High Availability System:
  - On Solaris or SUSE Linux:
    1. Log in to the OS as the **t2000nmsuser** user.
    2. Open a CLI. Then, run the following commands to switch to the **root** user:

       `$` **su**

       `Password:` *password_of_user_root*
    3. Run the following commands on the master server of the primary and secondary sites:

       `#` **vxdisk list**

       The following information is displayed:

       ```
       DEVICE TYPE DISK GROUP STATUS
       c1t0d0s2 auto:sliced rootdisk datadg online
       c1t1d0s2 auto:sliced rootmirror datadg online
       ```

       NOTE

       The equipment names in the **DEVICE** column may be different from those displayed on the terminal according to the actual situation of the workstation. The displayed number of columns is consistent with the number of disks.
  - On Windows, run the following commands on the master server of the primary and secondary sites:

    `C:\>` **vxdisk list**

----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 **vxdisk list** command, the disk is in the **online** state.
3. After you run the **iostat -E** command, if the **Hard Errors** of the disk is **0**, the physical status of the disk is normal.

Troubleshooting

If a disk does not function properly, contact the equipment supplier to repair or replace the disk in a timely manner.

13.4.2 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:

  View the disk space of the server in the **Computer** window. 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%.

13.4.3 Checking the Logs of the Oracle Database

This topic describes how to check the logs of the Oracle database.

Procedure

Check the log file *alert_$ORACLE_SID.log* in the **$ORACLE_BASE/diag/rdbms/$ORACLE_SID/$ORACLE_SID/trace/** path.

Reference Standard

No ORA-* information is contained in the file.

Troubleshooting

Fix the system according to the error information in the log file. If the problem still persists, contact technical support engineers of Huawei.

13.4.4 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.

13.5 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.

13.5.1 Maintaining User Information

This topic describes how to view or modify the user information after a user is created.

Prerequisite

You have permission to maintaining user information.

Procedure

Step 1 On the main menu, choose **System** > **Security Management**.

Step 2 In the left navigation tree, choose **Rights Assignment** > **User**.

Step 3 In the **User** window, perform the following operations described in the following table.

Operation	Method
View	1. Select a user and click the user name. 2. View the related information.
Modify	1. Select a user and click  in the **Operation** column. 2. Modify the related information. 3. Click **OK**.
Reset password	1. Select a user and click  in the **Operation** column. 2. Modify the password. 3. Click **OK**. **NOTE** The password of the default system user **admin** cannot be reset.
Delete	1. Select a user and click  in the **Operation** column. 2. Confirm the system message. **NOTE** The default system user **admin** and the current user cannot be deleted.

Operation	Method
Enabled/Disabled	1. Click / to enable or disable the account of a user. 2. The **Status** column displays the status of user accounts.

----End

13.5.2 Changing the Password of the Current 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.

Prerequisite

The new password must comply with the password policy.

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

13.6 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.

13.6.1 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%

Item	Index
Dust condition	Clear and spotless
Power supply	The power supply is normal, which ensures the normal running of the equipment in the equipment room.
Air filter	The air filter is clean and the cabinet is in good ventilation condition.
Fire alarm system	The fire alarm system works properly and can effectively sense fire accidents.
Lightning proof system	The lightning proof system works properly and can effectively prevent the lightning stroke.

Troubleshooting

1. Adjust the temperature and humidity properly. Make sure that the doors and windows are airtight.
2. Remove the air filter from the cabinet, remove the dusts on the air filter with the vacuum cleaner, and then place the air filter in the cabinet.
3. Repair the power supply system, fire alarm system, and lightning proof system to ensure that the equipment in the equipment room works properly and securely.

13.6.2 Checking the Power Supply of the eSight Server

This topic describes how to check whether the power supply of the eSight server is normal.

Prerequisite

The eSight server must be powered on.

Procedure

Step 1 Check whether the power indicators of the server and monitor are normal.

Step 2 Run the following commands to view information about the power supply faults in the logs recorded in recent days:

more */var/log/messages*

more */var/log/warn*

Information similar to the following is displayed:

```
Jun 23 16:53:40 Server rmclomv: [ID 632913 kern.error] Input power unavailable for
PSU @ PS1.
```

If **error** or **WARN** is contained in the command output, the power supply is in the abnormal state.

Step 3 Check the faults of the external power of the system.

Step 4 Confirm that the power supply of the server is normal.

----End

Reference Standard

In normal cases, all the power indicators of the server peripherals turn green and all fault indicators are off.

Troubleshooting

If a fault about the external power of the system occurs, the system does not record the related information. In this case, you must detect the external power supply and circuits in other methods. For details, refer to the delivery manual of the server. If you encounter complicated problems, contact the manufacturer to repair or replace the server.

13.6.3 Checking Hardware and Peripherals of the eSight Server

This topic describes how to check the status of hardware and peripherals of the eSight server.

Prerequisite

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.

A Glossary

A

AAA	See **Authentication, Authorization and Accounting.**
AH	See **Authentication Header.**
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.

D

DHCP	See **Dynamic Host Configuration Protocol.**
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.

I

IETF	See **Internet Engineering Task Force.**
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.
IPSec	See **IP Security.**

Internet Engineering Task Force (IETF)	A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.
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.

L

LAN	See **local area network.**
LLDP	See **Link Layer Discovery Protocol.**
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.
local area network (LAN)	A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building. It features high speed and low error rate. Ethernet, FDDI, and Token Ring are three technologies used to implement a LAN. Current LANs are generally based on switched Ethernet or Wi-Fi technology and running at 1,000 Mbit/s (that is, 1 Gbit/s).

M

MIB	See **management information base.**
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.

R

RF	See **radio frequency.**
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.

S

SA	See **security association.**
SMPP	See **Short Message Peer to Peer.**
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).

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.

T

TCP	See **Transmission Control Protocol.**
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.

W

WLAN	See **wireless local area network.**
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.