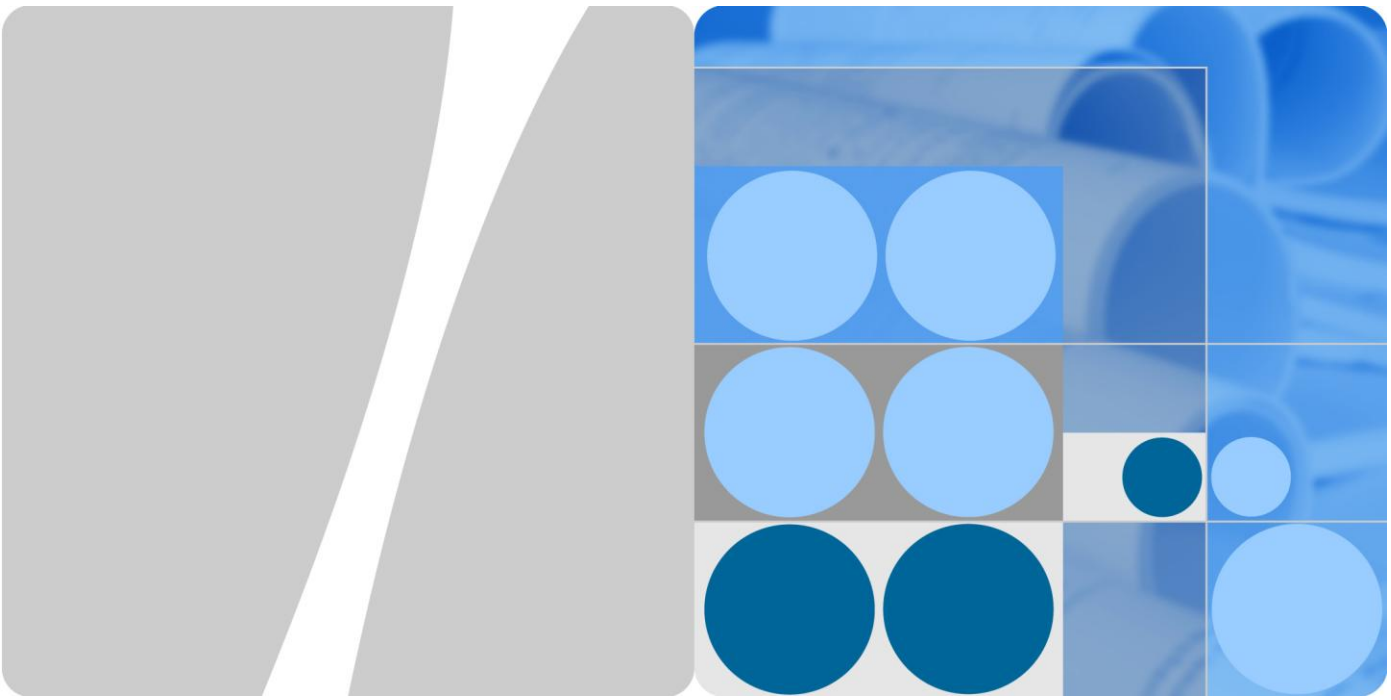


eSight
V200R003C00
Product Technical White Paper

Issue 01

Date 2012-12-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

About This Document

Overview

This document describes the comprehensive eSight solution, including eSight basic management components, key technologies, function constraints, and typical applications.

Intended Audience

This document is intended for:

- Technical support personnel
- Maintenance personnel

Symbol Conventions

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

Symbol	Description
DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Provides additional information to emphasize or supplement important points in the main text.
NOTE	Provides a tip that may help you solve a problem or save time.

Change History

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

Issue 01 (2012-12-31)

This issue is the first release.

Contents

1 Executive Summary

eSight is a comprehensive solution developed by Huawei for the management of enterprise networks, such as the wired or wireless enterprise campus, branch, and data center (DC) networks. eSight aims to implement unified management of and intelligent interaction among enterprise resources, services, and users.

2 Overview

eSight provides various editions (compact, standard, and professional) to meet requirements of different enterprise customers. Various service components are incrementally integrated to the eSight solution based on basic management components. Enterprise customers can flexibly select management components according to their requirements.

Edition	Function
Compact	Allow a user to manage the alarms, performance,topology, configuration files, network elements (NEs), links, logs ,physical resources and electronic labels. Only one user is supported.
Standard	Provides all functions of the compact edition, report, IP topology, Smart Configuration Tool, customized device management, security management. Multiple users are supported. Provides WLAN management, NTA network traffic analysis,SLA management, QoS management, MPLS VPN management, MPLS tunnel management,Terminal Access management, IPSec VPN management, SNMP northbound interface. Provides system monitor tool, database backup&restore tool, fault information collection tool.
Professional	Provides all functions of the standard edition, DC nCenter, and hierarchical network management.

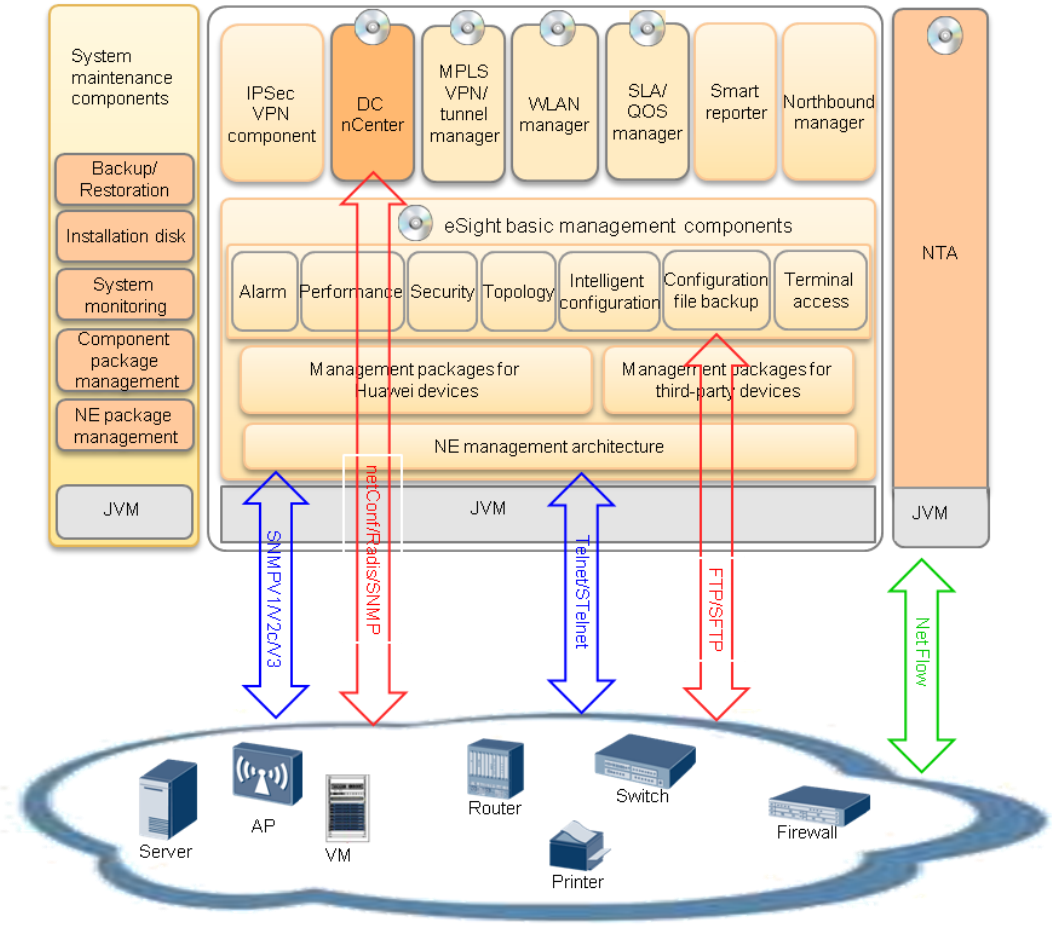
3 Solutions

3.1 eSight Solution

3.1.1 Component-based Architecture

eSight uses the component-based architecture and Open Services Gateway initiative (OSGI) to implement dynamic pluggable capabilities of application components. Customers can select components based on their network types.

Figure 3-1 eSight architecture



Component	Description	Technical White Paper for Reference
Basic network management component	Provides an intelligent configuration tool and allows users to manage devices from multiple vendors, topologies, device performance, security, configuration files, and faults.	eSight V200R003C00 Product Technical White Paper eSight V200R003C00 Security Technology White Paper Huawei eSight V200R002C00 SCT Technical White Paper
Terminal	Allows users to manage all access terminals on the network	eSight

Component	Description	Technical White Paper for Reference
Access Manager	by analyzing the MAC address forwarding tables and ARP tables.	V200R003C00 Terminal Access Technical White Paper
Smart Reporter	Presets various report templates to meet requirements in most maintenance scenarios and provides the professional report design tool for users to customize statistics reports.	eSight V200R003C00 Product Technical White Paper
SLA Manager	Integrates with devices' network quality analysis (NQA) function to diagnose link performance between network devices 24/7 hours.	eSight V200R003C00 SLA Technical White Paper
WLAN Manager	Provides integrated management for wired and wireless networks, and enables batch service deployment, adjustment, troubleshooting, and routine maintenance.	eSight V200R003C00 WLAN Technical White Paper
NTA	Helps network administrators monitor the traffic and bandwidth usage and detect network bottlenecks in a timely manner based on the NetFlow, NetStream, and sFlow protocols, which provides evidence for network planning and fault diagnosis.	eSight V200R002C01 NTA Technical White Paper
MPLS VPN Manager	Integrates discrete VPN information on the network into visible manageable objects and simplifies VPN service monitoring and fault diagnosis, which ensure QoS and reliability of key services.	Huawei eSight V200R002C00 BGP MPLS VPN Technical White Paper
MPLS Tunnel Manager	Automatically discovers multiprotocol label switching traffic engineering (MPLS TE) tunnels and Label Distribution Protocol (LDP) tunnels, dynamically displays tunnel running status, and provides visualized route management.	eSight V200R002C00 BGP MPLS Tunnel Technical White Paper
QoS Manager	Monitors network QoS in real time and provides all-round functions of the QoS configuration, monitoring, and optimization.	eSight V200R003C00 QoS Technical White Paper
DC nCenter	Monitors network resources including physical servers, virtual machines (VMs), virtual switches, and top of rack	eSight V200R003C0

Component	Description	Technical White Paper for Reference
	(ToR) switches, displays the topology of virtual resources and physical devices, and dynamically adjusts the physical network policies based on VM changes.	0 DC nCenter Technical White Paper

3.1.2 Product Technologies

Web-based Architecture

The eSight uses the B/S structure and therefore has all advantages of the B/S structure. eSight runs on browsers, so only the eSight server needs the upgrade and maintenance. The advantages are as follows:

- Allows users to perform operations such as querying and browsing anywhere at any time based on the distributed feature.
- Allows users to expand services only by upgrading the server software.

Adaptation Capability for Multiple Vendors

eSight provides adaptation capability for devices from vendors such as Huawei, H3C, and Cisco. eSight provides default adaptation plans and user-defined device management plans to meet the different adaptation requirements for network devices, IT servers, and IP terminals from multiple vendors in the enterprise market.

1. Default adaptation plan for vendors

   eSight provides basic adaptation capabilities for devices from Huawei, Cisco, and H3C, including topology management, standard alarms, standard performance counters (CPU/memory), configuration file backup, and panel display.
2. User-defined device management plan

eSight supports customization of basic management functions for unknown devices by entering the device object identifier (OID), alarm information, performance counters, configuration commands, and high-fidelity panels.

Device Adaptation Package

eSight features consist of the following independent components: eSight model, common logic, and device adaptation. Parts that are related to device types in each feature are extracted as expansion points and implemented by device adaptation packages. The device adaptation technology aims to load different adaptation packages on a stable eSight edition to manage various devices.

Device adaptation parts are released in device adaptation packages. When the service functions remain the same, device adaptation packages are updated to adapt new device versions. Users can obtain the latest device adaptation packages at the Huawei website for Huawei devices, and develop adaptation packages for devices from other vendors.

3.2 Basic Component Management

Basic components implement basic IP network management functions, including performance, fault, configuration, accounting, and security management defined by telecommunications management network (TMN). eSight basic components do not provide the accounting management function.

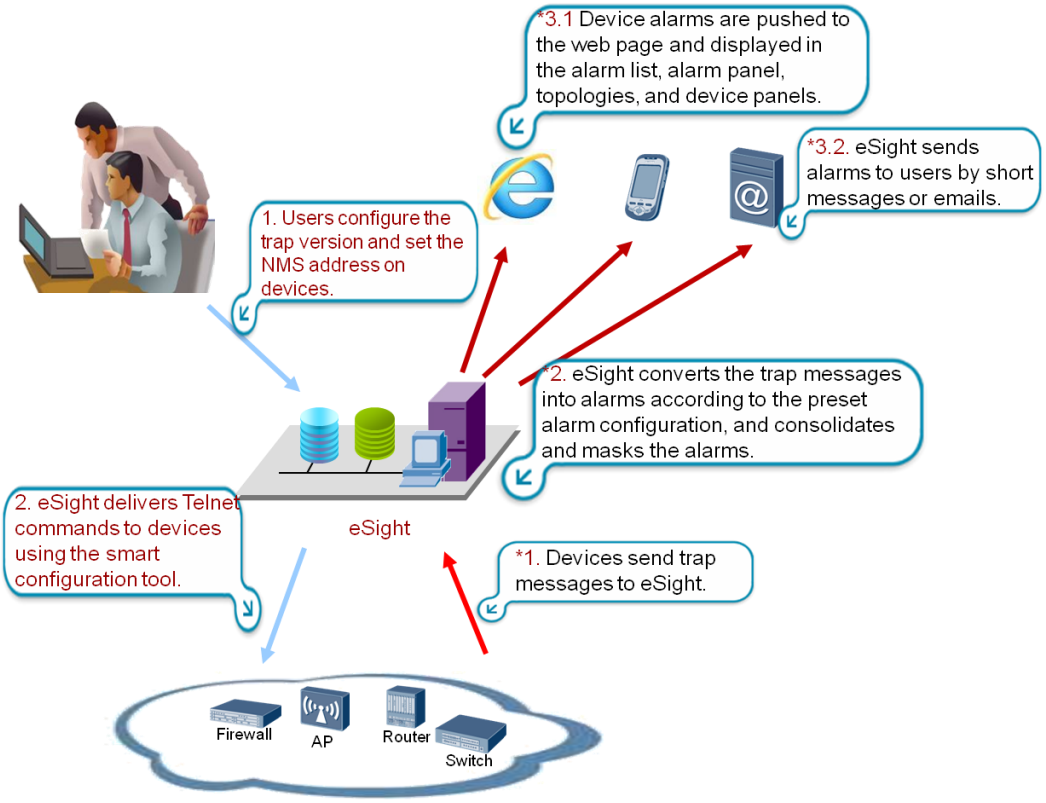
Function	Description
Performance management	Supports performance data collection, report analysis, and Portal top N monitoring, which monitor, analyze, and evaluate networks and devices.
Fault management	Receives traps reported by devices, pushes the traps and topologies to the web page, and notifies users of network faults by short messages or emails in a timely manner.
Configuration management	Backs up device configuration files and restores the configuration using the backup configuration files when a device fault occurs or components on a device are replaced.
Security management	Supports identity authentication, access control, security-related alarms, and security logs to ensure security of services and resources.

3.3 Performance Management

3.3.1 Introduction

eSight collects device performance data and supports report analysis, Portal top N monitoring, and performance threshold alarms based on the collected data, implementing data display and analysis.

Figure 3-2 Performance management solution



eSight also provides an NTA component to allow users to analyze service flows based on parameters such as protocols used on networks. For details, see the *eSight V200R002C01 NTA Technical White Paper*.

3.3.2 Key Technologies

Performance Collection Task Management

eSight collects performance counters of devices on IP networks using Simple Network Management Protocol (SNMP) at the interval specified in a performance collection task.

Performance Data Consolidation

eSight periodically collects device performance data and saves the data to the database, saving disk space on the device and preventing a slow data query speed due to a large amount of data.

By default, eSight saves original performance data in the latest three months. Data saved for more than three months is consolidated by hour and day. Hourly data is saved for one year, and daily data is permanently saved.

To improve the performance data query efficiency, the following rules are defined:

1. Daily data is displayed when users query performance data in more than one month.
2. Hourly data is displayed when users query performance data in one week to one month.
3. Original data is displayed when users query performance data within one week.

3.3.3 Function Constraints

Applicable Device Types

eSight can collect performance data of all network devices based on different preset performance counters. For details, see the *eSight V200R003C00 Specification List.xlsx*.

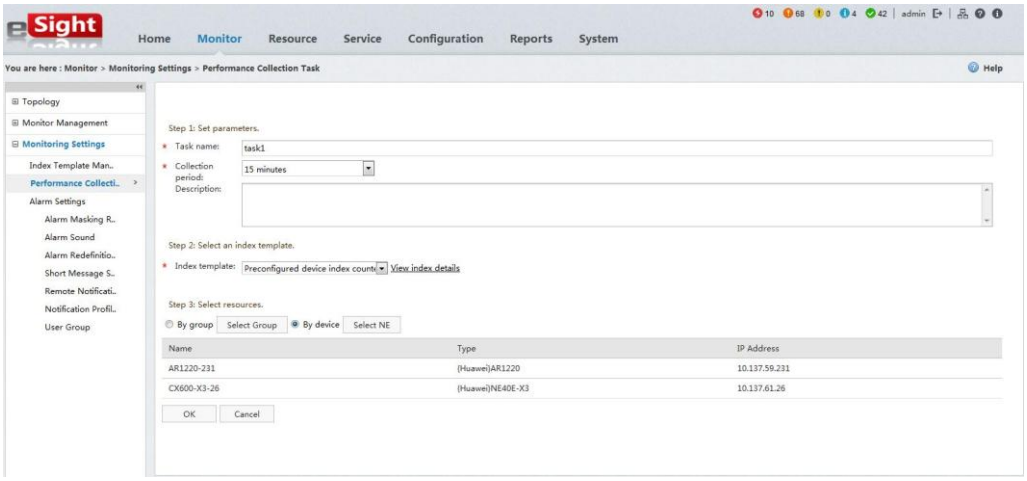
Technical Constraint

The parameter **SNMP Read** must be correctly set on collected devices.

3.3.4 Typical Applications

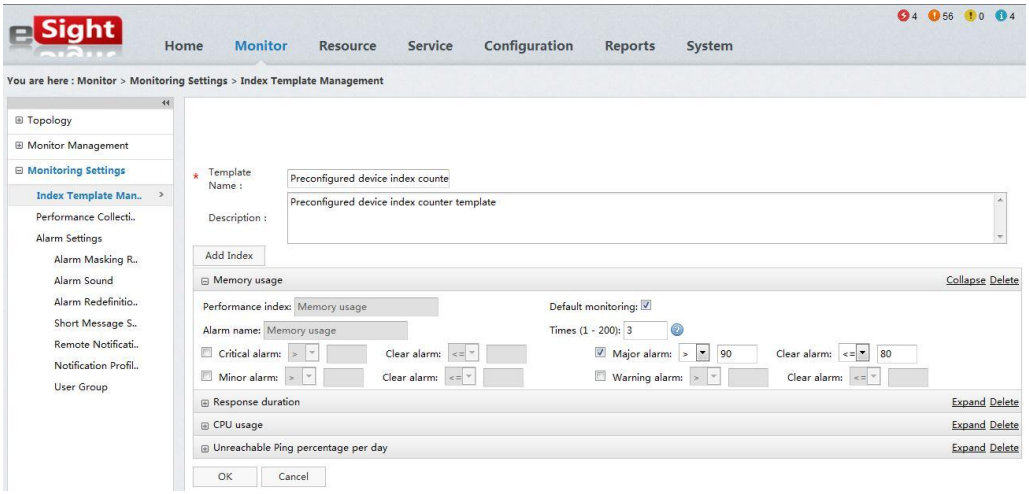
1. eSight collects performance counters of devices on IP networks using SNMP at the interval specified in a preset or manually created performance collection task

Figure 3-3 Performance Collection Task Managerment



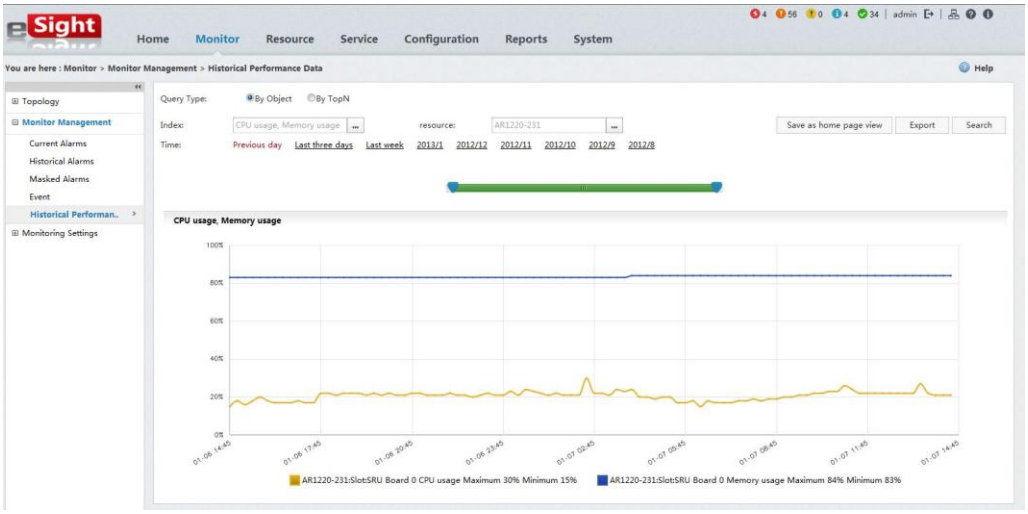
2. After collecting performance data, eSight saves the data to the performance database and starts data consolidation.
3. An alarm is generated when a performance counter exceeds the preset threshold to provide network exception data for users.

Figure 3-4 Index Template Management (Set alarm threshold)



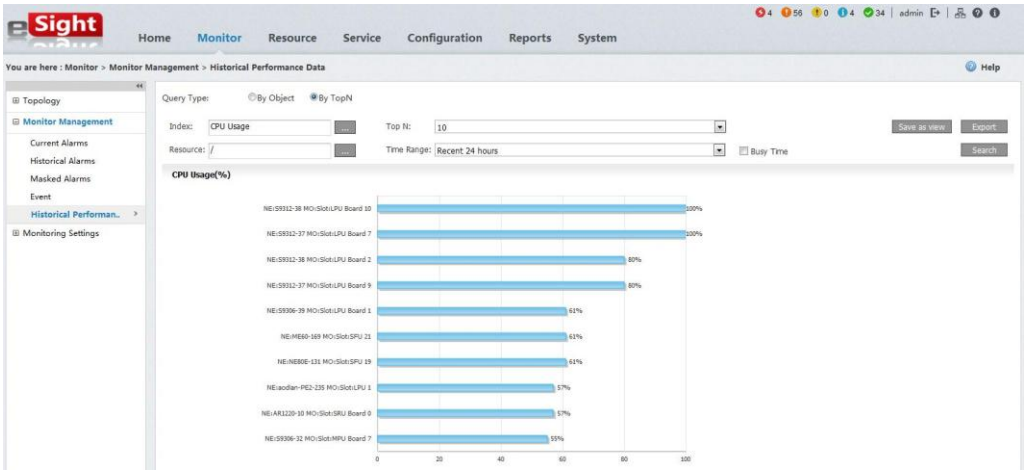
4. Users can query history device performance data according to query criteria such as performance counters, subnet areas/collected devices, and collection time.

Figure 3-5 Historical Performance Data



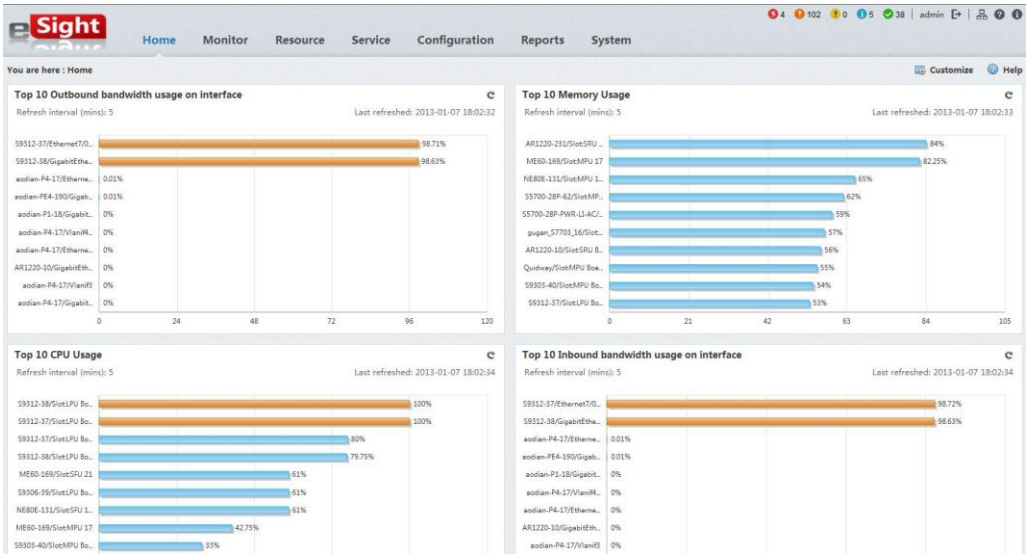
5. Users can also query performance data of top N collected devices on a specified subnet based on performance counters and collection time, which helps monitor the network.

Figure 3-6 TopN Performance Data



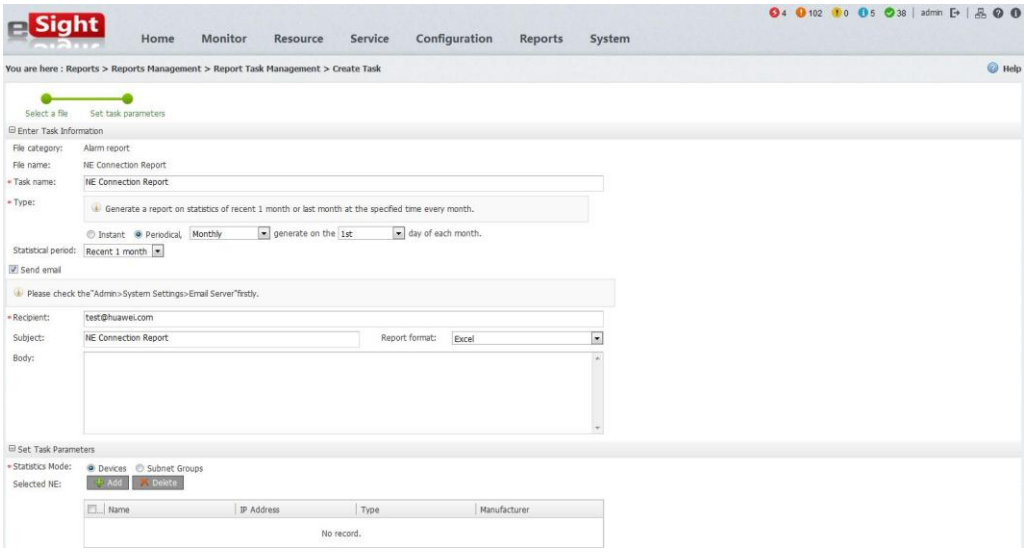
6. The system Portal provides many monitoring panels on the main page and periodically updates top N performance data, helping users to monitor networks in real time.

Figure 3-7 System Portal



7. The Smart Reporter collects statistics on device performance and sends the statistics to users' email boxes.

Figure 3-8 Create Report Task

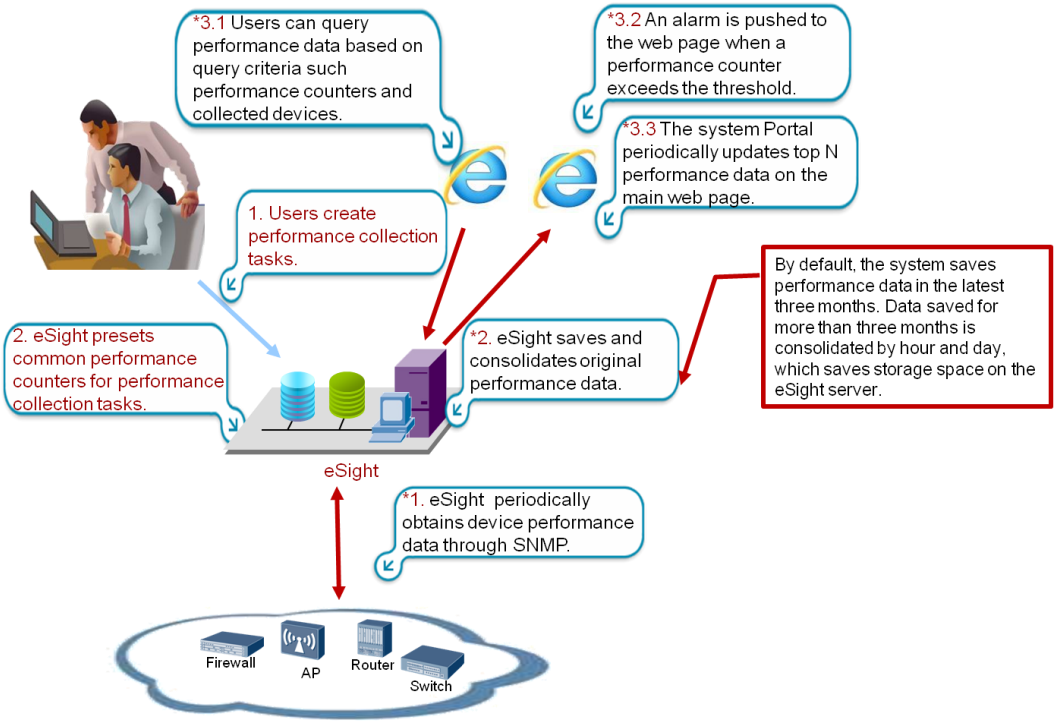


3.4 Alarm Management

3.4.1 Introduction

When a fault occurs on a device, the device generates a trap message and sends it to the eSight server. The eSight converts the tarp message into an alarm based on the configured alarm information and displays the alarm on the web page, monitoring network devices based on alarms.

Figure 3-9 Alarm management solution

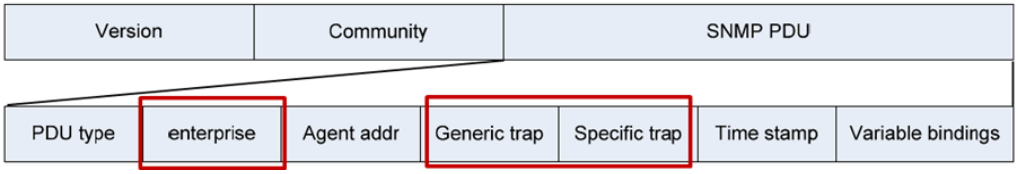


3.4.2 Key Technologies

Trap Receiving

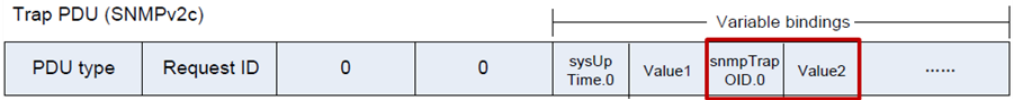
Devices can send SNMP trap messages to the destination address specified using commands. eSight supports trap messages of SNMPv1, SNMPv2c, and SNMPv3.

1. SNMPv1 trap message



The fields **enterprise** (trap source type), **Generic Trap** (common trap), and **Specific trap** (enterprise private trap) uniquely identify a trap message. eSight parses the **Variable bindings** field in the trap message and displays the parsed value on the web page.

2. SNMPv2c and SNMPv3 trap messages

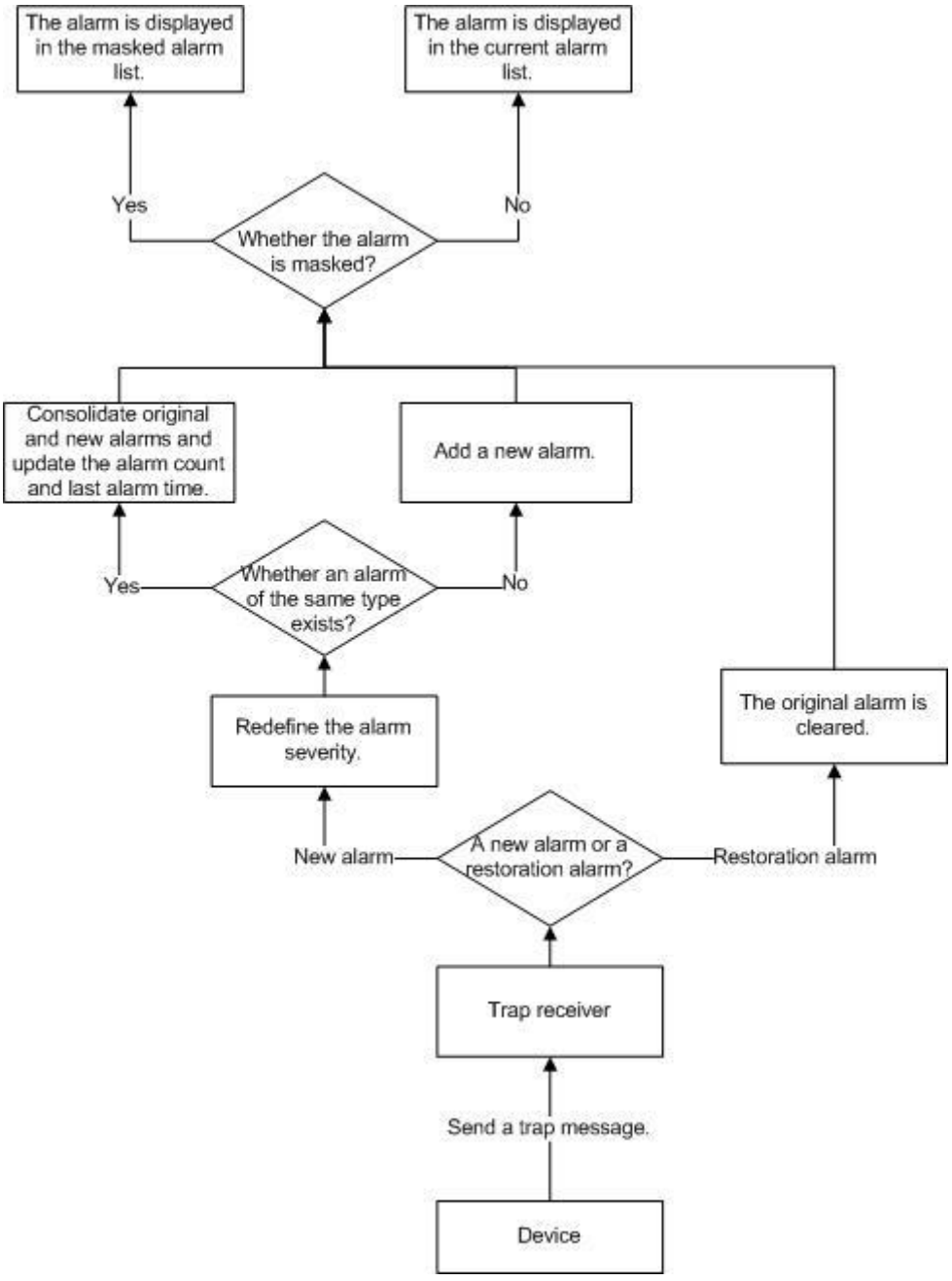


The field **snmpTrapOID** uniquely identifies a trap message. eSight parses the **Variable bindings** field in the trap message and displays the parsed value on the web page.

Compared with the SNMPv2c trap message, an encryption header is added to the SNMPv3 trap message. The packet data unit (PDU) is the same in the SNMPv2c and SNMPv3 trap messages.

Trap Processing

After receiving trap messages, eSight parses the trap messages based on the static alarm configuration, redefines the alarm severity, and masks alarms.



3.4.3 Function Constraints

Applicable Device Types

All network devices are supported and can be configured with different alarm adaption information. For details, see the *eSight V200R003C00 Specification List.xlsx*.

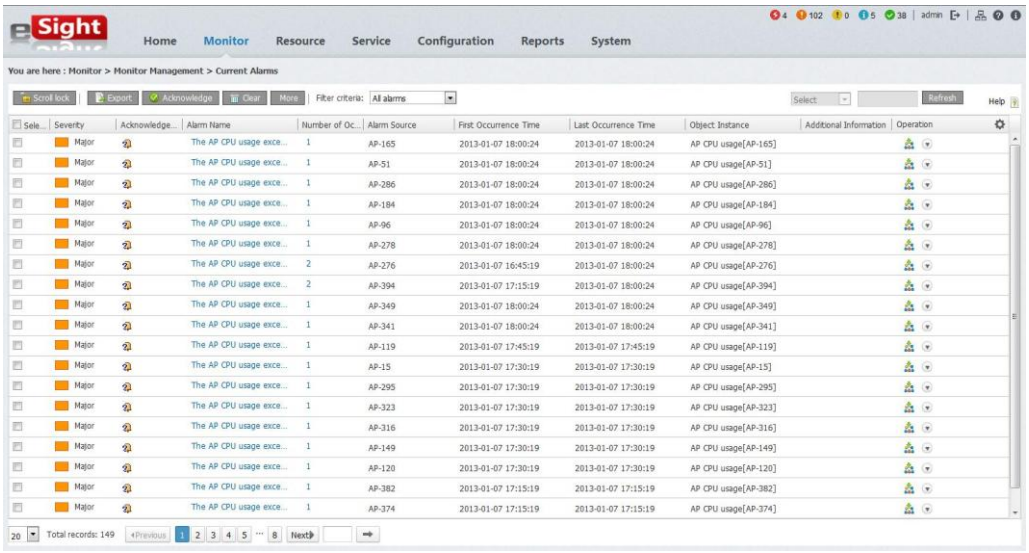
Technical Constraint

The parameter **Trap-Host** must be set to the eSight server on the device, and the parameter **SNMP Read** must be correctly set on the eSight server.

3.4.4 Typical Applications

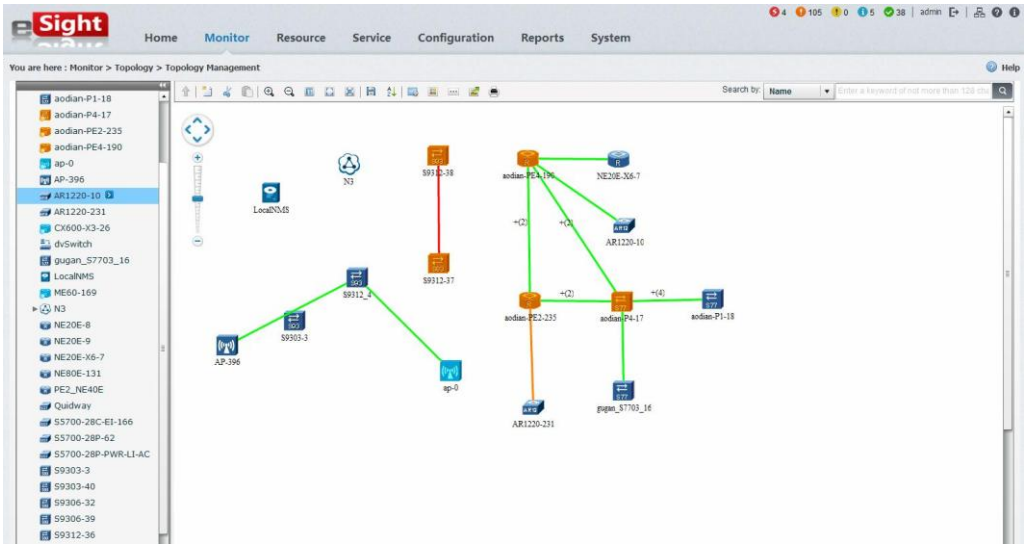
1. eSight displays a network alarm list and notifies users of alarms by sounds.
2. The alarm panel dynamically updates the number of alarms of various levels.

Figure 3-10 Current Alarm & Alarm Panel



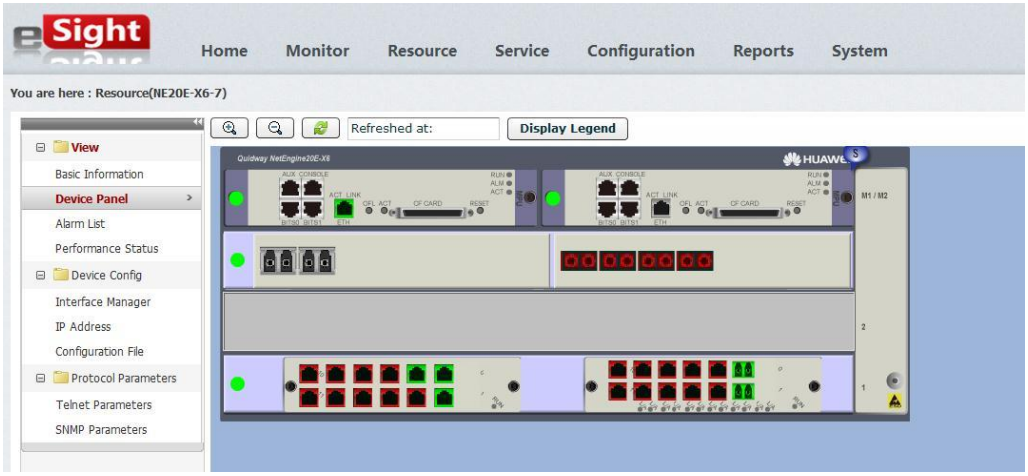
3. The colors of device icons and links are updated in the topology in real time to notify users of alarm status.

Figure 3-11 TOPO Management



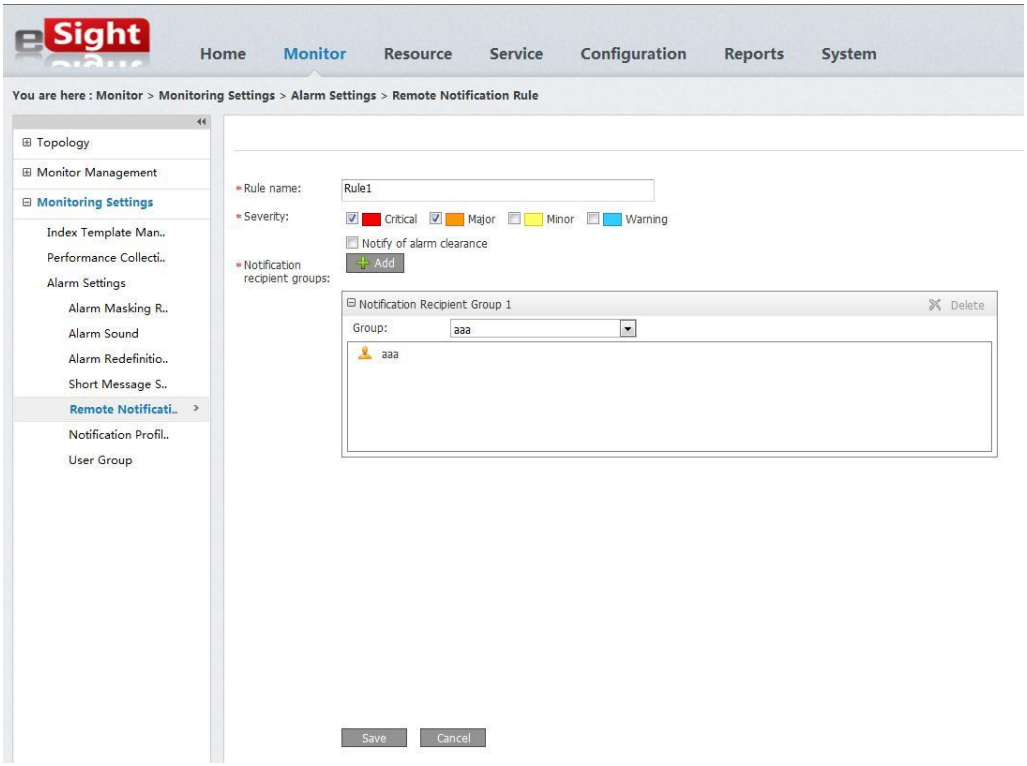
4. The colors of cards and ports are updated on the NE Manager panel in real time to notify users of alarm status.

Figure 3-12 Device Panel



5. eSight sends the received trap messages to users by short messages or emails.

Figure 3-13 Alarm Remote Notification

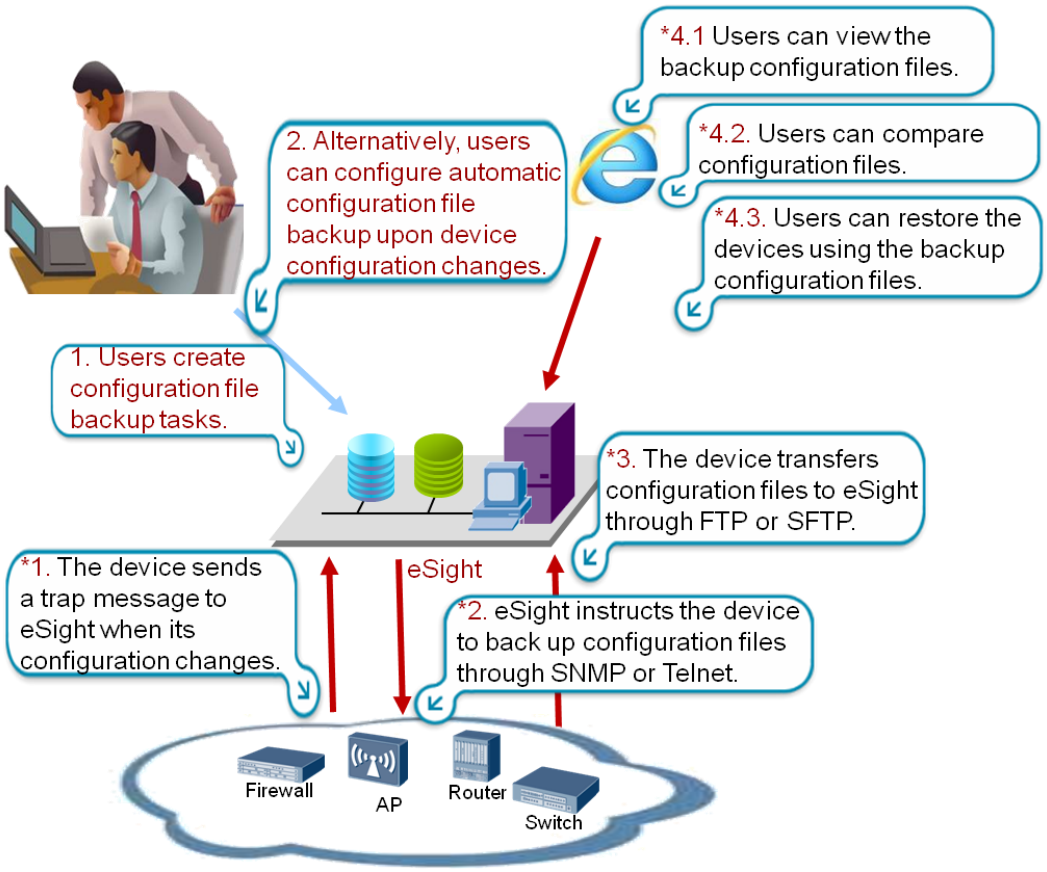


3.5 Configuration File Backup

3.5.1 Introduction

Services can run properly on network devices only when related parameters are correctly set. Users can back up configuration files of important devices and restore the configuration using the backup configuration files when a device fault occurs or components on a device are replaced.

Figure 3-14 Configuration file backup



3.5.2 Key Technologies

eSight can function as a File Transfer Protocol (FTP) server or a Secure File Transfer Protocol (SFTP) server. eSight instructs devices to back up configuration files using a MIB interface or command lines periodically, or when the device configuration changes. Devices upload configuration files to the specified directory on eSight using FTP or SFTP.

1. Huawei devices

a. eSight periodically notifies Huawei devices of configuration file backup and restoration through Huawei proprietary MIB interface based on scheduled tasks.

b. When the configuration of a Huawei device changes, it sends a trap message to eSight. After receiving the trap message, eSight notifies the Huawei device of configuration file backup and restoration through Huawei proprietary MIB interface.

2. Third-party devices

eSight periodically notifies third-party devices of configuration file backup and restoration using command lines based on scheduled tasks.

3.5.3 Function Constraints

Applicable Device Types

All network devices are supported. By default, the configuration file backup function has been configured for Huawei, Cisco, and H3C devices. Users can set command lines for backing up configuration files of devices from other vendors.

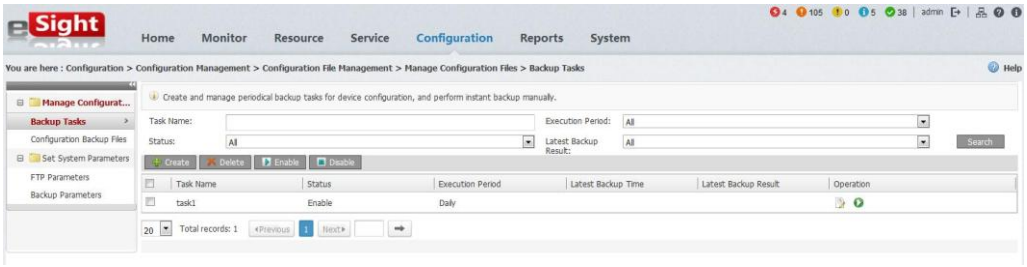
Technical Constraint

The parameter **SNMP Read** and **SNMP Write** must be correctly set on Huawei devices and eSight. Command lines and Telnet parameters must be set on third-party devices and eSight.

3.5.4 Typical Applications

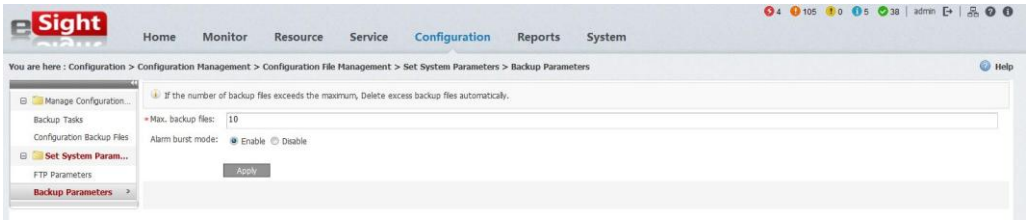
1. Users can configure scheduled configuration file backup tasks.

Figure 3-15 Backup task



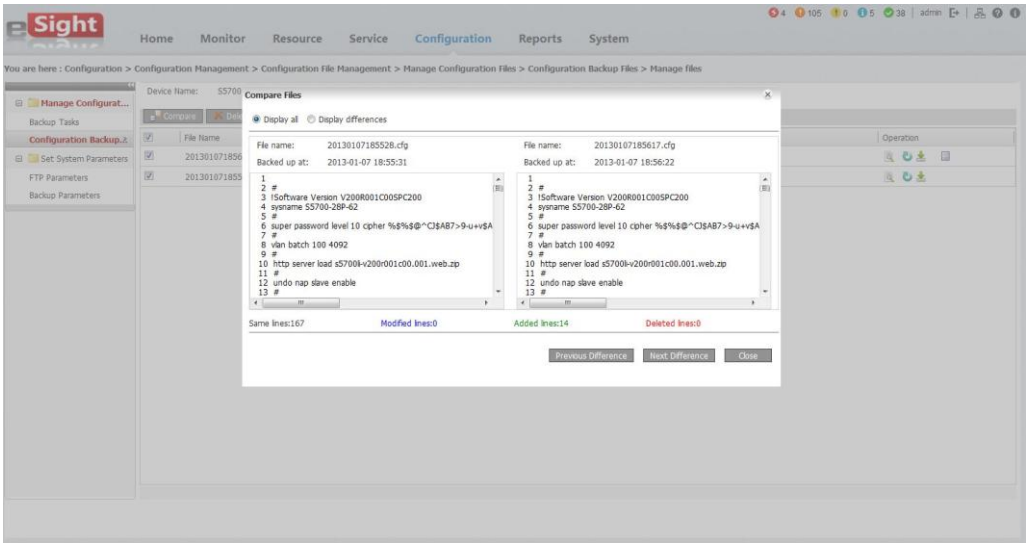
2. eSight instructs devices to back up configuration files when the device configuration changes.

Figure 3-16 Backup Parameters



3. When the network is stable, users can specify a configuration backup file as a baseline file that will be permanently saved on the device.
4. Users can compare the currently used configuration file with the baseline file to locate network faults.

Figure 3-17 Backup File Compare



5. Users can restore devices using the configuration files saved on eSight.

3.6 Security Management

eSight security solution ensures eSight software security. In addition, eSight provides suggestions on the security of the physical layer and management layer to ensure the implementation of security measures. The security solution covers the following three aspects:

- Application layer security: protects applications with a variety of security measures such as access control, data security, and communication and coding security.
- System layer security: protects operating systems, databases, middleware, and services that applications depend on.
- Network layer security: protects the entire network to ensure that all service systems running on the network are stable.

For details, see the *eSight V200R003C00 Security Technology White Paper.doc*.

4 Promotion

- Comprehensive IP network monitoring

eSight basic components implement basic IP network management functions, including performance, fault, configuration, and security management. eSight monitors and manages network quality and faults.

- Comprehensive service monitoring on the entire network

The WLAN Manager, SLA Manager, VPN Manager, DC nCenter, and NTA monitor the entire network.

5 Conclusion

eSight manages IP networks, monitors the networks, and collects network quality data in real time, helping users to know about the network status and service quality.

6 Acronyms and Abbreviations

Acronyms and Abbreviations	Full Name
NBI	Northbound Interface
CLI	Command Line Interface
ESN	Equipment Serial Number
FTP	File Transfer Protocol
OSS	Operating Support System
RSA	Revist-Shamir-Adleman Algorithm
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TMN	Telecommunication Management Network
UDP	User Datagram Protocol
VMM	Virtual Machine Manager
XML	Extensible Markup Language