

Huawei eSight Full Product Datasheet







Huawei eSight Full Product Datasheet

Product Overview

eSight is a unified enterprise network management system provided by Huawei enterprise network product line. eSight consists of the unified network management platform, Smart Reporter, SLA manager, QoS manager, WLAN manager, Network Traffic Analyzer, MPLS VPN manager, MPLS Tunnel manager, Data Center nCenter manager, Secure Center, and LogCenter log manager. All of these components provide enterprises and partners with an abundant comprehensive and open network management platform, managing the network, services, and users in a unified manner.

Product Characteristics

One Management

One Management

- Unified management of the wired and wireless networks
- Unified management of network devices and security devices
- Third-party device management

One Policy

One Policy

- Policy authorization based on roles and scenarios and scenario-based access control (based on user identity, terminal type, access location, time, and access method)
- Rich security policy to enhance terminal security
- Full access lifecycle solution

Easy to Use

Easy to Use

- Visualization management
- Easy troubleshooting
- User-friendly GUI

Product Components

eSight provides a unified operation and maintenance (O&M) platform and specific components to meet enterprise user requirements.

Component	Description
eSight Unified Network Management Platform	Provides compact, standard, and professional editions for enterprise users. In addition to unified management of devices from various vendors, topology management, fault management, performance management, smart configuration tool, configuration file management, and SNMP northbound interface, eSight Unified Network Management Platform allows users to customize third-party devices, helping users to establish a network management system catering for their own needs.
eSight Smart Reporter	Provides preset report templates to meet requirements in most management scenarios. Provides the professional report design tool for users to customize statistics reports.
eSight SLA Manager	Integrates with devices network quality analysis (NQA) function to diagnose and measure the link performance between network devices 24/7 hours and displays quality of service (QoS) statistics. Administrators can set the QoS threshold. eSight notifies administrators remotely when QoS reaches the threshold. Administrators can use the quick diagnosis function to monitor link performance in real time and diagnose faults, which improves management efficiency.
eSight QoS Manager	Monitors network QoS in real time. Provides multi-dimensional data analysis and displays QoS information in graphs and dashboards, simplifying network management.
eSight WLAN Manager	Integrates the management of wired and wireless networks and implements batch service deployment, service adjustment, troubleshooting, and routine maintenance.
eSight Network Traffic Analyzer	Collects traffic of routers and Layer 3 switches, analyzes network traffic based on the NetFlow, NetStream, and sFlow protocols, and allows users to customize reports. This helps network administrators to monitor the traffic and bandwidth usage and detect network bottlenecks in a timely manner, providing evidence for network planning and fault diagnosis.
eSight MPLS VPN Manager	Works with the MPLS function of routers and switches to provide visible end-to-end (E2E) MPLS service monitoring and faults diagnosis.
eSight MPLS Tunnel Manager	Automatically discovers the MPLS TE tunnels and LDP tunnels that have been deployed on the network, monitors the tunnels in real time, displays tunnel running status dynamically, and monitors active-standby switchover and bypasses.
eSight DC nCenter	Monitors network resources (including physical servers, VMs, vSwitches, and TOR switches), displays the topology of virtual resources and physical devices, and dynamically adjusts physical network profiles based on VM changes.
eSight Secure Center	Provides unified security services management functions for the whole network. Provides central management for Huawei firewalls, UTMs, and access routers (AR).
eSight LogCenter	Provides a platform for collecting, storing, and auditing large-scale logs of multiple types in a unified manner. Manages logs from Huawei and other vendors' devices. Provides industrial leading NAT tracing and security events analysis functions.

eSight Unified Network Management Platform

Product Overview

As the network scales and the number of enterprise network applications continue to grow, more and more devices, such as multi-service routers, security gateways, and WLAN Access Points (APs) that implement communication and collaboration services in decentralized networks like enterprise campus networks and branch office networks. An increasing number of core and access devices provided by multiple vendors are used in an enterprise. Each device has its own management system, creating a nightmare for system and network administrators.

To alleviate the operational burden, Huawei has developed eSight Unified Network Management Platform, a unified network management system that provides a comprehensive view and management of all network and system resources, ensures network stability, and improves O&M efficiency.

eSight Unified Network Management Platform provides compact, standard, and professional editions for enterprise users. In addition to unified management of devices from various vendors, topology management, fault management, performance management, smart configuration tool, configuration file management, and SNMP northbound interface, eSight Unified Network Management Platform allows users to customize third-party devices, helping users to establish a network management system catering for their own needs.

Characteristics

eSight Unified Network Management Platform provides compact, standard, and professional editions for enterprise users.

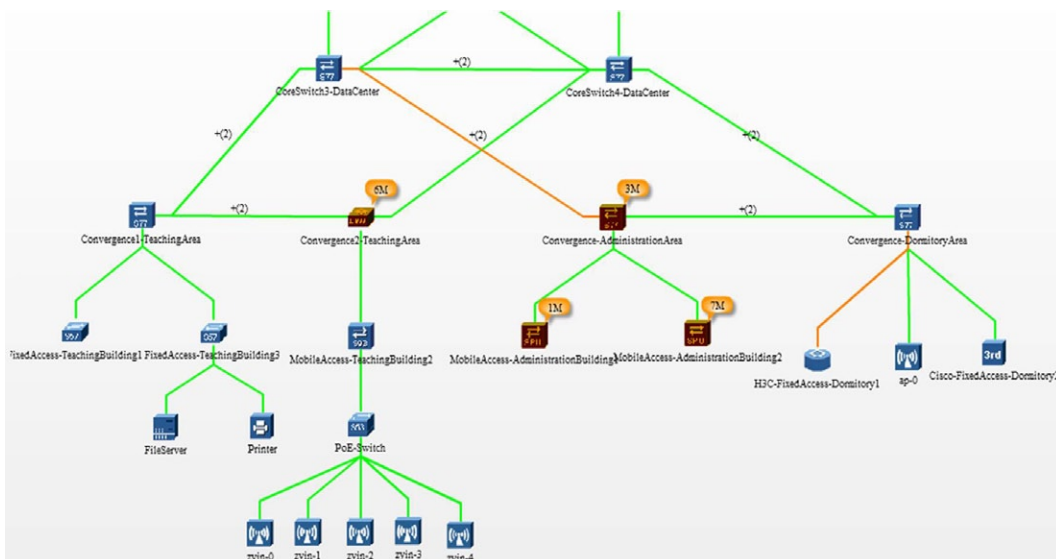
Edition	Functions
Compact edition	Supports management of topology, network elements (NEs), links, physical resources, e-labels, alarms, performance, configuration files, logs, customized device management, report management, the smart configuration tool, and security management. Provides database backup tool and fault collection tool.
Standard edition	Supports all functions of the compact edition, Smart Reporter, SNMP north bound interface, SLA management, QoS management, WLAN management, NTA network traffic analysis, MPLS VPN management, MPLS tunnel management, Secure Center, LogCenter management, and IPSec VPN management.
Professional edition	Supports all functions of the standard edition, hierarchical NMS management, HA architecture, and the DC nCenter.

eSight is a B/S architecture system, supporting multiple operating systems.

- eSight uses the browser/server (B/S) architecture that does not require any client software. You only need to update the server when the software updates.
- The platform supports Windows and SUSE Linux operating systems and Oracle, MySQL, and SQL Server databases.

eSight can manage devices from different vendors and multiple resources to provide unified management across the whole network.

- Comprehensive device management: In addition to Huawei routers, switches, ARs, security devices, WLAN devices, and firewalls, eSight can manage devices from major vendors such as HP and Cisco, and can also manage IT resources such as servers and printers.
- Third-party device customization: eSight allows customers to define vendor names, device types, panel style, performance presentation, and alarms for third-party devices.
- NE adaptation package: Flexible NE packages can implement rapid device adaptation, increasing the types and functions of managed devices.



eSight provides hierarchical, domain-based, and time-based authorization and flexible network user authentication methods.

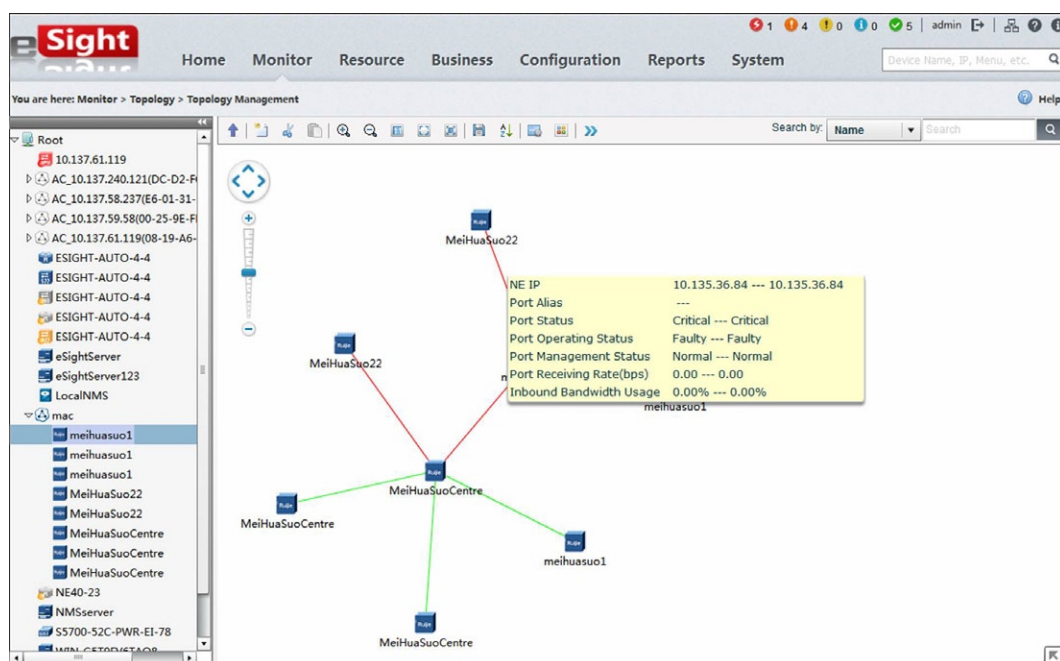
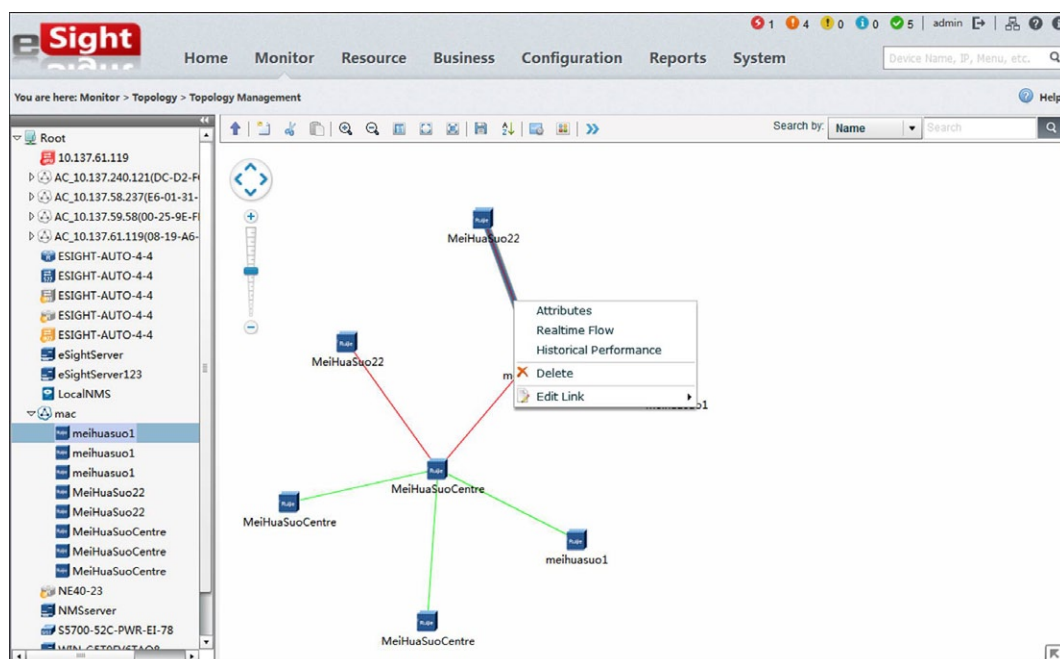
- By assigning different user name and passwords to administrators, controlling administrator management authority, management range, time range allowed to log in, and IP range allowed to log in, eSight can implement a refined management authorization.
- eSight supports LDAP, RADIUS, and local authorization methods.

The comprehensive fault monitoring system enables real-time fault diagnosis and provides instructions for quick troubleshooting.

- eSight provides alarms for all types of faults, including IP, IT, and service faults.
- eSight provides 24/7 fault monitoring, real-time notification, and remote fault notification.
- The system can quickly switch between fault or topology views and device panels.
- eSight categorizes and shields alarms to reduce the number of alarms displayed.

eSight provides visual management of the whole network topology and status monitoring.

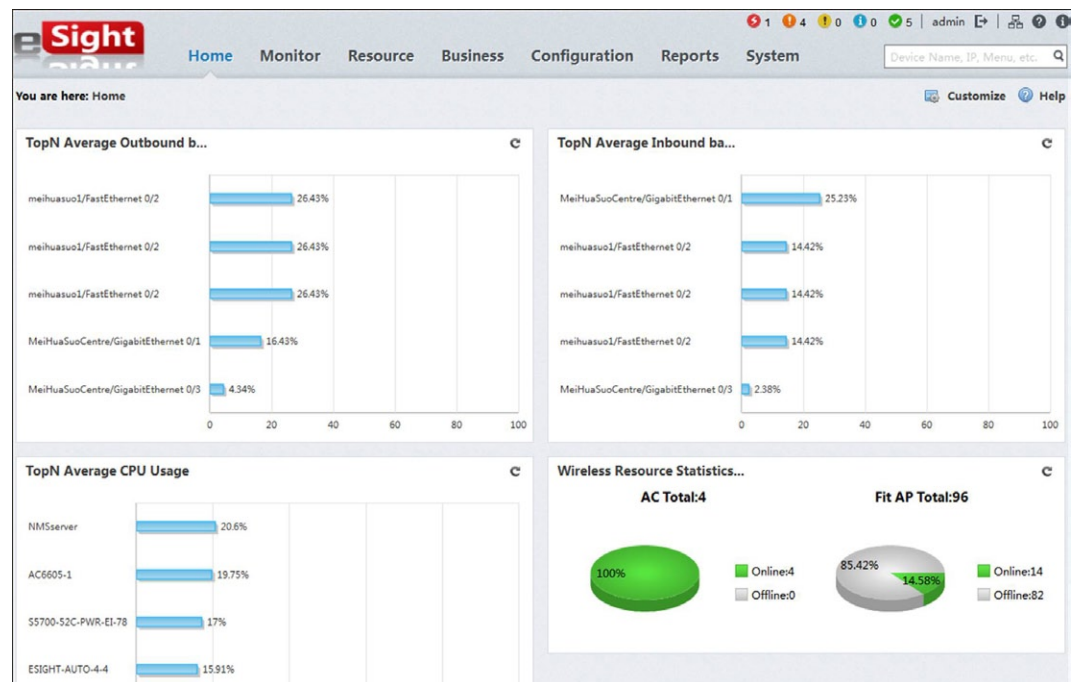
- Various device discovery methods: eSight can discover devices automatically, separately or in a batch. Automatic device discovery model can add new devices periodically. eSight supports IPv6 address devices.
- Various network topology views: eSight provides physical topology and IP topology, shows network structure hierarchically, and shows sub-net, device, and link runtime states by different colors. Administrators can view link basic information, such as device name, link type, link state, bandwidth, reception speed, package reception error rate, package sending error rate, reception package loss rate, and sending package loss rate. Based on the importance of devices, administrators can set the size of device icon. Administrators can zoom out or zoom in on the topology view to show the global view or details.



- eSight shows device, frame, board, sub-card, port on panel, shows port state, and allows administrators to enable or disable ports.
- Powerful performance management: eSight provides performance parameter management templates, supports batch device performance monitoring and visual performance data view, and history data analysis. Administrators can set different alarm severity and threshold. eSight sends an alarm based on the times of performance indexes exceeding the threshold value, improving the alarm function availability.
- Terminal resource management: eSight provides comprehensive terminal access records, including terminal MAC, terminal IP address, terminal device name, IP address, and port number, helping administrators find out the switch and port on the switch through which a terminal is connected to the network based on the terminal MAC or IP address. Administrators can configure the authorized terminal IP address, MAC address, and PORT-IP, PORT-MAC, and IP-MAC matching rules. Then when terminal access illegally, eSight sends emails and record comprehensive information of illegal terminal, provides the basis for illegal user audit.
- Hierarchical network management: Users at headquarters can view alarm, topology, and performance information from lower-level network management systems. Hierarchical network management meets large scale network management requirements.

Simple and convenient daily maintenance operation and lower technical requirements of maintenance stuff, effectively improving work efficiency.

- The customized portal allows users to receive all information in home page. eSight can also integrate third-party software portal to home page.



- Convenient resource searching on the entire network helps administrators quickly locate resources and access corresponding services.
- Intelligent configuration: eSight is preconfigured with multiple common service configuration templates. Users can select an appropriate template to perform the same configurations on devices in a batch or use a file to perform different configurations on different groups of devices in a batch.

- Configuration file management: Configuration files for multiple devices can be backed up, compared, and restored. The backup function includes immediate backup, periodic backup, and backup triggered by device configuration changes.
- MIB management: eSight provides MIB compilation, loading functions and Get, GetNext, Walk, and TableView operations.

Disaster recovery (DR) protection ensures service continuity and system reliability.

- eSight supports two-node clusters in hot standby mode.
- eSight supports the Linux operating system.

Running Environment

Configuration requirements for eSight Unified Network Management Platform (compact edition) are as follows.

Managed Nodes	Hardware	Operating System	Database
0-40	CPU: Dual-core 2.0 GHz or higher Memory: 4 GB Disk space: 40 GB	Windows 7 (32-bit)	MySQL 5.5

Configuration requirements for eSight Unified Network Management Platform (standard edition) are as follows.

Managed Nodes	Hardware	Operating System	Database
0-200	CPU: 1 x dual-core 2 GHz or higher Memory: 4 GB Disk space: 40 GB NOTE: You are advised to use PC servers.	Windows Server 2008 R2 standard (64-bit) + MySQL 5.5 Or Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard Or Novell SUSE Linux Enterprise Server-Multi-language-Enterprise-11.0 SP1 + Oracle Database Standard Edition 11g R2	
200-500	CPU: 2 x dual-core 2 GHz or higher Memory: 4 GB Disk space: 60 GB NOTE: You are advised to use PC servers.		
500-2000	CPU: 2 x quad-core 2 GHz or higher Memory: 8 GB Disk space: 120 GB NOTE: You are advised to use PC servers.		
2000-5000	CPU: 2 x quad-core 2 GHz or higher Memory: 16 GB Disk space: 250 GB NOTE: You are advised to use PC servers.		

Configuration requirements for eSight Unified Network Management Platform (professional edition) are as follows.

Managed Nodes	Hardware	Operating System	Database
0-200	CPU: 1 x dual-core 2 GHz or higher Memory: 4 GB Disk space: 40 GB NOTE: You are advised to use PC servers.	Windows Server 2008 R2 standard (64-bit) + MySQL 5.5 Or Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard Or Novell SUSE Linux Enterprise Server-Multi-language-Enterprise-11.0 SP1 + Oracle Database Standard Edition 11g R2	
200-500	CPU: 2 x dual-core 2 GHz or higher Memory: 4 GB Disk space: 60 GB NOTE: You are advised to use PC servers.		
500-2000	CPU: 2 x quad-core 2 GHz or higher Memory: 8 GB Disk space: 120 GB NOTE: You are advised to use PC servers.		
2000-5000	CPU: 2 x quad-core 2 GHz or higher Memory: 16 GB Disk space: 250 GB NOTE: You are advised to use PC servers.		
5000-20000	CPU: 4 x quad-core 2 GHz or higher Memory: 32 GB Disk space: 320 GB NOTE: You are advised to use PC servers.	Novell SUSE Linux Enterprise Server-Multi-language-Enterprise-11.0 SP1	Oracle Database Standard Edition 11g R2

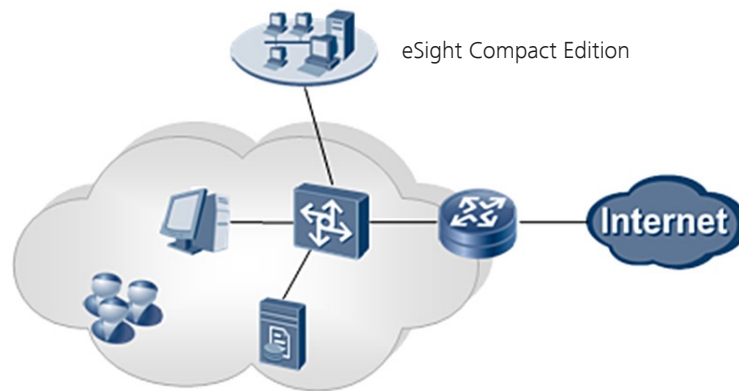
eSight standard and professional editions can run on VMs. Requirements for VMs are as follows.

Managed Nodes	Resources Required by a VM	Operating System	Database
0-500	VMware ESXI 5.0 CPU: 1 x quad-core 2 GHz or higher Memory: 6 GB Disk space: 300 GB	Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard	
500-2000	VMware ESXI 5.0 CPU: 2 x quad-core 2 GHz or higher Memory: 12 GB Disk space: 600 GB		

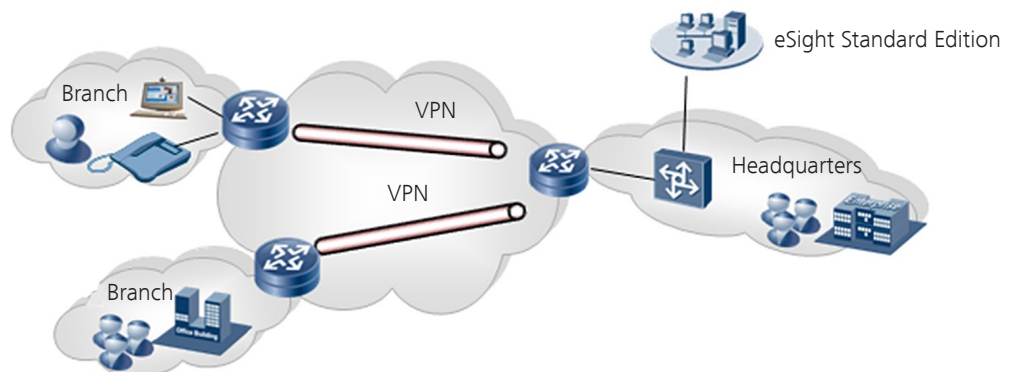
Deployment Scenarios

The eSight network does not have special requirements when managed devices are connected to the eSight server and devices support the Simple Network Management Protocol (SNMP).

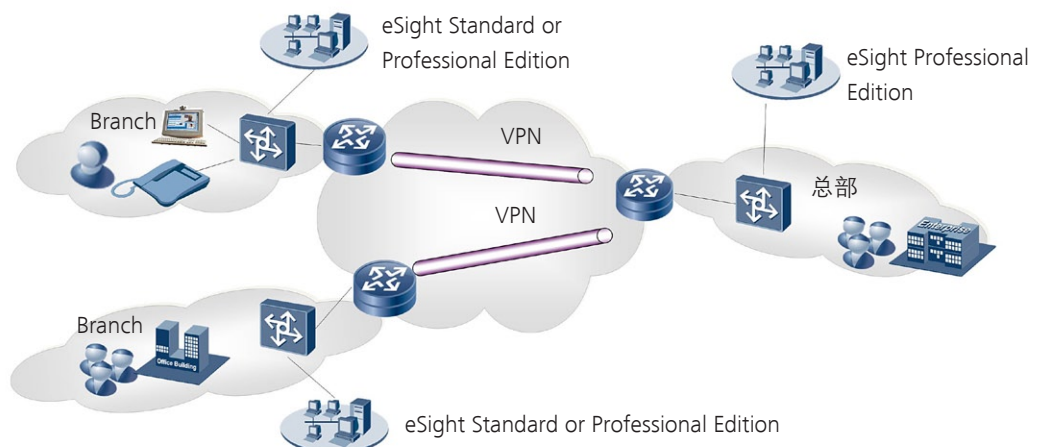
eSight compact edition applies to small- and medium-sized enterprises.



eSight standard edition applies to medium- and large-sized enterprises.



eSight professional edition applies to ultra large enterprises. eSight professional edition is deployed at the headquarters and eSight standard edition or eSight professional edition is deployed at branches. Administrators at the headquarters can check the network status of each branch.



Ordering Information

Ordering information for eSight compact edition

Item	Quantity	Remarks
eSight Application Base-Compact (including 40 device licenses)	1	Mandatory for eSight Unified Network Management Platform.

Ordering information for eSight standard edition

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight Standard NMS License (for 25 incremental devices)	Optional	One license manages 25 incremental devices.
eSight Standard NMS License (for 50 incremental devices)	Optional	One license manages 50 incremental devices.
eSight Standard NMS License (for 100 incremental devices)	Optional	One license manages 100 incremental devices.
eSight Standard NMS License (for 200 incremental devices)	Optional	One license manages 200 incremental devices.
eSight Standard NMS License (for 300 incremental devices)	Optional	One license manages 300 incremental devices.
eSight Standard NMS License- (for 500 incremental devices)	Optional	One license manages 500 incremental devices.
eSight Standard NMS License (for 1000 incremental devices)	Optional	One license manages 1000 incremental devices.
eSight Standard NMS License (for 2000 incremental devices)	Optional	One license manages 2000 incremental devices.
eSight Standard NMS License (for 5000 incremental devices)	Optional	One license manages 5000 incremental devices.
eSight SNMP NBI Component	Optional	Adds SNMP northbound interfaces.

Ordering information for eSight professional edition

Item	Quantity	Remarks
eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight Professional NMS License (for 50 incremental devices)	Optional	One license manages 50 incremental devices.
eSight Professional NMS License (for 100 incremental devices)	Optional	One license manages 100 incremental devices.
eSight Professional NMS License (for 200 incremental devices)	Optional	One license manages 200 incremental devices.
eSight Professional NMS License (for 300 incremental devices)	Optional	One license manages 300 incremental devices.
eSight Professional NMS License (for 500 incremental devices)	Optional	One license manages 500 incremental devices.
eSight Professional NMS License (for 1000 incremental devices)	Optional	One license manages 1000 incremental devices.
eSight Professional NMS License (for 2000 incremental devices)	Optional	One license manages 2000 incremental devices.
eSight Professional NMS License (for 5000 incremental devices)	Optional	One license manages 5000 incremental devices.
eSight SNMP NBI Component	Optional	Adds SNMP northbound interfaces.

eSight Smart Reporter

Product Overview

With rapid network development and continual integration of network applications and service management, information increases remarkably. It is impossible for administrators to obtain valuable information from the bulk information. Therefore, enterprises are in an urgent need of an information management system that can collect, arrange, analyze, and display data to help improve operating efficiency. The information display mode directly affects users' understanding and provides the basis for decision making. eSight provides eSight Smart Reporter as a powerful report tool.

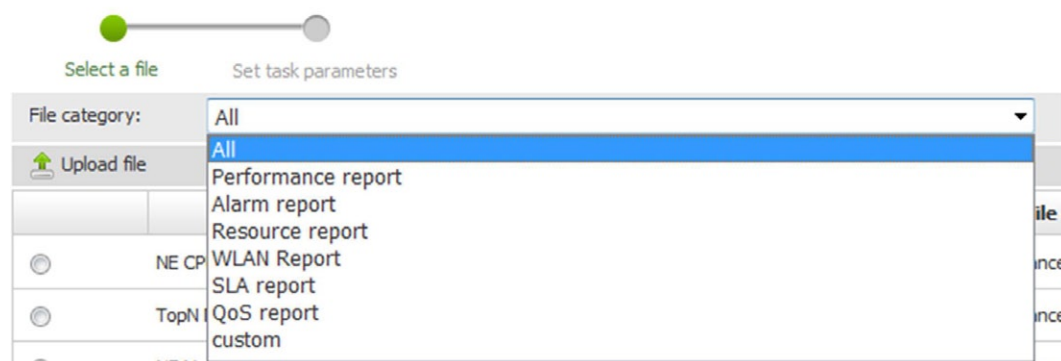
Huawei eSight Smart Reporter provides preset report templates to meet requirements in most maintenance scenarios and provides the professional report design tool for users to customize statistics reports.

Characteristics

eSight Smart Reporter supports right- and domain-based management.

eSight Smart Reporter provides preset report templates to meet requirements in most maintenance scenarios.

eSight provides dozens of preset report templates for various statistics fields, such as performance, alarm, resources, WLAN, service level agreement (SLA), and Quality of Service (QoS), helping users obtain statistics with ease.



The powerful quick report function provides direct resource statistics.

The quick report function collects statistics on the CPU, memory, interface traffic, AP associated resources, AP traffic, AP radio, and terminal traffic. When a user selects the statistics dimension and device resources, eSight generates a report immediately. The user can save the report to the local host and view the report.

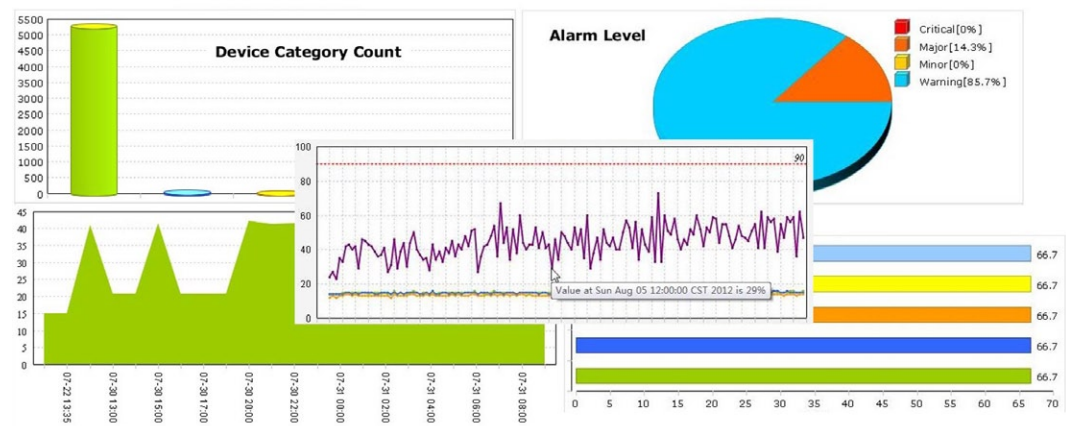
- NE Basic Performance
 - CPU and Memory
 - Interface Flux Stat
- WLAN Performance
 - AP Associated Statistics
 - AP Traffic Statistics
 - AP Radio Statistics
 - Terminal Traffic Statistics

Statistics in multiple dimensions allow users to understand data from various perspectives.

eSight Smart Reporter provides statistics in different dimensions, including top N statistics, statistics at different levels (NE level, subnet level, and region level), interface information (interface connection and disconnection, interface traffic, and interface performance), device resource usage (CPU and memory), and wireless resource usage (access users, AP traffic, AP rate, AP access failure, air interface usage, and AP radio).

Reports in multiple modes present statistics directly and intuitively.

eSight Smart Reporter supports not only tables but also graphs such as line charts, column charts, and pie charts, presenting users with concise and direct statistics.



Reports in multiple file formats apply to various scenarios.

eSight allows users to export report statistics into Excel, Word, or PDF files.

The screenshot shows the "Export Report" dialog box with the following details:

- Export Format:** A dropdown menu currently showing "Excel". A red message states: "Reports exported in Excel contain no figures." The menu also lists "Excel", "PDF", and "Word".
- Page Selection:** The "All pages" radio button is selected.
- Pages:** A text input field for specifying page numbers or ranges.
- Instructions:** "(Enter page number(s) and/or page range(s). For example: 1-6 or 1,3,6)"
- Layout Options:** "Actual size" is selected over "Fit to whole page".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Flexible report settings meet various statistics requirements.

- eSight supports both manual reports and periodic reports. Users can specify the time interval for executing report tasks periodically.
- Users can set the time range for statistics.
- eSight can collect statistics on multiple NEs simultaneously.
- eSight can automatically send reports to users by email.

☒ Send email

⚠ Please check the "System configuration> Basic Settings> Email Server Settings" firstly.

Recipient:

Subject: Report format:

Body:

- Users can specify the peak hours for eSight to collect data generated during the peak hours.

Report System Configuration > **Busy Time Configuration** Help

⚠ You can set the aggregation busy time range. The aggregation time is expressed in intervals. Each check box represents a time range of one hour.

☐ 00:00~01:00
 ☐ 01:00~02:00
 ☐ 02:00~03:00
 ☐ 03:00~04:00
 ☐ 04:00~05:00
 ☐ 05:00~06:00
 ☐ 06:00~07:00
 ☐ 07:00~08:00
 ☐ 08:00~09:00
 ☐ 09:00~10:00
 ☐ 10:00~11:00
 ☐ 11:00~12:00
 ☐ 12:00~13:00
 ☐ 13:00~14:00
 ☐ 14:00~15:00
 ☐ 15:00~16:00
 ☐ 16:00~17:00
 ☐ 17:00~18:00
 ☐ 18:00~19:00
 ☐ 19:00~20:00
 ☐ 20:00~21:00
 ☐ 21:00~22:00
 ☐ 22:00~23:00
 ☐ 23:00~00:00

Running Environment

eSight Smart Reporter is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios

The deployment scenarios for eSight Smart Reporter are the same as those for eSight Unified Network Management Platform.

Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight Smart Reporter	1	Mandatory for eSight Smart Reporter.
eSight Smart Reporter-Special Services-customize template development (for each template)	Optional	Indicates the number of customized templates.

eSight SLA Manager

Product Overview

When the number of services carried by the IP network increases, optimal user experience is difficult to guarantee. Administrators must detect potential faults in advance and use efficient fault diagnosis methods to quickly troubleshoot and recover services.

Huawei eSight SLA Manager integrates with device NQA function to diagnose and measure the link performance between network devices 24/7 hours and displays QoS statistics. Administrators can set the QoS threshold. eSight notifies administrators remotely when QoS reaches the threshold. Administrators can also use the quick diagnosis function to monitor link performance in real time and diagnose faults, which improves maintenance efficiency.

Characteristics

Service-oriented SLA and easy operation simplify O&M needs.

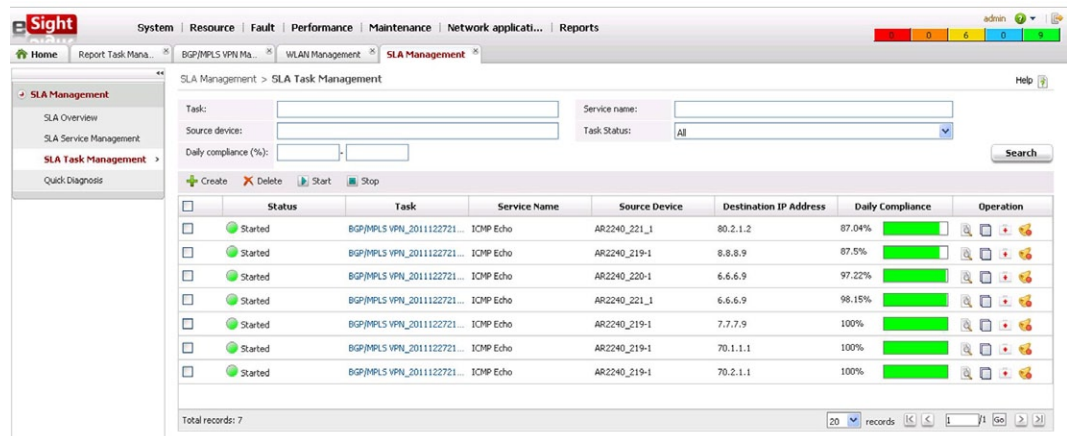
Users can create an SLA service to carry out E2E network QoS monitoring and evaluate network and service QoS based on SLA compliance. eSight has more than 20 SLA service configuration items for video, audio, and network applications, allowing customers to define SLA services to meet their particular requirements.

Service Name	Description	Rating	Compliance Threshold (%)	Type	Status	Operation
Video	Video	4-star	80	Predefined	Unused	[Icon]
Audio	Audio	5-star	80	Predefined	Unused	[Icon]
Data	Data	3-star	80	Predefined	Unused	[Icon]
Web page browsing	Web page browsing	4-star	80	Predefined	Unused	[Icon]
FTP application	FTP application	4-star	80	Predefined	Unused	[Icon]

Total records: 20

eSight SLA Manager displays network QoS statistics and generates alarms in advance to ensure user experience.

After a user creates an SLA task, the task will be executed periodically. QoS statistics are displayed based on daily compliance. When QoS meets the threshold conditions, eSight notifies administrators remotely. Administrators can diagnose faults in advance to ensure user experience.

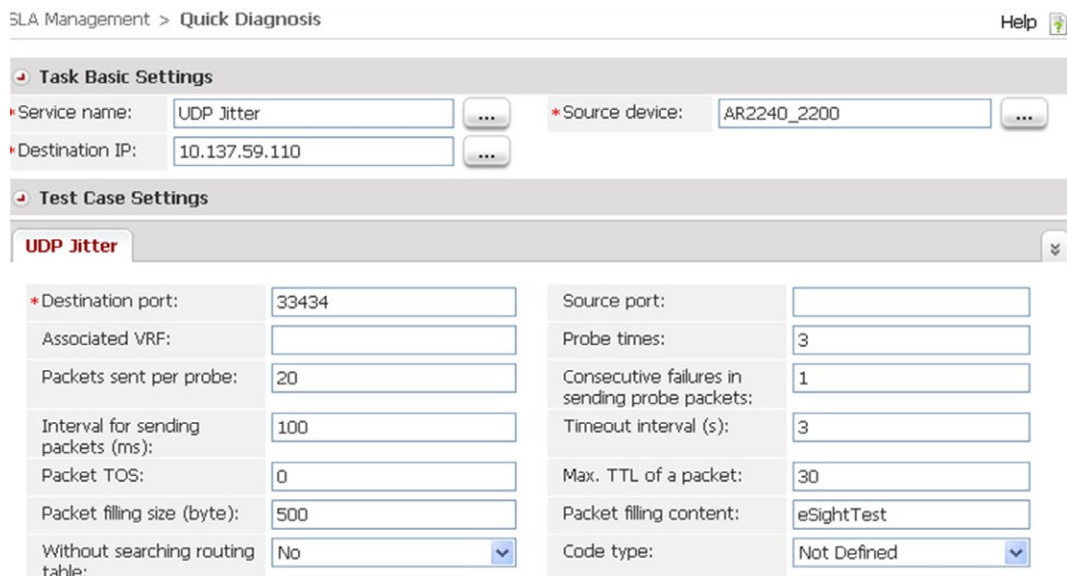


The screenshot shows the 'SLA Management' section of the eSight interface. It includes a sidebar with 'SLA Management', 'SLA Overview', 'SLA Service Management', 'SLA Task Management', and 'Quick Diagnosis'. The main area displays a table of SLA tasks with columns for Status, Task, Service Name, Source Device, Destination IP Address, Daily Compliance, and Operation. The table lists 7 tasks, all with a 'Started' status and 100% daily compliance. The tasks are for ICMP Echo tests between various source devices and destination IP addresses.

Status	Task	Service Name	Source Device	Destination IP Address	Daily Compliance	Operation
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_221_1	80.2.1.2	87.04%	[Icons]
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_219-1	8.8.8.9	87.5%	[Icons]
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_220-1	6.6.6.9	97.22%	[Icons]
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_221_1	6.6.6.9	98.15%	[Icons]
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_219-1	7.7.7.9	100%	[Icons]
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_219-1	70.1.1.1	100%	[Icons]
Started	BGP/MPLS VPN_2011122721...	ICMP Echo	AR2240_219-1	70.2.1.1	100%	[Icons]

eSight SLA Manager provides the quick diagnosis function to narrow the fault scope and shorten the fault diagnosis time.

eSight provides the quick diagnosis function for users to locate faults by link segments, narrowing the fault scope.



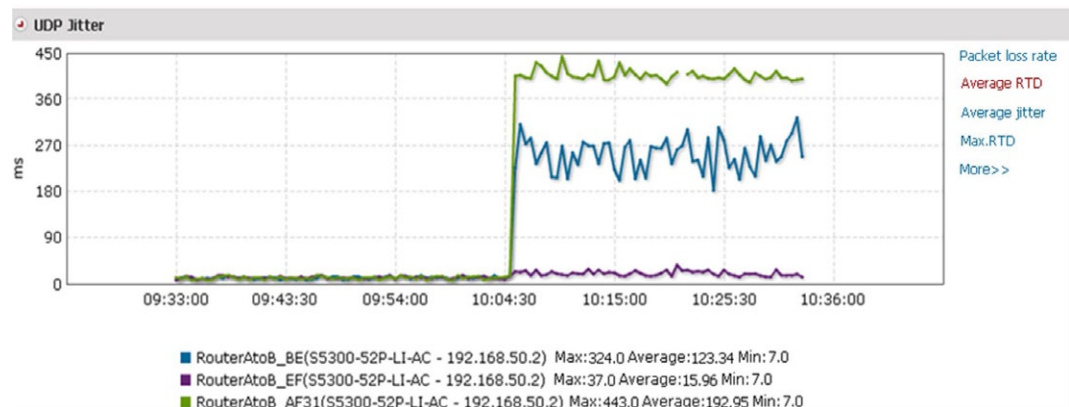
The screenshot shows the 'Quick Diagnosis' section of the eSight interface. It includes a sidebar with 'SLA Management' and 'Quick Diagnosis'. The main area displays 'Task Basic Settings' and 'Test Case Settings'. The 'Task Basic Settings' section includes fields for Service name (UDP Jitter), Source device (AR2240_2200), and Destination IP (10.137.59.110). The 'Test Case Settings' section includes fields for Destination port (33434), Associated VRF, Packets sent per probe (20), Interval for sending packets (ms) (100), Packet TOS (0), Packet filling size (byte) (500), Without searching routing table (No), Source port, Probe times (3), Consecutive failures in sending probe packets (1), Timeout interval (s) (3), Max. TTL of a packet (30), Packet filling content (eSightTest), and Code type (Not Defined).

Task Basic Settings	
*Service name:	UDP Jitter
*Source device:	AR2240_2200
*Destination IP:	10.137.59.110

Test Case Settings	
*Destination port:	33434
Associated VRF:	
Packets sent per probe:	20
Interval for sending packets (ms):	100
Packet TOS:	0
Packet filling size (byte):	500
Without searching routing table:	No
Source port:	
Probe times:	3
Consecutive failures in sending probe packets:	1
Timeout interval (s):	3
Max. TTL of a packet:	30
Packet filling content:	eSightTest
Code type:	Not Defined

Visible historical network data provides a basis for network optimization.

In actual applications, different QoS values indicate services of different priorities. Different services on a same link can be compared. The comparison result shows whether QoS on a network has taken effect and provides a basis for QoS policy adjustment.



Running Environment

eSight SLA Manager is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios

The deployment scenarios for eSight SLA Manager are the same as those for eSight Unified Network Management Platform. Source devices must be added to eSight. The IP addresses of the source and destination devices can be pinged.

Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight SLA Manager	1	Mandatory for eSight SLA Manager.

WLAN Manager

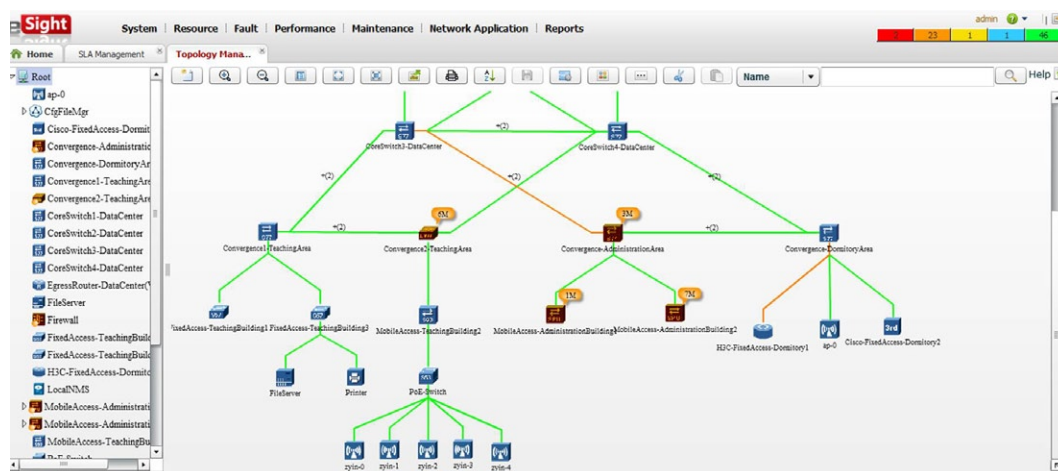
Product Overview

With network development, Wireless Fidelity (Wi-Fi), a low-cost and highly efficient network deployment and maintenance mode, has been widely recognized by customers. However, Wi-Fi's high requirements on environment and distributed deployment of a large number of ACs and APs on WLAN networks have made the maintenance costly and difficult. Therefore, an easy-to-use and efficient WLAN management system is the key to ensure enterprise E2E operations.

Huawei eSight WLAN Manager integrates the management of wired and wireless networks and implements batch service deployment, service adjustment, troubleshooting, and routine maintenance.

Characteristics

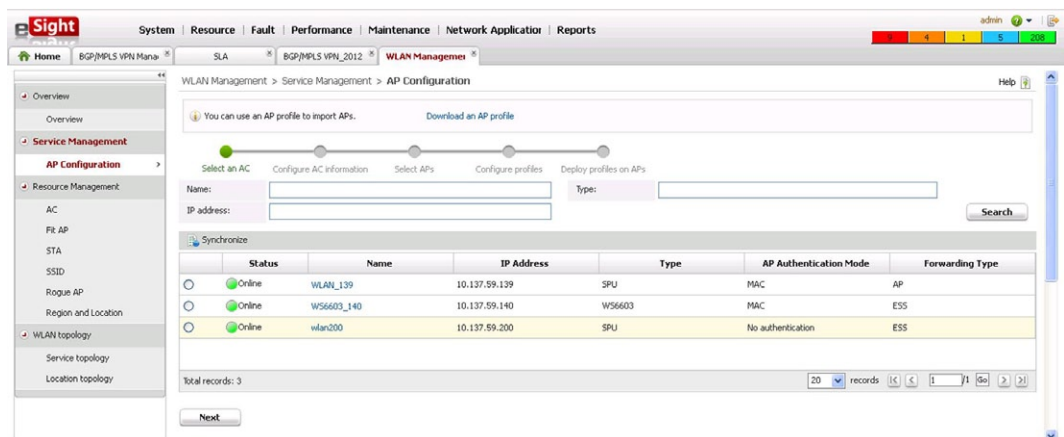
eSight WLAN Manager integrates the management of wired and wireless networks.



In eSight physical topology, users can monitor switches, routers, security devices, IT devices, H3C devices, and Cisco devices in a unified manner. By centralized management of wired and wireless devices, such as ACs, power over Ethernet (PoE) switches, and APs, users can directly view device connections, status, and alarms on the entire network.

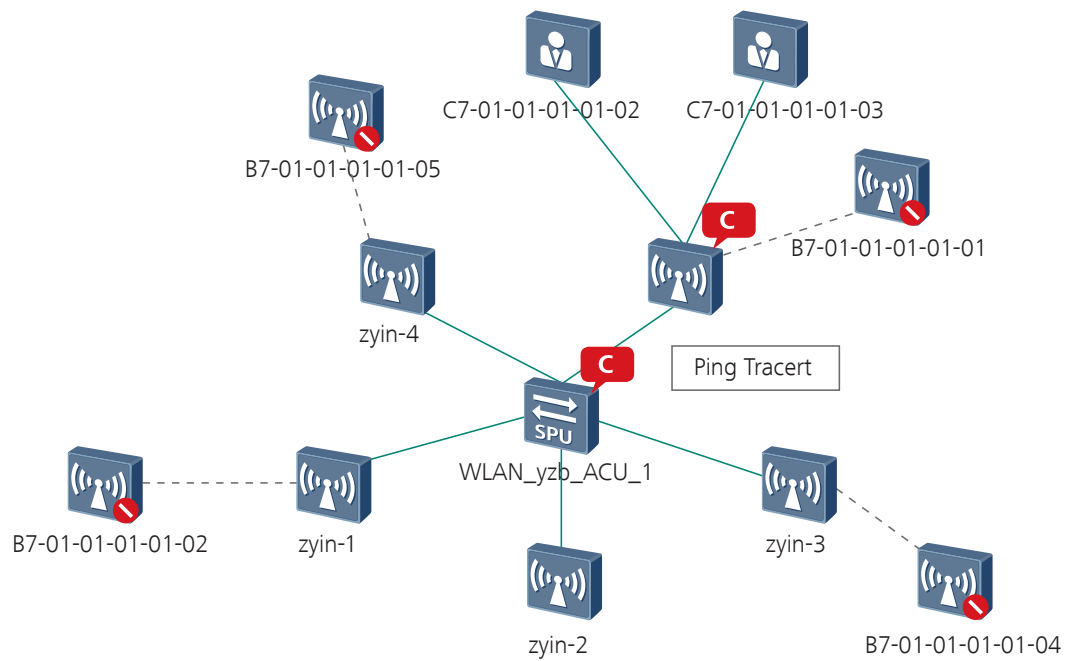
Deploying services on wireless devices in batches improves the management efficiency.

Users can use the wizard to deploy services, greatly accelerating service deployment rate. Users can manage Huawei ACs to configure WLAN services. AP configurations are stored on the AC. After tunnels are set up between the AC and APs, the APs obtain the configurations from the AC.

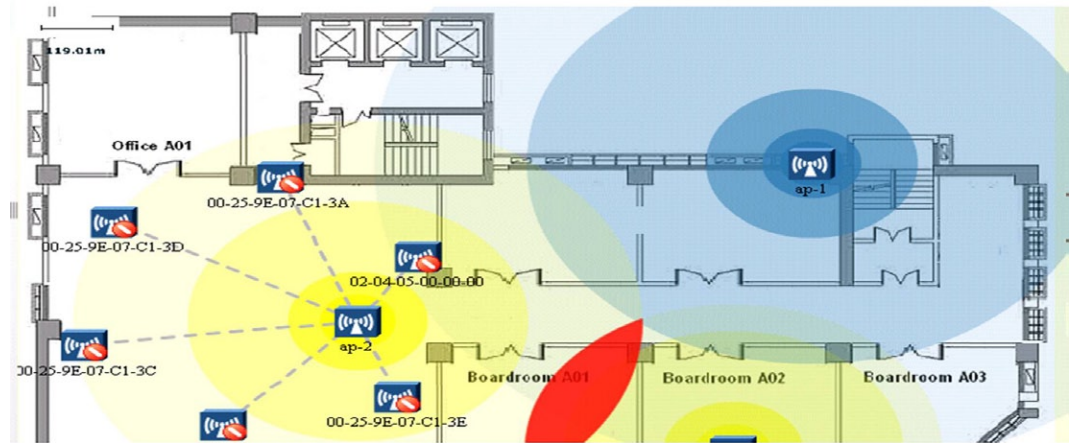


Various topology views help users to understand the wireless network status in different dimensions.

Service topology: The service topology shows connections between the ACs, APs, and STAs and marks rouge APs. Users can view the detailed information about the ACs, APs, STAs, and rouge APs and diagnose wireless service faults (such as by the ping operation).



Location topology: The location topology shows the hotspots and radio signal coverage scope and marks unauthorized APs and collision domains. The color indicates the frequency band, and the color depth indicates signal strength. The red area indicates collision domains. In the location topology, users can set blocks to test the impact of different blocks on signal attenuation.



Real-time WLAN Location Service

- WLAN manager provides wireless location features for system users to locate unauthorized APs, Ad-hoc networks, unauthorized network bridges, and interferences. These features have significant meaning for wireless network troubleshooting, security and marketing requirements based on WLAN location services.

Wireless Network Security Detection

The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non-Wi-Fi interferences, and provides frequency spectrum analysis features.

- WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. When detecting an interference, the WIDS chooses whether to generate an alarm or not based on user alarm configurations.

Overview

Service Management

Configuration Wizard

Resource Management

AC

Fit AP

Client

SSID

Region

Client Access History

WLAN Topology

Service Topology

Location Topology

WIDS Management

Rule

BSSID:

Channel:

SSID:

Rule:

Synchronize

BSSID	Device type	SSID	Rule	Classification	RSST (dBm)	Channel	Last Detec Time
4C-1F-CC-45-B3-FB	AP	FatAP153-1	RogueAp	Rogue	-45.00	1	2013-05-20 06:55:43
80-F8-06-76-99-81	AP	y00201692-2000...	test	Rogue	-60.00	1	2013-05-20 06:56:43
80-F8-06-76-99-80	AP	z00109358wlan200	test	Rogue	-59.00	1	2013-05-20 06:56:43
00-25-9E-26-A3-97	AP	test1234	test	Rogue	-53.00	11	2013-05-20 06:58:43
4C-1F-CC-45-B3-FA	AP	h1	test	Rogue	-45.00	1	2013-05-20 06:55:43
4C-1F-CC-45-B3-FC	AP	esighttest	test	Rogue	-44.00	1	2013-05-20 06:55:43
4C-1F-CC-45-B3-F7	AP		test	Rogue	-44.00	1	2013-05-20 09:44:45
B9-01-15-08-01-04	AP	wlanAccess	test	Rogue	-60.00	6	2013-03-21 03:02:05
0C-37-DC-48-E0-9A	AP	MobileWiFi-e09a			-83.00	1	2013-05-20 08:52:06
B9-01-15-08-01-05	AD Hoc	wlanAccess			-90.00	11	2013-03-21 03:02:05

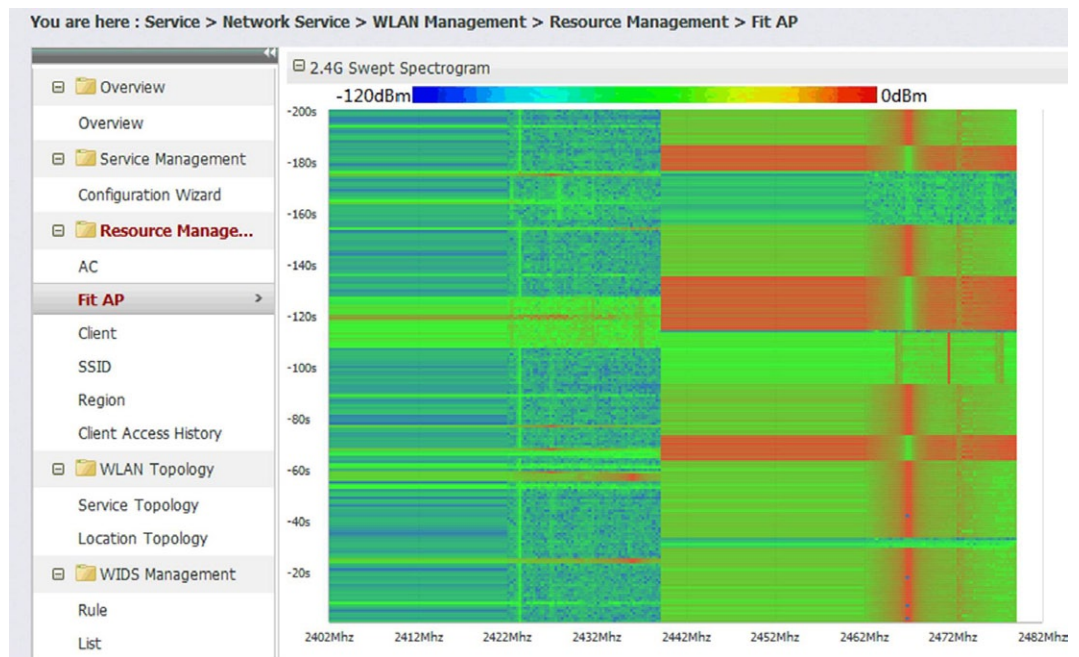
20

Total records: 10

Previous

Next

- Frequency spectrum analysis: Users can obtain the channel quality and interference source information from spectrograms, which contain real-time grams, in-depth grams, channel quality grams, channel quality trend grams, and device duty cycle.



The WIDS provides the detailed interference source list and the influences of these interference sources on normal APs.

Position : Network Application > Network Application Management > WLAN Management > WIDS Management > List

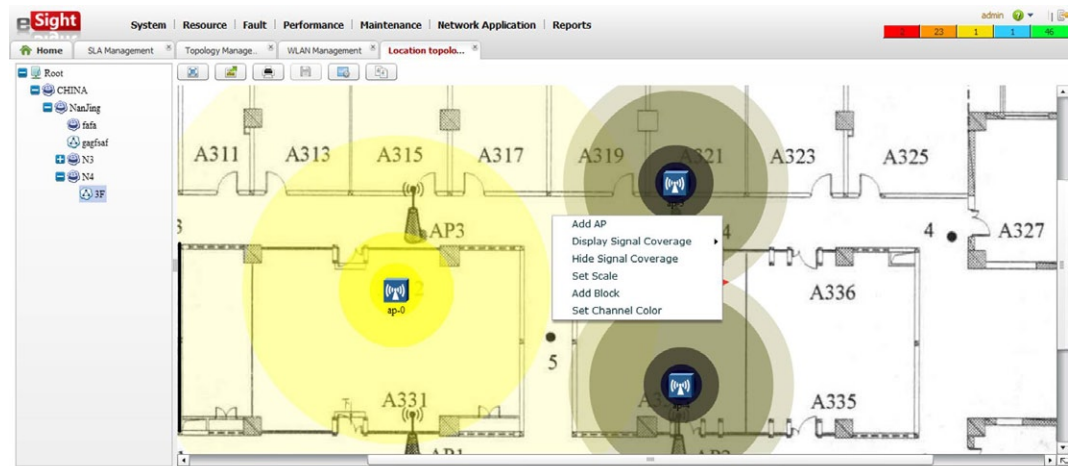
Help

BSSID: Channel: SSID: Rule: Search Advanced

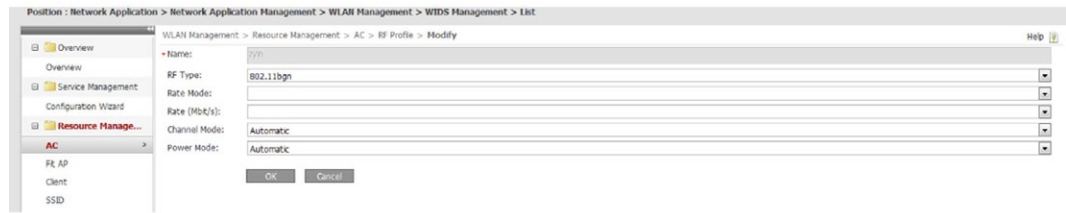
BSSID	SSID	Rule	Classification	RSSI (dBm)	Channel	Last Detect Time
24:0B:AC:34:09:87	m3			-93.00	4	2012-11-24 16:5...
00:23:81:28:FF:30	AndroidAP-Lenovo			-93.00	6	2012-11-24 20:3...
5C:4C:A9:08:08:A1	X00109358wlan200			-91.00	11	2012-11-24 15:4...
24:89:58:58:19:A2	g00220917-wpa2-comp			-77.00	4	2012-11-24 19:5...
E4:1F:13:C5:16:18				-75.00	1	2012-11-24 19:4...
54:89:58:58:19:A1	g00220917-share-key			-75.00	4	2012-11-24 15:4...
7C:61:92:12:62:94	HTC Portable Hotspot			-73.00	1	2012-11-24 17:4...
3B:72:06:16:07:89				-73.00	12	2012-11-24 19:4...
78:1D:8A:53:7F:81				-70.00	11	2012-11-24 19:4...
2C:69:28:65:6C:3C				-65.00	5	2012-11-24 20:3...
54:89:58:58:19:A3	g00220917-wpa2-comp			-61.00	4	2012-11-24 17:3...
F0:0E:F1:40:22:31				-60.00	10	2012-11-24 19:4...
00:10:10:10:10:10				-60.00	11	2012-11-24 19:4...

Provides quick service adjustment to cover hotspots and optimize the radio frequency.

If a coverage hole exists on the network, users can use eSight WLAN Manager to quickly deploy services on new APs to cover hotspots.



When a carrier's APs or private APs occupy the planned channels and interfere with APs on the live network, users can use eSight WLAN Manager to quickly change the channel if negotiation is unavailable.



Quick AP fault diagnosis



eSight can restart, replace, and restore APs to factory settings in a batch.

- During WLAN network debugging or when APs are faulty, users can remotely restore APs to factory settings in a batch using eSight.
- During WLAN network debugging or when APs are upgraded, users can remotely restart APs in a batch using eSight.
- If an AP is faulty, users can quickly replace the AP in eSight. The replacement does not affect AP configurations.

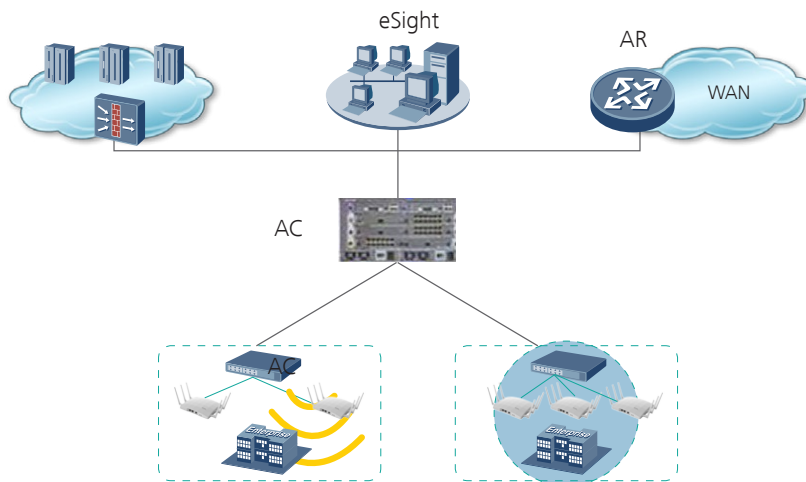
Resource statistics meets O&M requirements.

- Entire-network resource statistics: An online user line chart shows the top 5 accessed fit APs and SSIDs, top 5 device alarms, and physical resource statistics on the entire network.
- AC statistics: A line chart shows statistics about online users collected by AC, including AP information, domain information, and top 5 AC alarms.
- AP statistics: top 5 AP alarms and AP performance counters (including the number of terminals connected to APs, AP physical attributes, AP traffic, and radio traffic).
- SSID statistics: number of APs, number of VAPs, and number of terminals connected to APs.
- Region and location statistics: total number of APs, number of online APs, and number of online STAs by region and location.

Running Environment

eSight WLAN Manager is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios



Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight WLAN Manager	1	Mandatory.
eSight WLAN License (for 50 APs)	Optional	One license manages 50 incremental APs.
eSight WLAN License (for 100 APs)	Optional	One license manages 100 incremental APs.
eSight WLAN License (for 200 APs)	Optional	One license manages 200 incremental APs.
eSight WLAN License (for 500 APs)	Optional	One license manages 500 incremental APs.
eSight WLAN License (for 1000 APs)	Optional	One license manages 1000 incremental APs.
eSight WLAN License (for 2000 APs)	Optional	One license manages 2000 incremental APs.
eSight WLAN License (for 5000 APs)	Optional	One license manages 5000 incremental APs.
eSight WLAN Real-Time Location System (RTLS)	Optional	WLAN Real-Time Location Function.
eSight WLAN RTLS -5 Application Base Location Services License	Optional	One license manages 5 incremental RTLS APs.
eSight WLAN RTLS -25 Application Base Location Services License	Optional	One license manages 25 incremental RTLS APs.
eSight WLAN RTLS -100 Application Base Location Services License	Optional	One license manages 100 incremental RTLS APs.

eSight Network Traffic Analyzer

Product Overview

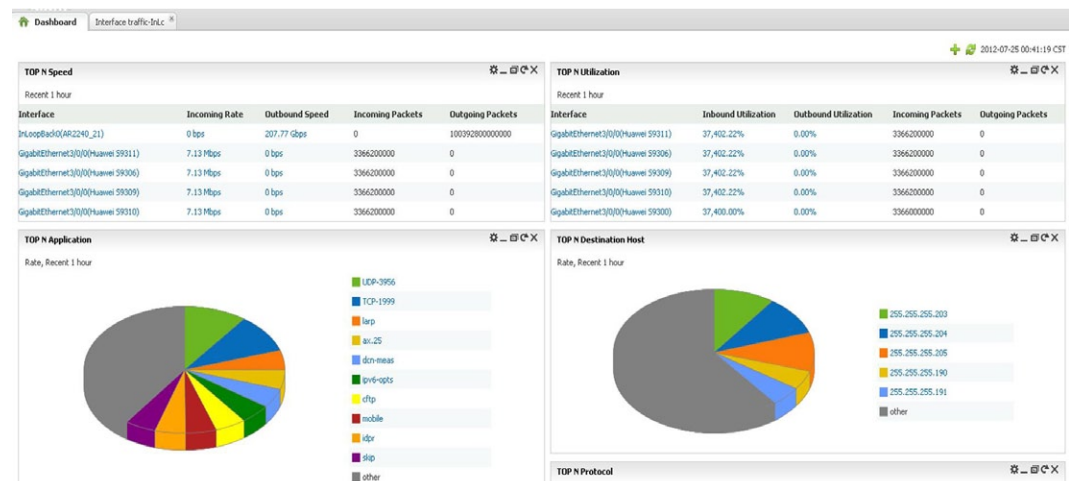
Fast and stable access speeds improve office work efficiency, while low access speeds often affect office work. Administrators need to determine which applications consume a lot of bandwidth and generate heavy traffic and which employees use these applications, change the network QoS policy, and expand the network when necessary.

eSight Network Traffic Analyzer (NTA) supports NetFlow, NetStream, and sFlow. eSight Network Traffic Analyzer collects traffic information output by routers and Layer 3 switches, and provides user-defined reports for network administrators to analyze so that they can learn about traffic and bandwidth usage and detect network bottlenecks. eSight Network Traffic Analyzer also provides information that network administrators can use for network planning and troubleshooting.

Characteristics

eSight Network Traffic Analyzer supports mainstream network traffic protocols including NetStream, NetFlow, and sFlow.

Customized Dashboard page



- Multiple dimensions: eSight Network Traffic Analyzer ranks the traffic on devices and interfaces, interface usage traffic, application traffic, host traffic, session traffic, and DSCP traffic.
- Customization: eSight Network Traffic Analyzer allows users to customize the presented content, format, and formatting style and supports partial traffic update without changing the GUI.
- The interface traffic rankings and interface usage rankings display interface traffic statistics, including the incoming rate, outgoing rate, incoming data packets, and outgoing data packets. You can click an interface and learn about the traffic composition on this interface at different time based on multiple dimensions including the application, host, session, and DSCP.

Customized Traffic Applications and Group Network Traffic

You can customize traffic applications and group network traffic, as follows:

- Customized applications
- Customized DSCP group
- Customized application group
- Customized IP address group or interface group

Customized Applications

- Customized application: eSight Network Traffic Analyzer components are recognized based on the protocol and port number, and hundreds of standard applications and common Layer 4 applications are preset. Protocols and port numbers can also be added in unknown applications. Network administrators can add applications as required. You can customize applications based on the specified protocol, port number, and IP address ranges.

Customized DSCP Group

- DSCP group is a logical group. You can create a group to differentiate DSCP composition. For example, in WAN QoS monitoring, you can create a voice group (EF), a video group (AF31), and a group of the other DSCP. Therefore, eSight Network Traffic Analyzer can provide reference for proper QoS bandwidth planning and key service bandwidth planning for an enterprise.

Customized Application Group

- You can create application groups as required to obtain comprehensive information of specific applications. For example, you can create an application group named Mail Service, and combine Lotus Notes, pop3, and SMTP applications into the group to learn about the traffic of mail applications.

Customized IP Address Group or Interface Group

- You can consider the IP addresses or interfaces in a certain range as a whole to calculate traffic statistics. For example, assume that an enterprise has two floors and you need to calculate the total traffic of the enterprise. You can combine all the switch interfaces on the two floors into an interface group and analyze the total traffic.

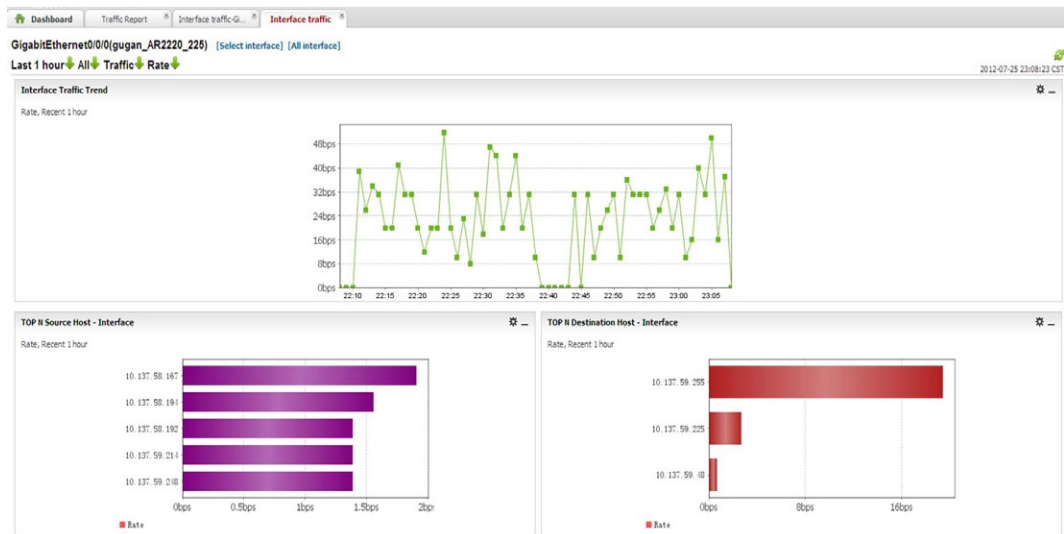
Monitoring Multi-dimensional Traffic

Overall network traffic analysis depends on high performance traffic analysis. Network administrators only need to add a monitoring interface and configure the traffic sampling ratio before monitoring and analyzing traffic of the interface from multiple dimensions, including the following:

- Interface traffic analysis
- Application traffic analysis
- Source/Destination host traffic analysis
- DSCP traffic analysis
- Session traffic analysis

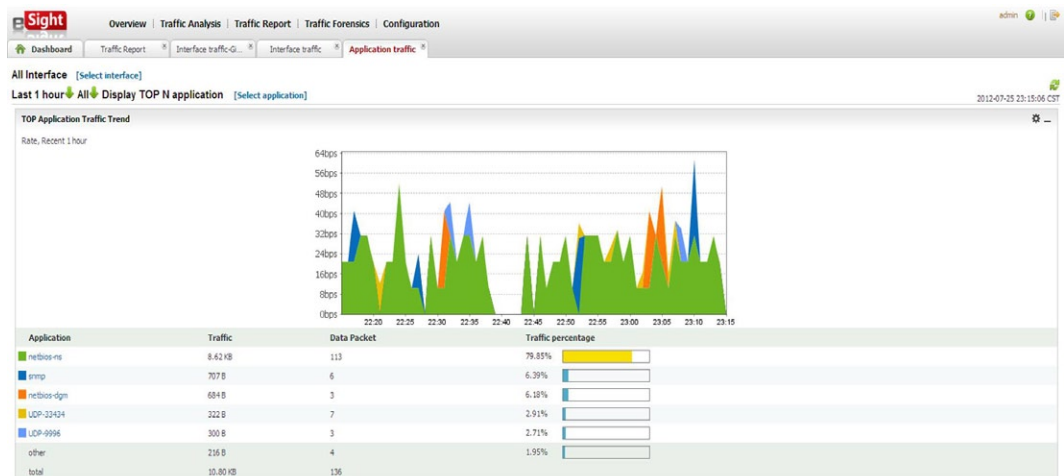
NOTE: You can analyze traffic on the traffic trend diagram, which displays traffic and packets respectively on two coordinates.

Interface Traffic Analysis



Interface traffic analysis checks the trend of traffic for a specified interface, time range, and incoming and outgoing traffic. Based on interface traffic analysis, network administrators can identify the interfaces that are used most frequently on the network so that they can have a comprehensive understanding about the whole network status. Administrators can detect interfaces with abnormal traffic in time and locate faults before network performance is affected.

Application Traffic Analysis



Application traffic analysis checks the trend of application changes for a specified interface, time range, and incoming and outgoing traffic. Administrators can locate the host that causes performance problems based on the source ranking and destination hosts using a specific application.

Source/Destination Host Traffic Analysis

Source/destination host traffic analysis checks the trend in changes of source/destination host bandwidth usage for a specified interface, time range, and incoming and outgoing traffic. Based on source/destination host analysis, network administrators can identify the host that consumes a high bandwidth and solve any bandwidth problems in time to ensure bandwidth usage efficiency.

Session Traffic Analysis

Session traffic analysis checks the trend of session traffic for a specified interface and time range. Session traffic analysis provides detailed session information that the network administrator can use for further fault location.

DSCP Traffic Analysis

DSCP traffic analysis checks the trend of DSCP traffic for a specified interface and time range. Therefore, you can plan QoS bandwidth properly to ensure the quality of key services.

Group Traffic Analysis

Group traffic analysis displays the traffic statistics of DSCP group, interface group, application group, and IP group on specified interfaces within specific time range. Network administrators can conveniently analyze specific traffic as required to satisfy special maintenance requirements.

Customized Traffic Report

eSight Network Traffic Analyzer can customize reports by specifying filtering rules, report type and report layout configuration. Traffic reports provide references for further network planning.

Network Traffic Report > Create



Abstract

Name:	gugan
Report Category:	Default
Description:	
Interface:	GigabitEthernet0/0/0
Filter:	
Summary Type:	Application summary , Session summary , DSCP summary , Source host summary , Destination host summary
Layout:	Application summary - Pie chart Session summary - Table DSCP summary - Line graph - Traffic Source host summary - Region - Traffic Destination host summary - Region - Traffic
Time Range:	Current time: Before 1days

[Previous](#) [Save](#) [Save and Execute](#) [Cancel](#)

Traffic Auditing

NTA can extract an original data stream based on a specified time range and filtering rules for further analysis and fault location. Original traffic information includes the router address, source address, destination address, application, source port, destination port, protocol, inbound interface, outbound interface, and DSCP, traffic, and data packets.

Back

Name: gugu

Description:

Time Range: From 2012-07-25 22:00:40 To 2012-07-25 22:06:51

Filter:

Router Address	Inbound interface	Outbound interface	Source address	Source port	Destination address	Destination port	Protocol	Apply	DSCP	Traffic (bytes)	Data Packet
10.137.59.225	GigabitEthernet0/0/0		10.107.226.40	2,051	10.137.59.225	161	udp	snmp	C50	1198	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.32	137	10.137.59.255	137	udp	netbios-ns	C50	788	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.57	137	10.137.59.255	137	udp	netbios-ns	C50	788	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.59	137	10.137.59.255	137	udp	netbios-ns	C50	968	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.167	137	10.137.59.255	137	udp	netbios-ns	C50	234B	3
10.137.59.225	GigabitEthernet0/0/0		10.137.59.171	137	10.137.59.255	137	udp	netbios-ns	C50	3908	5
10.137.59.225	GigabitEthernet0/0/0		10.137.59.180	138	10.137.59.255	138	udp	netbios-dgm	C50	2298	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.189	138	10.137.59.255	138	udp	netbios-dgm	C50	2298	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.192	137	10.137.59.255	137	udp	netbios-ns	C50	788	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.194	137	10.137.59.255	137	udp	netbios-ns	C50	234B	3
10.137.59.225	GigabitEthernet0/0/0		10.137.59.216	137	10.137.59.255	137	udp	netbios-ns	C50	1568	2
10.137.59.225	GigabitEthernet0/0/0		10.137.59.217	138	10.137.59.255	138	udp	netbios-dgm	C50	2298	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.228	137	10.137.59.255	137	udp	netbios-ns	C50	788	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.20	54,218	10.137.59.225	33,434	udp	UDP-33434	C50	468	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.31	137	10.137.59.255	137	udp	netbios-ns	C50	788	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.42	137	10.137.59.255	137	udp	netbios-ns	C50	788	1
10.137.59.225	GigabitEthernet0/0/0		10.137.59.46	137	10.137.59.255	137	udp	netbios-ns	C50	234B	3
10.137.59.225	GigabitEthernet0/0/0		10.137.59.59	59,726	10.137.59.225	161	udp	snmp	C50	2298	2

Total records: 18

Running Environment

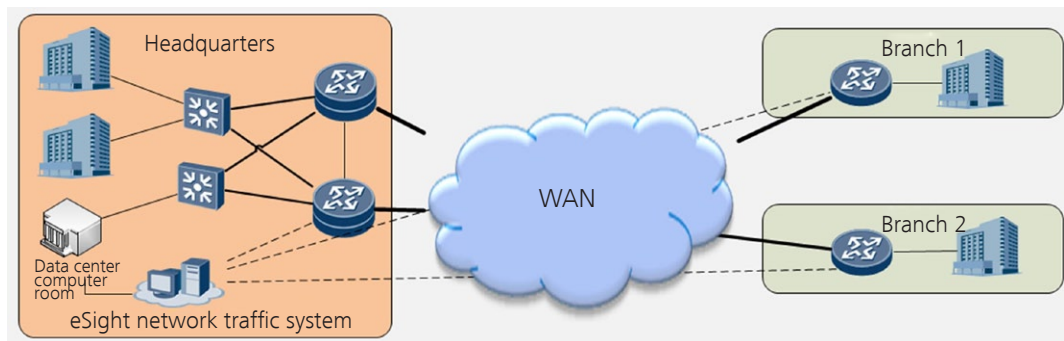
eSight Network Traffic Analyzer can be deployed on the same server as or on different server from eSight Unified Network Management Platform standard or professional edition. Considering the high requirement on server performance in case of huge traffic, you are advised to deploy eSight Network Traffic Analyzer and eSight Unified Network Management Platform on different servers based on the following requirements for running environment.

Managed Nodes	Hardware	Operating System	Database
0–100 (0–10000 flows per second)	CPU: 1 x quad-core 2 GHz or higher Memory: 4 GB Disk space: 120 GB NOTE: You are advised to use PC servers.	Windows Server 2008 R2 standard (64-bit) + MySQL 5.5 Or	
100–350 (10000–30000 flows per second)	CPU: 2 x quad-core 2 GHz or higher Memory: 16 GB Disk space: 250 GB NOTE: You are advised to use PC servers.	Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard	

When eSight Network Traffic Analyzer and eSight Unified Network Management Platform are deployed on different servers, eSight Network Traffic Analyzer can be deployed on a virtual machine (VM). The resource requirements for the VM are as follows.

Managed Nodes	Resources Required by a VM	Operating System	Database
0–100 (0–10000 flows per second)	VMware ESXI 5.0 CPU: 1 x quad-core 2 GHz or higher RAM: 6 GB Disk space: 300 GB	Windows Server 2008 R2 standard (64-bit)	Microsoft SQL Server 2008 R2 standard

Deployment Scenarios



eSight Network Traffic Analyzer enables NetStream on the WAN-link device ports of an enterprise to send traffic information to the eSight Network Traffic Analyzer, which:

- Analyzes the current WAN link traffic composition
- Helps recognize abnormal traffic and junk applications
- Quickly locates the IP address of the terminal that generates abnormal traffic
- Optimizes link application traffic distribution
- Improves WAN link usage
- Recognizes DSCP bandwidth distribution on the enterprise branch egress
- Adjusts service priority policies
- Periodically generates a link interface traffic report
- Detects the network application traffic increase
- Facilitates network plan and expansion in advance

Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard(including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight Network Traffic Analyzer Manager	1	Mandatory for eSight Network Traffic Analyzer.
eSight Network Traffic Analyzer License (for 1 incremental device)	Optional	One license manages 1 incremental device.
eSight Network Traffic Analyzer License (for 2 incremental devices)	Optional	One license manages 2 incremental devices.
eSight Network Traffic Analyzer License (for 5 incremental devices)	Optional	One license manages 5 incremental devices.

MPLS VPN Manager

Product Overview

VPNs are complex. They bear various services such as data, voice, and video. Huawei eSight MPLS VPN Manager is introduced to deal with the complex scenarios such as the following in routine maintenance:

- Shielding complex services and allowing maintenance personnel to know the running status of deployed VPN services in real time and perform troubleshooting in a timely manner.
- Monitoring the bandwidth usage of each service to ensure the priority of emergency command systems and important users.
- Ensuring the cross-region video meeting quality among provinces, cities, counties, and towns.

Huawei eSight MPLS VPN Manager integrates discrete VPN information on the network into visible manageable objects and displays them in topology. Administrators can easily monitor VPN services and diagnose faults to ensure QoS and reliability of key services.

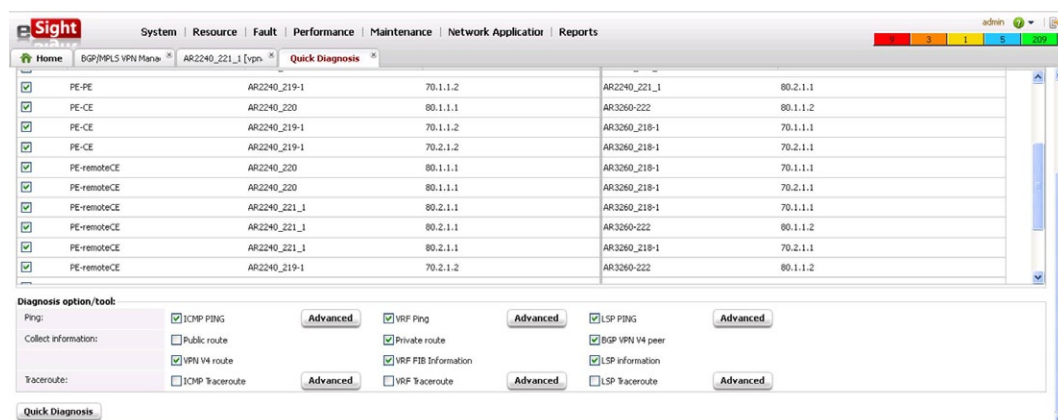
Characteristics

Simple and convenient auto-discovery of services simplifies O&M.

The MPLS VPN Manager combines policies and scopes for service discovery on the entire network. Users do not need to specify device roles. The MPLS VPN Manager can detect various types of networks, including full-mesh, hub-and-spoke, MCE, HoVPN, Inter-AS VPN-Option A, and Inter-AS VPN-Option B networks.

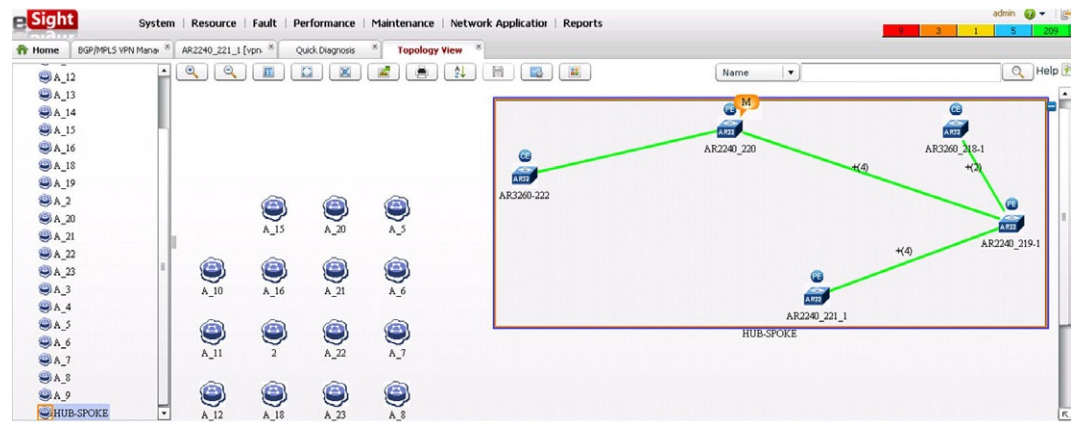
One-click fault diagnosis leads to fast fault identification.

The MPLS VPN Manager can identify service faults at different layers, including the access layer between provider edges (PEs) and customer edge (CEs), and public routes and LSPs between PEs.



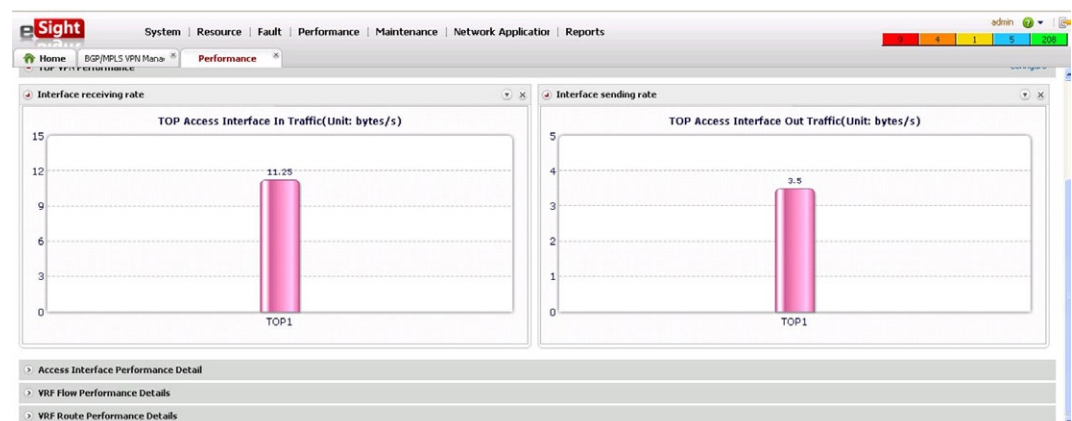
Visual service management facilitates unified monitoring on the entire network and provides real-time services operating status.

The access topology view displays devices based on services currently running on them and displays alarms and the link status of current services for quick diagnosis.

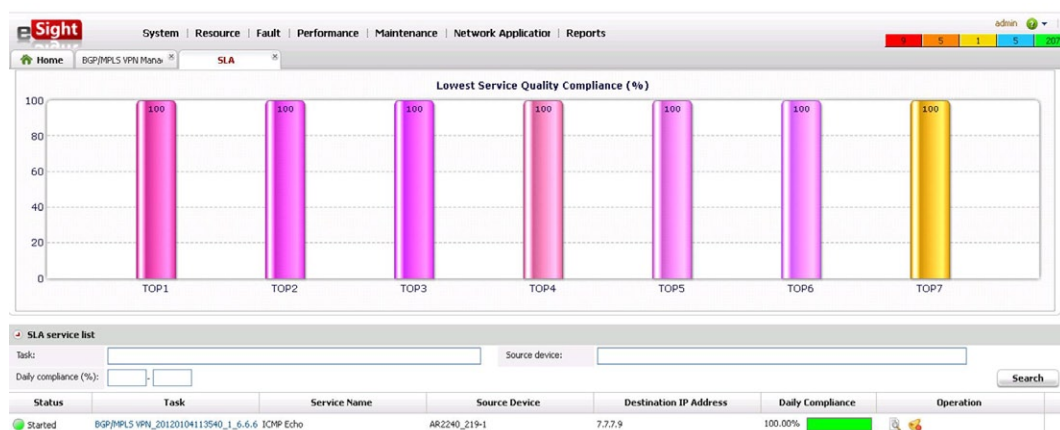


eSight MPLS VPN Manager interacts with report, SLA, and performance monitoring.

Intelligent interaction with performance monitoring: eSight MPLS VPN Manager allows users to customize and view traffic statistics, VRF traffic statistics, and the number of active VRF routes on the 5 or 10 most active access interfaces. eSight MPLS VPN Manager also provides traffic trend charts with detailed counters.



Intelligent interaction with SLA: eSight MPLS VPN Manager provides SLA assessment on service links between a PE and a CE, and between PEs based on ICMP Echo service.

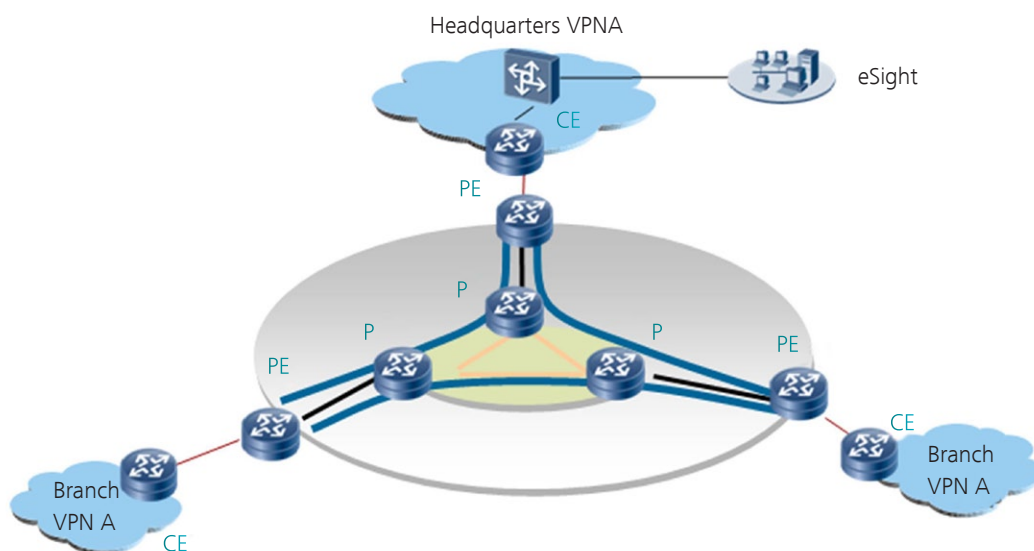


Intelligent interaction with report: eSight MPLS VPN Manager provides interface traffic statistics and service VRF statistics in reports. Customers can export these reports.

Running Environment

eSight MPLS VPN Manager is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios



Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight MPLS VPN manager (including 60 device licenses)	1	Mandatory for eSight MPLS VPN Manager, which can manage 60 PEs and CEs.
eSight MPLS VPN License (for 50 incremental devices)	Optional	One license manages 50 incremental PEs and CEs.
eSight MPLS VPN License (for 100 incremental devices)	Optional	One license manages 100 incremental PEs and CEs.
eSight MPLS VPN License (for 200 incremental devices)	Optional	One license manages 200 incremental PEs and CEs.
eSight MPLS VPN License (for 500 incremental devices)	Optional	One license manages 500 incremental PEs and CEs.
eSight MPLS VPN License (for 1000 incremental devices)	Optional	One license manages 1000 incremental PEs and CEs.
eSight MPLS VPN License (for unlimited number of incremental devices)	Optional	One license manages unlimited number of PEs and CEs, restricted only by the management capability of a specific eSight version.



eSight MPLS Tunnel Manager

Product Overview

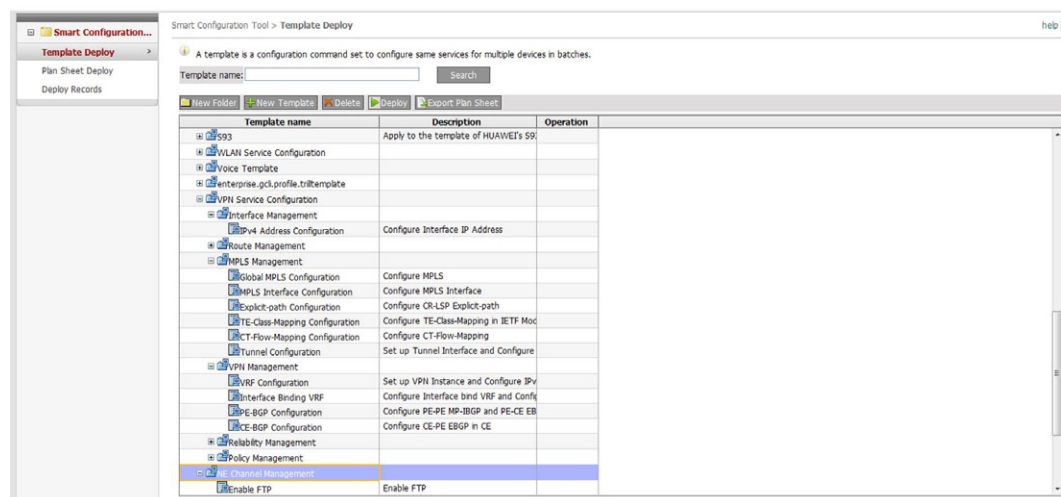
The tunnel technology is widely used on networks. Enterprises choose tunnels based on service features. Generally, LDP tunnels carry services that have low requirements on bandwidth and QoS, and MPLS TE tunnels carry services that have high requirements on bandwidth and QoS. To ensure that services run properly, administrators must know the following tunnel information on the current network: number of tunnels, tunnel types, path of each tunnel, tunnels with the protection function, and whether a tunnel switchover occurs.

eSight MPLS Tunnel Manager automatically discovers the MPLS TE tunnels (RSVP-TE signaling-based dynamic tunnels and CR-Static signaling-based static tunnels) and LDP tunnels that have been deployed on the network, monitors the tunnels in real time, and displays tunnel running status dynamically. In addition, eSight MPLS Tunnel Manager monitors active-standby switchover and bypasses.

Characteristics

eSight MPLS Tunnel Manager allows users to configure tunnel policies using a template, which is easy and efficient.

Users can use the smart configuration tool to deliver tunnel policies in a batch, which reduces errors and improves efficiency.



eSight MPLS Tunnel Manager automatically discovers tunnels deployed on the network to obtain information such as the number of tunnels, tunnel types, and tunnel status.

eSight MPLS Tunnel Manager uses the automatic discovery function to discover the MPLS TE tunnels (RSVP-TE signaling-based dynamic tunnels and CR-Static signaling-based static tunnels) and LDP tunnels that have been deployed on the network to eSight from specified or all devices.

Position : Network Application > Network Application Management > MPLS Tunnel Management > Tunnel Management > Tunnel List

Quick Start
Quick Start
Tunnel Management
Tunnel List
Explicit Path List
Tunnel Topology

Tunnel Name: Running Status: All
Source Node: Sink Node: Search

Auto Discovery Delete

	Running Status	Backup Status	Alarm Severity	Tunnel Name	Tunnel ID	Direction	Source Node	Sink Node	Signaling	Tunnel T...	FRR Stat...	Operation
Down	--	Minor	LDP: 202.92...	--	Unidirectional	L3VPN-P1-18	aodan-PE4-1...	LDP	LDP Tu...	--		
Down	--	Minor	LDP: 202.92...	--	Unidirectional	L3VPN-P1-18	L3VPN-P4-17	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	L3VPN-P2-203	L3VPN-P3-201	LDP	LDP Tu...	--		
Down	--	Minor	LDP: 202.92...	--	Unidirectional	L3VPN-P2-203	aodan-PE1-2...	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE3-2...	aodan-PE1-2...	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE1-2...	aodan-PE4-1...	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE1-2...	L3VPN-P4-17	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE1-2...	L3VPN-P1-18	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE1-2...	L3VPN-P3-201	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE1-2...	L3VPN-P2-203	LDP	LDP Tu...	--		
Up	--		LDP: 202.92...	--	Unidirectional	aodan-PE1-2...	aodan-PE3-2...	LDP	LDP Tu...	--		
Up	UnSwitc...		RSVP-TE: Tu...	111	Unidirectional	aodan-PE1-2...	L3VPN-P4-17	RSVP-TE	Primary...	Enabled		
Up	UnSwitc...		RSVP-TE: Tu...	477	Unidirectional	aodan-PE1-2...	aodan-PE4-1...	RSVP-TE	Primary...	Disabled		
Up	--		RSVP-TE: Tu...	123	Unidirectional	L3VPN-P2-203	L3VPN-P1-18	RSVP-TE	Bypass...	--		
Up	--		RSVP-TE: Tu...	300	Unidirectional	L3VPN-P1-18	L3VPN-P2-203	RSVP-TE	Bypass...	--		

eSight MPLS Tunnel Manager monitors tunnels in real time and dynamically displays the tunnel running status.

When receiving an alarm, eSight MPLS Tunnel Manager notifies users of the tunnel status change in a timely manner. The tunnel topology displays tunnel status and provides entries for users to view the link bandwidth information (such as bandwidth on outbound interfaces or inbound interfaces and maximum reserved bandwidth), link interface information, and whether MPLS is enabled on devices. Such information helps users to diagnose faults.

When receiving an alarm, users can directly access the Tunnel Topology page from the alarm page to check the tunnel status.

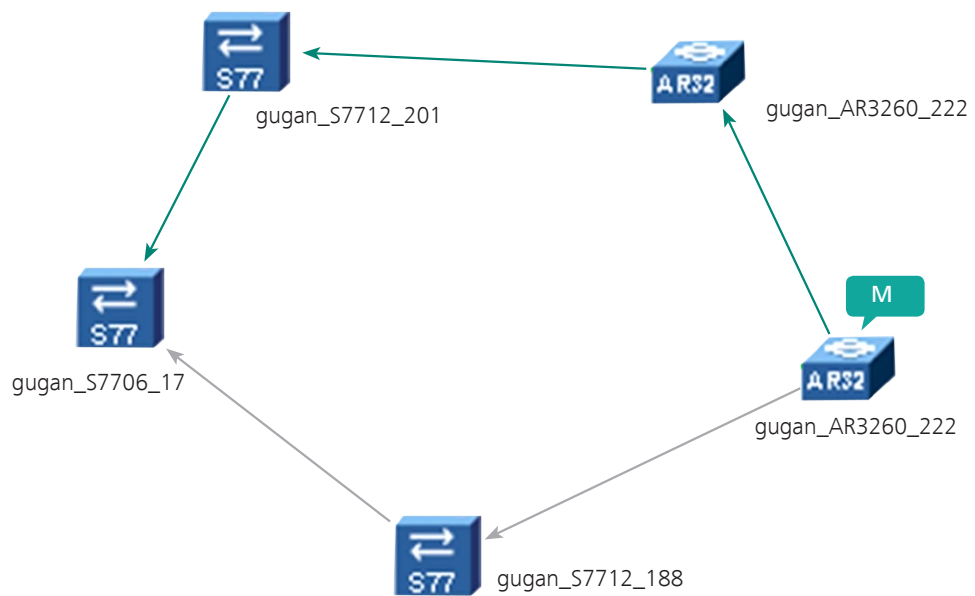
Export Acknowledge Clear More Filter criteria: All alarms

Select Search

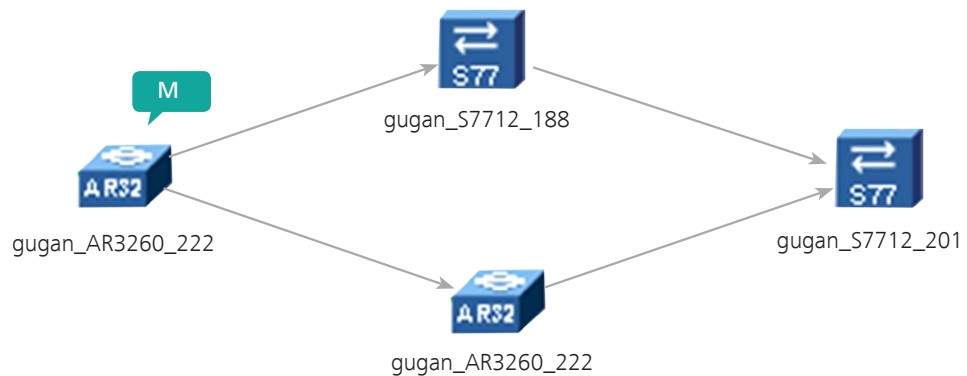
Select	Severity	Acknowledged	Alarm Name	Number of Occ...	Alarm Source	First Occurrence Time	Last Occurrence Time	Object Instance	Operation
	Major		OSPF Neighbor State Changes	43	L3VPN-P2-203	2012-11-24 03:55:33	2012-11-24 21:28:19	Router Id=202.92.36.203,Ne...	
	Major		OSPF Interface State Chang...	43	L3VPN-P2-203	2012-11-24 03:54:49	2012-11-24 21:27:51	OSPF Router Id=202.92.36.2...	
	Critical		Link Down	1	L3VPN-P2-203	2012-11-24 21:27:51	2012-11-24 21:27:51	If Index=476,If Name=Tunn...	
	Major		MPLS Tunnel PrimaryDown	1	L3VPN-P2-203	2012-11-24 21:27:51	2012-11-24 21:27:51	hwMplsTunnelInterfaceName...	
	Major		MPLS ExtTunnel Down	1	L3VPN-P2-203	2012-11-24 21:27:51	2012-11-24 21:27:51	hwMplsTunnelInterfaceName...	
	Major		MPLS Tunnel Failure	1	L3VPN-P2-203	2012-11-24 21:27:51	2012-11-24 21:27:51	Mpls Tunnel Id=123	
	Minor		Ldp Tunnel Down	9	L3VPN-P2-203	2012-11-24 18:50:26	2012-11-24 21:27:45	Egress LSR Id=202.92.36.222	
	Major		Static Tunnel Down	1	aodan-PE1-222	2012-11-24 21:27:44	2012-11-24 21:27:44	Mpls Tunnel Id=212	
	Minor		Ldp Tunnel Down	2	L3VPN-P2-203	2012-11-24 19:49:28	2012-11-24 20:06:09	Egress LSR Id=202.92.36.18	
	Minor		Ldp Tunnel Down	1	aodan-PE1-222	2012-11-24 17:38:38	2012-11-24 17:38:38	Egress LSR Id=202.92.36.203	
	Minor		Ldp Tunnel Down	2	aodan-PE1-222	2012-11-24 17:35:20	2012-11-24 17:38:18	Egress LSR Id=202.92.36.14	
	Minor		Ldp Tunnel Down	1	aodan-PE1-222	2012-11-24 17:38:18	2012-11-24 17:38:18	Egress LSR Id=202.92.36.17	
	Minor		Ldp Tunnel Down	1	aodan-PE1-222	2012-11-24 17:38:18	2012-11-24 17:38:18	Egress LSR Id=1.1.1.190	
	Major		OSPF Interface State Chang...	4	aodan-PE1-222	2012-11-24 17:35:14	2012-11-24 17:38:14	OSPF Router Id=202.92.36.2...	

Jump to Panel
Tunnel Topology
Mask Rules
Redefine Alarm Severity

When detecting that the active LSP is faulty, eSight MPLS Tunnel Manager performs an active-standby switchover or bypasses the faulty LSP. All paths of the original tunnel before the switchover or bypass are unavailable. The active-standby tunnel switchover status is displayed in the tunnel topology.



When an LDP tunnel is faulty, all links in the tunnel topology are unavailable.



eSight MPLS Tunnel Manager cooperates with the MPLS VPN Manager so that users can quickly locate services affected by tunnel faults and check whether a service fault is caused by a tunnel fault.

In the service list of eSight MPLS VPN Manager, users can click Tunnel List to view tunnels that carry a VPN. Users can check whether a service fault is caused by a tunnel fault based on the tunnel status.

Position : Network Application > Network Application Management > BGP/MPLS VPN Management > Service Management > Service List

VPN name: Search

Auto Discovery Delete Enable Disable

VPN Name	Running Status	Enable Status	Alarm Severity	Operation
BGP/MPLS VPN_DCH_20121124034807_1	Up	Disabled		Topology View View Alarms SLA Modify Name Tunnel List
BGP/MPLS VPN_optionA_20121124034807_7	Down	Enabled		
BGP/MPLS VPN_testvpfnr_20121124034930_1	Down	Disabled		
BGP/MPLS VPN_vpna_admin_20121124034807_6	Up	Enabled		
BGP/MPLS VPN_vpna_data_20121124034807_4	Up	Enabled		
BGP/MPLS VPN_vpna_monitor_20121124034807_3	Up	Enabled		
BGP/MPLS VPN_vpna_video_20121124034807_8	Up	Enabled		
BGP/MPLS VPN_vpna_voip_20121124034807_5	Down	Disabled		
BGP/MPLS VPN_vpna_20121124034807_2	Up	Enabled		

In the tunnel list of eSight MPLS Tunnel Manager, users can click View VPN to view VPNs carried on a tunnel and know the VPNs that will be affected by a tunnel fault.

Position : Network Application > Network Application Management > MPLS Tunnel Management > Tunnel Management > Tunnel List

Quick Start
Quick Start
Tunnel Management
Tunnel List
Explicit Path List
Tunnel Topology

Tunnel Name: Running Status: All
Source Node: Sink Node: Search

Auto Discovery Delete

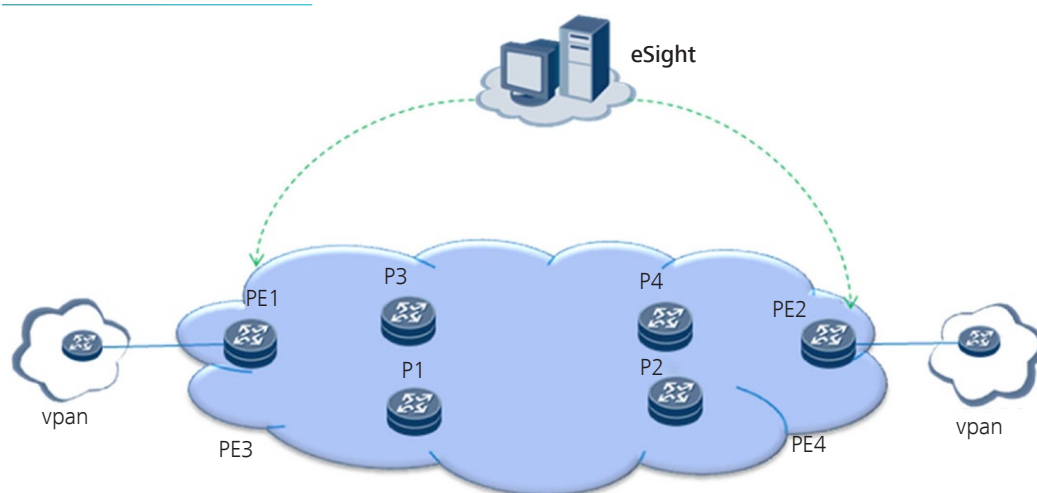
	Running Status	Backup Status	Alarm Severity	Tunnel Name	Tunnel ID	Direction	Source Node	Sink Node	Signaling	Tunnel T...	FRR Stat...	Operation
	Up	—		CR-Static: Tu...	212	Unidirectional	aodan-PE1-2...	aodan-PE2-2...	CR Static	Primary...	—	
	Down	—	Minor	LDP: 202.92...	—	Unidirectional	aodan-PE1-2...	L3VPN-P2-203	LDP	LDP Tu...	—	
	Up	—		LDP: 202.92...	—	Unidirectional	aodan-PE2-2...	aodan-PE1-2...	LDP	LDP Tu...	—	
	Up	UnSwitc...		RSVP-TE: Tu...	100	Unidirectional	aodan-PE1-2...	aodan-PE2-2...	RSVP-TE	Primary...	Enabled	
	Up	UnSwitc...		RSVP-TE: Tu...	100	Unidirectional	aodan-PE2-2...	aodan-PE1-2...	RSVP-TE	Primary...	Disabled	
	Up	UnSwitc...		RSVP-TE: Tu...	200	Unidirectional	aodan-PE1-2...	aodan-PE2-2...	RSVP-TE	Primary...	Enabled	
	Up	Switched		RSVP-TE: Tu...	200	Unidirectional	aodan-PE2-2...	aodan-PE1-2...	RSVP-TE	Primary...	Disabled	
	Up	UnSwitc...		RSVP-TE: Tu...	300	Unidirectional	aodan-PE2-2...	aodan-PE4-1...	RSVP-TE	Primary...	Disabled	
	Up	UnSwitc...		RSVP-TE: Tu...	111	Unidirectional	aodan-PE1-2...	L3VPN-P4-17	RSVP-TE	Primary...	Enabled	
	Up	UnSwitc...		RSVP-TE: Tu...	7	Unidirectional	aodan-PE2-2...	aodan-PE4-1...	RSVP-TE	Primary...	Disabled	
	Up	UnSwitc...		RSVP-TE: Tu...	477	Unidirectional	aodan-PE1-2...	aodan-PE4-1...	RSVP-TE	Primary...	Disabled	
	Up	—		RSVP-TE: Tu...	123	Unidirectional	L3VPN-P2-203	L3VPN-P1-18	RSVP-TE	Bypass...	—	
	Up	—		RSVP-TE: Tu...	300	Unidirectional	L3VPN-P1-18	L3VPN-P2-203	RSVP-TE	Bypass...	—	

OS-TE Information
View VPN
Explicit Path List

Running Environment

eSight MPLS Tunnel Manager is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios



Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight MPLS Tunnel	1	Mandatory for eSight MPLS Tunnel Manager.

eSight QoS Manager

Product Overview

With rapid network development, an increasing number of users transmit data through networks. IP networks carry data services and VoIP, VPN, and ERP services to meet diversified user requirements. New services all feature high requirements on transmission performance such as bandwidth, latency, and jitter. Users expect better experience during packet transmission. The QoS technology provides various QoS functions based on the requirements of different applications on the network, such as:

- Dedicated bandwidth
- Packet loss rate reeducation
- Network congestion management and prevention
- Network traffic adjustment
- Packet priority configuration

Unified QoS management can manage QoS services in a centralized manner on the entire network to ensure network QoS.

Huawei eSight QoS Manager monitors network QoS in real time, provides multi-dimensional data analysis, and displays QoS information in graphs and dashboards, simplifying network management. Integrating with the smart configuration tool, performance monitoring, eSight Network Traffic Analyzer, and eSight SLA Manager on eSight Unified Network Management Platform, eSight QoS Manager provides all-round functions for QoS configuration, monitoring, and optimization.

Characteristics

eSight QoS Manager uses a uniform dashboard to manage key information in a centralized manner.

The uniform dashboard displays top N information of various network QoS items, such as bandwidth usage of traffic classifier, rate of discarded bits, excess bandwidth rate, and rate of matched bits. Based on such information, users can know the QoS bandwidth usage and network faults in real time. In addition, users can specify information to be displayed on the dashboard.

eSight QoS Manager provides interface QoS management to directly display QoS traffic information.

eSight QoS Manager displays interface QoS traffic information in graphs and automatically updates the information. Visualized QoS management enables users to diagnose QoS faults in a timely manner.



eSight QoS Manager cooperates with various functional components integrated on eSight Unified Network Management Platform to implement E2E QoS management.

eSight QoS Manager integrates with the smart configuration tool, performance monitoring, eSight Network Traffic Analyzer, and eSight SLA Manager on eSight Unified Network Management Platform to provide E2E QoS management.

- Setting QoS parameters: The smart configuration tool quickly delivers QoS configurations to devices in batches or using templates.
- Checking QoS: eSight SLA Manager checks QoS items and displays QoS data in graphs in real time. Based on the real-time data, users can check whether the network QoS meets QoS configuration requirements.
- Monitoring QoS traffic information: eSight QoS Manager displays interface QoS traffic information, based on which users can discover QoS exceptions and diagnose faults in advance.
- Optimizing QoS configurations: Network Traffic Analyzer and performance management display performance and traffic data about the entire network. Based on such data, users can discover the nodes with performance or traffic exceptions and adjust QoS configurations correspondingly to ensure the traffic balance and stability on the entire network.

Running Environment

eSight QoS Manager is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios

The eSight network does not have special requirements when managed devices are connected to the eSight server.

Ordering Information

Item	Quantity	Remarks
eSight Application Base-Standard (including 60 device licenses) Or eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight SLA Manager	1	Mandatory for eSight SLA Manager, which provides the eSight QoS function.

eSight Secure Center

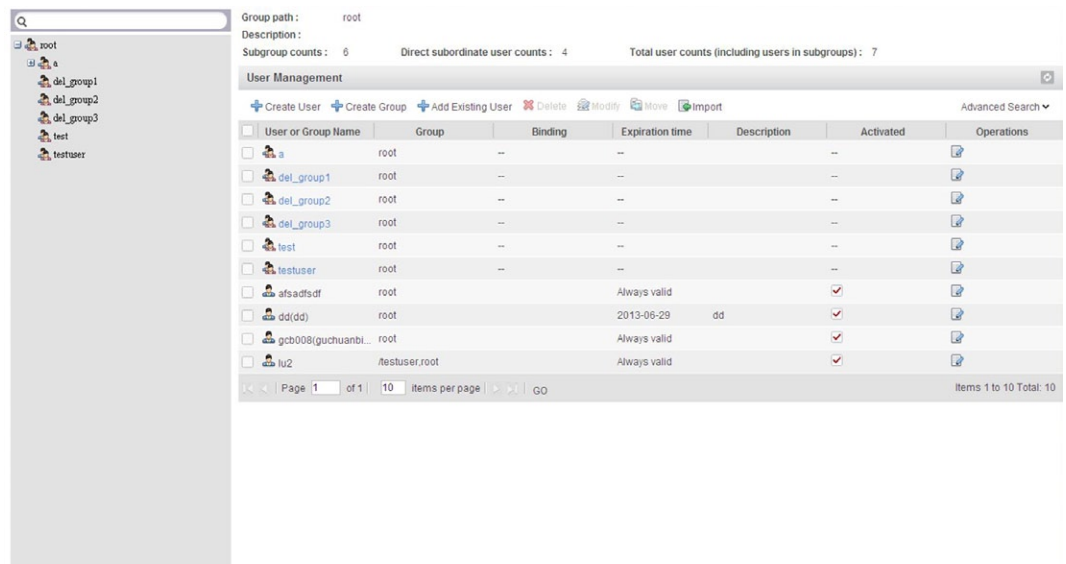
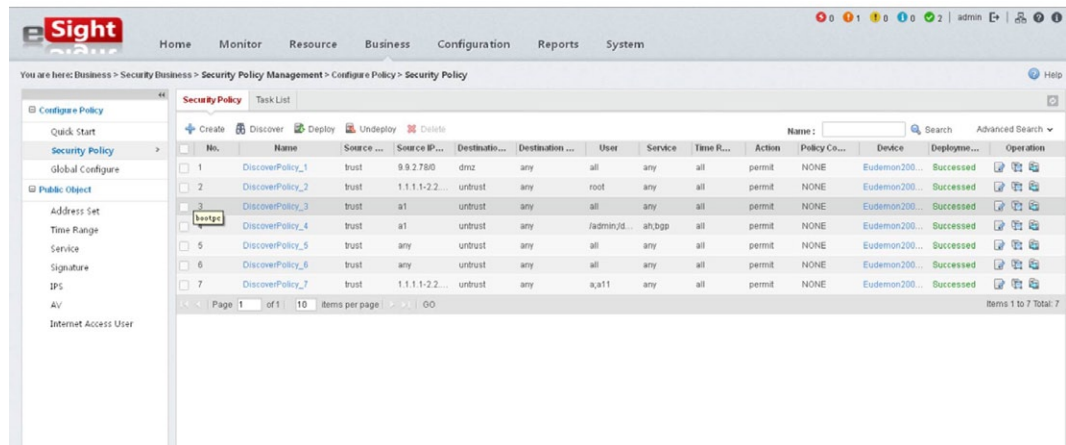
Product Overview

eSight Secure Center provides security policy management functions (such as unified configuration and deployment of security application policies on the entire network) for Huawei UTM, firewalls, and ARs, helping users manage multiple security devices in a unified manner and reducing secure O&M costs.

Characteristics

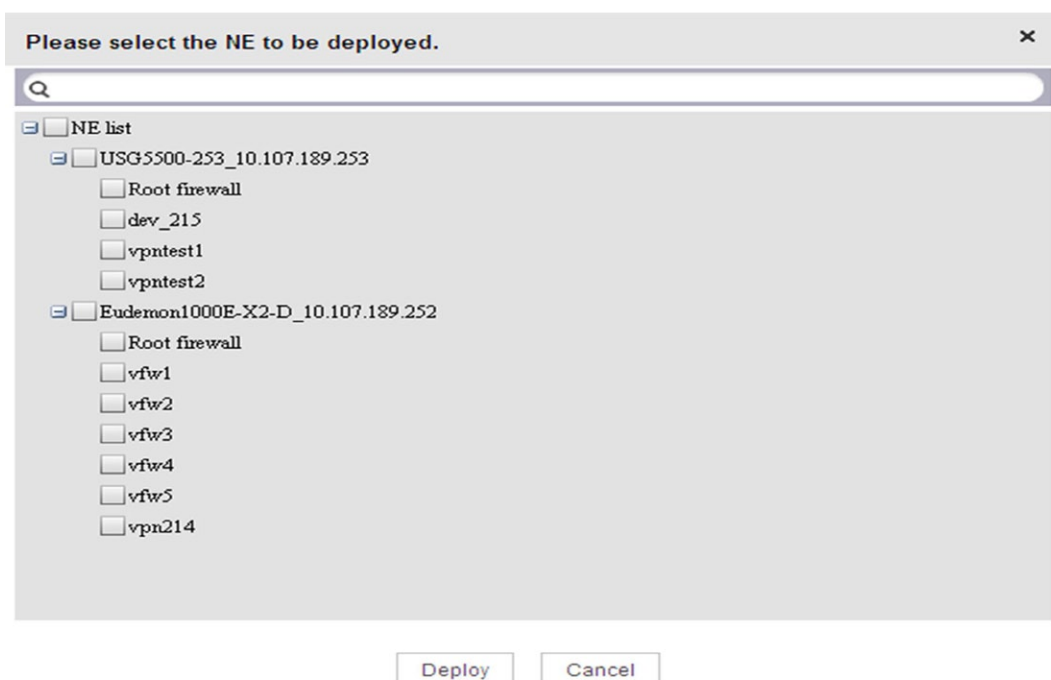
eSight Secure Center supports the unified configuration of security application policies.

eSight Secure Center manages security application policies on multiple devices including Huawei UTMs, firewalls, and ARs in a centralized manner. Users can configure device security application policies based on the user, user group, and device.



eSight Secure Center supports virtual firewall management.

eSight Secure Center automatically detects virtual firewalls and configures security policies on them. eSight Secure Center can configure and manage security policies on hundreds of virtual firewalls in a unified manner.



Running Environment

eSight Secure Center is installed on the same server as eSight Unified Network Management Platform standard or professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios

The deployment scenarios for eSight Security Center are the same as those for eSight Unified Network Management Platform.

Ordering Information

Description	Quantity Range	Remarks
eSight Application Base-Professional (including 60 device licenses) Or eSight Application Base-Standard (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight Secure Center	1	Mandatory. The eSight Secure Center provides basic functions of security policy management, including five device management licenses.
eSight Secure Center License (for 5 incremental devices)	0 to 600	Optional. One license manages 5 incremental devices.
eSight Secure Center License (for 25 incremental devices)	0 to 120	Optional. One license manages 25 incremental devices.

eSight LogCenter Log Manager

Product Overview

Massive application systems and network devices are deployed in an enterprise, including hosts, databases and other application systems, switches, and firewalls. Due to inconsistent device log formats, low readability, and difficulties in storing massive logs, major security risks cannot be promptly detected from logs.

Based on issued internal control laws and standards, the government and industrial organizations provide guidance and stipulations. Internal control laws pose higher requirements on the completeness, accuracy, and effectiveness of run logs and user logs.

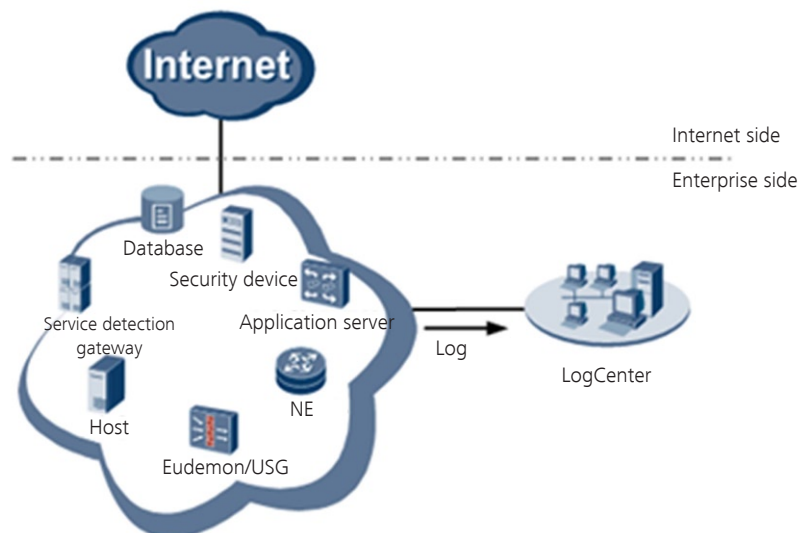
eSight LogCenter:

- Provides a platform for collecting, storing, and auditing large-scale logs of multiple types in a unified manner.
- Supports log management of Huawei and third-party vendors.
- Provides the industry leading NAT tracing function and security event analysis.

Characteristics

eSight LogCenter supports unified log management and quick matching capability.

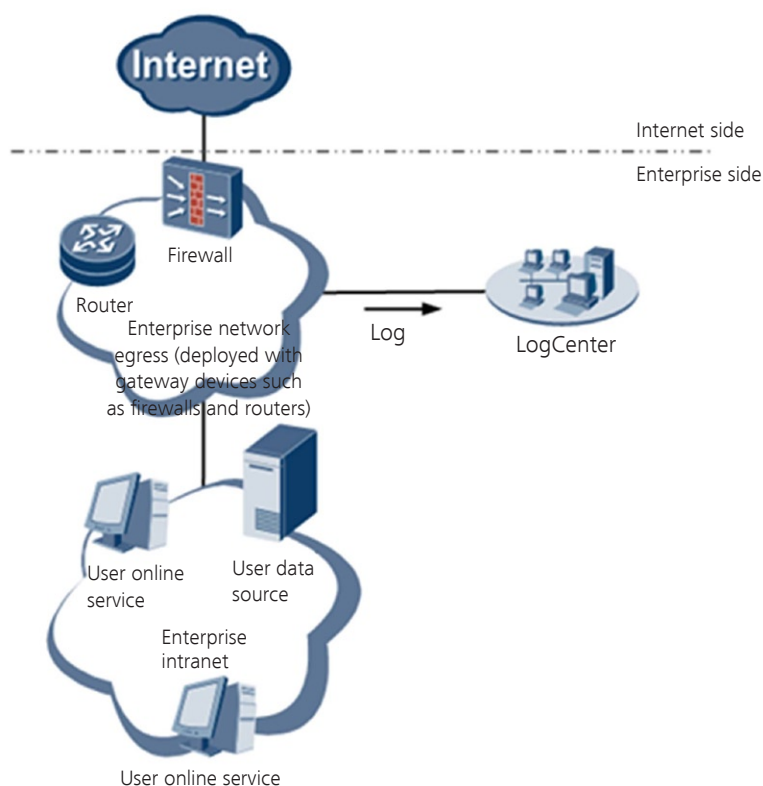
- eSight LogCenter supports multiple log collection modes including Syslog, session, SFTP, FTP static file, FTP dynamic file, and windows management instrumentation (WMI). Users can collect, classify, filter, summarize, analyze, store, and monitor logs reported from the application systems or NEs to help the administrator manage massive logs so that the administrator can know NE running status in time, trace network user behaviors, and quickly recognize and eliminate security risks.
- eSight LogCenter supports prompt notifications of key logs. The administrator can customize keywords, log type, and log level thresholds. When logs match customized keywords, log type, or log level, eSight LogCenter generates alarms in real time and notifies users using SMS messages or emails.



eSight LogCenter supports professional NAT tracing and automatic association with user information to audit users' online behaviors.

eSight LogCenter collects and analyzes logs about sessions on NAT devices (such as MA5200G, NE40E/80E, and USG firewalls) to obtain NAT information including the IP address, destination port, NAT source IP address, and protocols. eSight LogCenter traces NAT users' online behaviors by analyzing these logs and user data sources (such as the data source provided by the AAA server).

Tracing NAT users' online behaviors

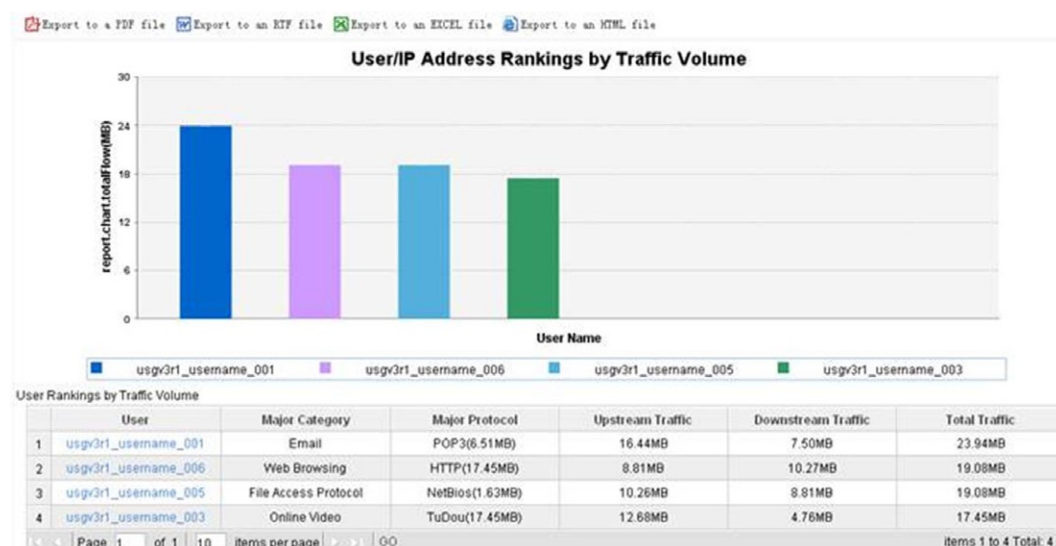


Session log query page

Query Result								
Export to a TXT file Export to an EXCEL file Export to a CSV file								
No.	Received at	Start Time	End Time	NE	User	Category ID	Protocol ID	Source IP Address
1	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	Online Video	TuDou	172.18.11.18:1
2	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	Online Video	TuDou	172.18.11.18:1
3	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	Online Video	TuDou	172.18.11.18:1
4	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	Online Video	TuDou	172.18.11.18:1
5	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	Online Video	TuDou	172.18.11.18:1
6	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	Flow Protocol	SMB	172.18.11.17:1
7	2012-06-27 17:33:54	2012-06-27 17:35:19	2012-06-27 17:36:19	Firewall	usgv3r1_usernam...	File Access Protoc...	NetBios	172.18.11.16:1

eSight LogCenter supports rich security event analysis reports showing the network security status.

eSight LogCenter collects security event logs about network security devices and systems such as Huawei network UTMs, firewalls, intrusion protection system, and Anti-DDoS system, analyzes them, and generates a report to help users learn about network security status.



eSight LogCenter supports million-level log processing capability per second, meeting requirements of state-level network audit.

eSight LogCenter meets the performance requirements of state-level network audit and collects and audits millions of system logs in a second, supporting high-performance log collection, storage, and audit functions for large and ultra large networks.

Running Environment

Related server and hardware description (1)

Scenario	Management Node	Hardware Configuration	Recommended Server	System Configuration
Single-node deployment (Application base+eSight LogCenter)	Application base: 0–500 EPS LogCenter: • Syslog: 0–2000 EPS • NAT: 0–10000 EPS	CPU: 2 x hexa-core 2.5 GHz or higher Memory: 12 GB Disk space: 8 x 300 GB or 2 x 300 GB + Disk arrays NOTE: You are advised to use PC servers.	X3650 M4-2*Xeon 6C E5-2640 2.5G or higher-32G(4*8G)-3*300G	Configuration 1: Windows Server 2008 R2 standard (64-bit) + MySQL 5.5 (provided in a standard eSight software package) Configuration 2: Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard

Scenario	Management Node	Hardware Configuration	Recommended Server	System Configuration
Single-node deployment (Application base+eSight LogCenter)	Application base: 2000–5000 EPS LogCenter: • Syslog: 0–2000 EPS • NAT: 0–10000 EPS	CPU: 2 x hexa-core 2.5 GHz or higher Memory: 16 GB Disk space: 8 x 300 GB or 2 x 300 GB + Disk arrays NOTE: You are advised to use PC servers.	X3650 M4-2*Xeon 6C E5-2640 2.5G or higher-32G(4*8G)-3*300G	Configuration 1: Windows Server 2008 R2 standard (64-bit) + MySQL 5.5 (provided in a standard eSight software package) Configuration 2: Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard
	Application base: 500–2000 EPS LogCenter: • Syslog: 0–2000 EPS • NAT: 0–10000 EPS	CPU: 2 x hexa-core 2.5 GHz or higher Memory: 24 GB Disk space: 8 x 300 GB or 2 x 300 GB + Disk arrays NOTE: You are advised to use PC servers.	IBM X3850 X5-4*Xeon 8C E7-4820 2.0G or higher-64G(8*8G)-8*300G	
Independent deployment of the Log Collector	The following lists the maximum numbers of different logs that a Log Collector collects every second: Session logs for online behavior analysis (excluding the disk cabinets): 150,000 EPS Session logs for traditional firewalls: 160,000 EPS Text logs: 8000 EPS Binary data flow logs: 20,000 EPS	CPU: 2 x quad-core 2 GHz or higher Memory: 8 GB Disk space: 8 x 300 GB NOTE: You are advised to use PC servers.	X3650M4-1*E5-2640 6c 2.5 GHz or higher-8G(2*4G)	No database needs to be installed on the Log Collector. Windows Server 2008 R2 standard (64-bit) is required.

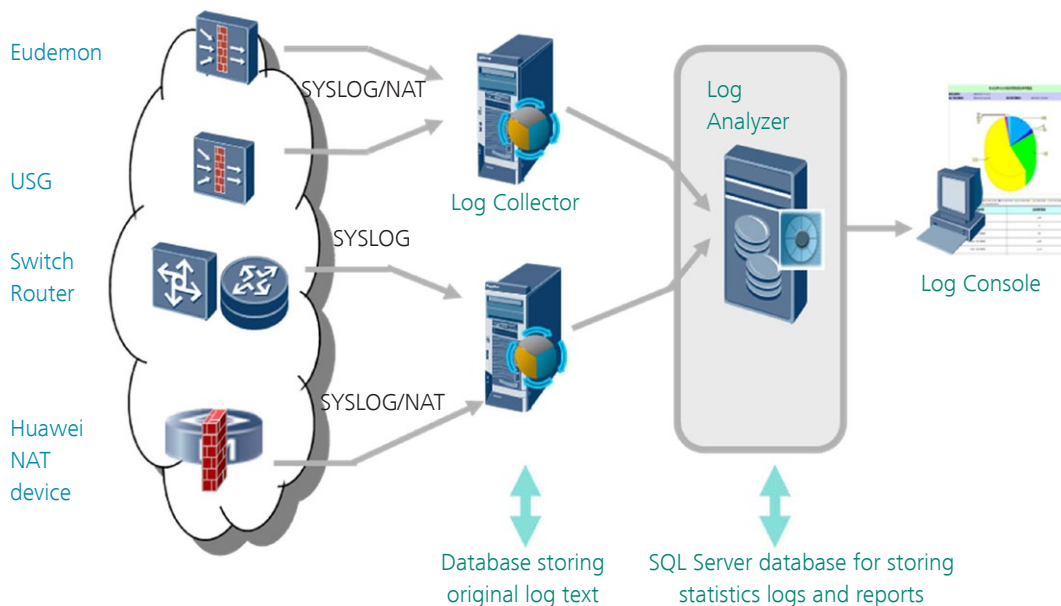
Related server and hardware description (2)

Scenario	Management Node	Hardware Configuration	Recommended Server	System Configuration
eSight components deployed on the same server (Application base + Any combination of eSight components)	Application base: 0–200 EPS eSight components: • Policy Center: manages 0 to 2000 online users • eSight Network Traffic Analyzer: manages 0 to 10 devices • LogCenter: manages 0–1000 EPS Syslog logs or 0–5000 EPS NAT logs	CPU: 2 x quad-core 2 GHz or higher Memory: 8 GB Disk space: 500 GB (The recommended Disk space is 1 TB.) NOTE: You are advised to use PC servers.	X3650M4-1*E5-2640 6c 2.5 GHz or higher-8G(2*4G)-2*300G	Windows Server 2008 R2 standard (64-bit) + Microsoft SQL Server 2008 R2 standard

Deployment Scenarios

eSight LogCenter network can be deployed in centralized or distributed ways.

- Distributed deployment: The Log Collector and the Log Analyzer are separately deployed on two servers.

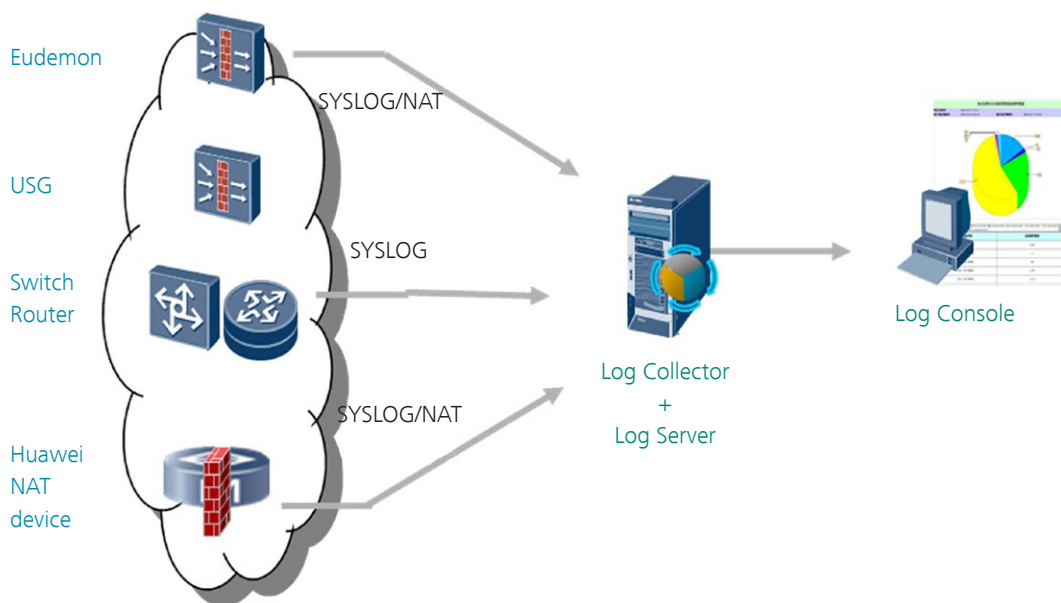


Log Collector: receives, summarizes, formats, filters, counts, and stores logs and generates alarms.

Log Analyzer: manages policies, reports, devices, systems, and users.

Log Console: provides an interaction GUI for managing foreground and background using the web.

- Centralized deployment: When performance requirements are low, eSight LogCenter can also be deployed in a centralized way.



When fewer than 2000 logs are managed every second in an SMB project, eSight LogCenter and eSight application base can be deployed on the same server.

Ordering Information

Description	Quantity Range	Remarks
Basic log management functions on eSight LogCenter (including a small-scale log management license)	1	Mandatory.
Extended management function components of eSight LogCenter (including third-party device log management and identity association)	0 or 1	Optional. Extended functions include third-party device log management and identity association.
eSight LogCenter log management function promotion packages	0 or 1	Optional. The basic and expandable packages are included.
Small-scale log management license (managing 250 Syslog logs every second for about 25 devices, tracing 1250 NAT logs with 250 Mbit/s outgoing bandwidth, and supporting 250 GB storage for about 60 days)	Optional	Optional. The log management capability is controlled by EPS, that is, the number of logs collected every second. The value is calculated assuming that 10 Syslog logs are collected on each device every second, and five session logs are generated on 1 Mbit/s bandwidth every second. Project requirements in most scenarios can be met. Requirements can also be adjusted if the customer requirements are obviously decreased or increased. For example, if most devices on the user network are switches, which do not send many Syslog logs, a user can use a small-scale package to manage a network consisting of 100 NEs. However, if the user network outgoing bandwidth is 200 Mbit/s while more than 2000 sessions are generated every second, a user can use two small-scale packages as required.
Medium-scale log management license (managing 1000 Syslog logs every second for about 100 devices, tracing 5000 NAT logs with 1 Gbit/s outgoing bandwidth, and supporting 1 TB storage for about 60 days)	Optional	
Large-scale log management license (managing 2500 Syslog logs every second for about 250 devices, tracing 125,000 NAT logs with 2.5 Gbit/s outgoing bandwidth, and supporting 2.5 TB storage for about 60 days)	Optional	
Storage expansion license for log management components of eSight LogCenter-1 TB-Configured only on one Log Collector	Optional	The log storage expansion license is optional.
Storage expansion license for log management components of eSight LogCenter-10 TB-Configured only on one Log Collector	Optional	
Storage expansion license for log management components of eSight LogCenter-30 TB-Configured only on one Log Collector	Optional	

eSight DC nCenter

Product Overview

With the help of virtualization software, one physical server can be virtualized to multiple VMs that share computer resources. To ensure communication between VMs and communication between VMs and switches, the virtual switch vSwitch is introduced. On the one hand, a vSwitch is deployed on a server and managed by the system administrator; on the other hand, a vSwitch is a switch that is managed by the network administrator. The unclear boarder between network management and server management requires cooperation between the system administrator and network administrator.

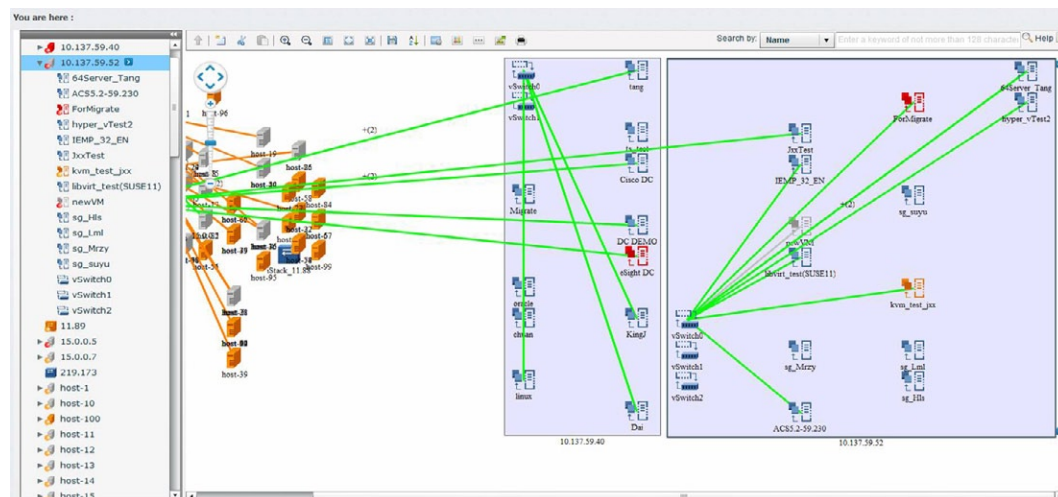
Sometimes, VMs that occupy fewer resources are migrated to another server to free unnecessary server space and reduce costs. Sometimes VMs are migrated to new servers that are added to satisfy service requirements. To meet the VM migration requirement, the destination network where a VM is to be migrated must be prepared in advanced. This brings new challenges to network management.

Huawei eSight DC nCenter monitors network resources (including physical servers, VMs, vSwitches, and TOR switches), displays the topology of virtual resources and physical devices, and dynamically adjusts physical network profiles based on VM changes.

Characteristics

eSight DC nCenter automatically discovers the virtual and network topologies and uniformly manages the data center network.

eSight DC nCenter automatically discovers physical and virtual devices and displays the device connections and status in topology views, including the subordinate and connection relationships between physical TOR switches, physical servers, vSwitches, and VMs.



eSight DC nCenter uniformly monitors data center network resources.

eSight DC nCenter monitors resources such as physical servers, VMs, port groups, and physical network adapters and manages VM performance and alarm information.

Physical server: basic information, quantity of VMs, and quantity of vSwitches.

Position : Network Application > Network Application Management > Virtual Network Management > Resource Management > Physical Server

Quick Start

Quick Start

Resource Management

VMM Connection Management

Physical Server

Virtual Machine

Port Group

Distributed Virtual Switch

Distributed Port Group

Service Management

Interface and User

IP address: Name:

Running status: All Remarks:

Export Modify Remarks Synchronize Move

Running Status	Name	Platform Type	IP Address	Memory Size (GB)	VM Quantity	Virtual Switch Quantity	VMH
Online	10.137.59.40	vmnic-x86		3.99	5	2	10.137.59.37
Online	10.137.59.52	vmnic-x86		3.99	11	7	10.137.59.37
Online	15.0.0.5	vmnic-x86		3.99	3	2	10.137.219.169
Online	15.0.0.7	vmnic-x86		3.99	5	2	10.137.219.169

20 Total records: 4 Previous Next

VM: name, VLAN ID, vSwitch and server to which a VM belongs, and bound physical network profile.

You are here : Resource(10.137.59.40)

View

Basic Information

Server View

Virtual Machine

Virtual Switch

Port Group

Physical network adapter

Information

IP address: Name:

Operating system: Profile name:

Export Modify Remarks Expand All

Running Sta...	Name	Operating System	Memory Siz...	MAC Address	IP Address	Port Group Name	Profile Name	Remarks	Operation
Online	Cisco DC	Microsoft Windows Server 2...	8.00	(2 MAC)	10.137.59.155				
Online	DC DEMO	Microsoft Windows Server 2...	2.00	00-50-56-81-57-04	10.137.59.156	VM Network			
Online	Dai	Microsoft Windows Server 2...	4.00	00-50-56-81-57-2c		datacenter	xxx		
Online	King	Microsoft Windows Server 2...	4.00	00-50-56-81-57-2a		datacenter	xxx		
Online	Migrate	Microsoft Windows Server 2...	4.00	00-50-56-81-57-2d		datacenter	xxx		
Online	chuan	Microsoft Windows Server 2...	4.00	00-50-56-81-57-28		xxx			
Online	eSight DC	Microsoft Windows Server 2...	8.00	00-50-56-80-5a-91	10.137.59.157	Netflow			
Online	bus	Microsoft Windows Server 2...	4.00	00-50-56-81-57-29		datacenter	xxx		
Online	oracle	Microsoft Windows Server 2...	4.00	00-50-56-81-57-2b		datacenter	xxx		
Online	tao	Microsoft Windows 7 (32-bit)	8.00	(3 MAC)	169.254.200.36				
Online	ta_test	Microsoft Windows 7 (32-bit)	1.00	(2 MAC)					

20 Total records: 11 Previous Next

Port group: port group name, VLAN ID, and virtual profiles (including profiles for security, traffic adjustment, and network adapter binding). Users can add, modify, and delete port groups.

You are here : Resource(10.137.59.52)

View

Basic Information

Server View

Virtual Machine

Virtual Switch

Port Group

Physical network adapter

Information

Name: VLAN ID:

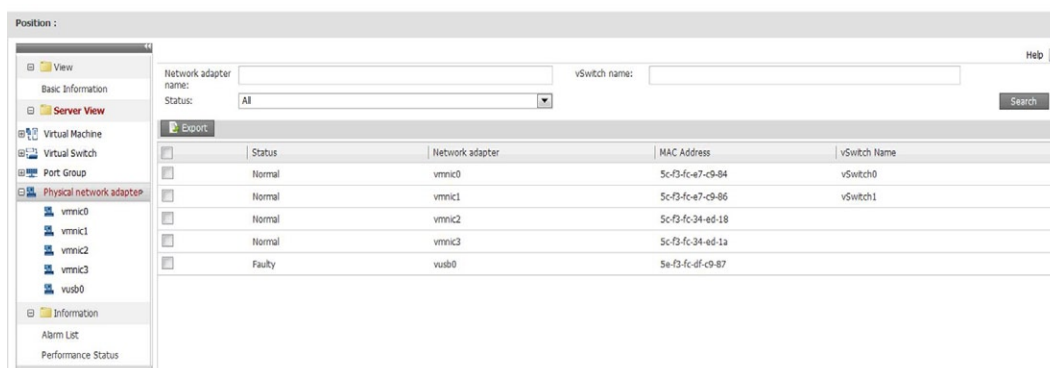
vSwitch: Profile name:

Create Delete Bind Profile Unbind Profile

Name	VLAN ID	vSwitch	Profile Name	Operation
8888	0	vSwitch0	xxx	
Management Network	0	vSwitch0	xxx	
VM Network	0	vSwitch0	xxx	
VMkernel	0	vSwitch1	xxx	

20 Total records: 4 Previous Next

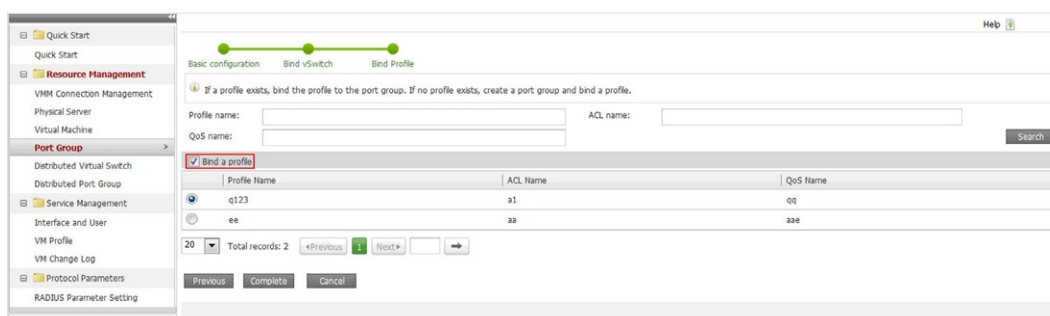
Physical network adapter: network adapter name and status, MAC address, and vSwitch name.



eSight DC nCenter automatically delivers network profiles during the VM deployment, which reduces the work complexity for network administrators and shortens the required time.

the VM to a port group and notifies nCenter of the binding relationship. When the VM is brought online, nCenter automatically and quickly delivers the network profile to the TOR switch.

When creating a VM using vCenter during the VM deployment, the server administrator binds



eSight DC nCenter synchronously migrates network profiles when migrating a VM, which prevents services from being affected by the migration.

eSight DC nCenter listens to VM changes (for example, a VM goes online, goes offline, or is migrated) using vCenter, synchronizes virtual network configurations to the physical network by changing network configurations between source and destination TOR switches, and generates VM change logs for future troubleshooting.

Running Environment

eSight DC nCenter is installed on the same server as eSight Unified Network Management Platform professional edition. Therefore, the configuration requirements for their running environments are the same.

Deployment Scenarios

The eSight network does not have special requirements when the physical server where a VM is deployed is connected to the eSight server and the VM has been added to eSight DC nCenter.

Ordering Information

Item	Quantity	Remarks
eSight Application Base-Professional (including 60 device licenses)	1	Mandatory for eSight Unified Network Management Platform.
eSight DC nCenter (including 10000 Virtual Machine Licenses)	1	Mandatory for eSight DC nCenter.
eSight DC nCenter License (for 10000 incremental VMs)	Optional	One license manages 10,000 incremental VMs.

Related Product: Policy Center

Huawei Policy Center provides unified policy engine, which deploys a unified access policy for the whole company, contains wired and wireless devices, and can be access by intranet and internet. The authentication can be deployed based on user, device type, asset type, access time, access location, and access method. Policy Center can meet hierarchy multi-terminal access requirements of enterprises, and implement full lifecycle access management, which allows visitors to go online anywhere anytime, improving network access efficiency, enhance enterprise brand. Policy Center also provides an abundant security policy sets to improve terminal security level and prevent unsafe terminals or unauthorized terminals from accessing the enterprise intranet, improving the enterprise security level.

Policy Center can be deployed separately or integrated with eSight, providing enterprises with a unified network and user management solution.

More Information

For more information, visit <http://enterprise.huawei.com>.



Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.

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

Trademark Notice

 , HUAWEI, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, product, service and company names mentioned are the property of their respective owners.

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI TECHNOLOGIES CO.,LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129,P.R.China
Tel: +86 755 28780808

www.huawei.com