EXECUTIVE SUMMARY

Huawei eSight is a new generation of unified operation and management (O&M) system for enterprise network infrastructure, unified communications, telepresence conferencing and video surveillance. Based upon “topology-centric, simplifying management, and improving the O&M efficiency” philosophy, eSight centrally manages corporate resources, services and users. Meanwhile, eSight provides a flexible and open platform that supports enterprise customization development to allow users to build their own personalized intelligent management system.

Huawei commissioned Tolly to evaluate the ease-of-use, wired and wireless networks converged management, full lifecycle WLAN management, intelligent network quality monitoring, fine right- and domain-based user management, multi-vendor device management capability and other key features.

<table>
<thead>
<tr>
<th>Huawei eSight Unified Management Platform Tolly Certified Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ease-of-use</strong></td>
</tr>
<tr>
<td>Entire network topology visualization and customizable management, real-time alarm monitoring and processing capability, group-based flexible performance management and bulk device configuration and management to simplify user operations.</td>
</tr>
<tr>
<td><strong>Wired and Wireless Networks Converged Management</strong></td>
</tr>
<tr>
<td>Huawei developed the proprietary Super Virtual Fabric (SVF) technology to virtualize wired and wireless network devices in different layers, including wireless Access Points (APs), into one network element for simplified management. With the capability to manage the SVF and all components in it, Huawei eSight achieved unified management for wired and wireless networks, devices and users.</td>
</tr>
<tr>
<td><strong>Full Lifecycle WLAN Management</strong></td>
</tr>
<tr>
<td>Provide from global to local comprehensive quality perception. Visually present wireless network quality, interference sources, wireless intrusion, access clients, etc. Support end-to-end troubleshooting from user --&gt; SSID --&gt; AP --&gt; AC to assist administrators to quickly identify the cause and locate the point of failure.</td>
</tr>
<tr>
<td><strong>Intelligent Network Quality Monitoring</strong></td>
</tr>
<tr>
<td>Support simulated traffic based evaluation as well as actual service traffic based detection (with the Huawei's proprietary iPCA network quality detection technology) to achieve entire network's quality visualization.</td>
</tr>
<tr>
<td><strong>Fine Right- and Domain-based User Management</strong></td>
</tr>
<tr>
<td>Different administrators with different management rights, management scopes, time windows and client IP address ranges.</td>
</tr>
<tr>
<td><strong>Multi-vendor Device Management</strong></td>
</tr>
<tr>
<td>In addition to the fine management of Huawei devices, eSight also supports managing other major vendors’ devices, with topology and link automatic discovery capability as well as device performance and panels monitoring capability. Meanwhile, traffic analysis protocols such as sFlow and NetFlow are also supported.</td>
</tr>
</tbody>
</table>

Source: Tolly, November 2014

Table 1
Test Results

Tolly engineers validated the feature set of the Huawei eSight Unified Management Platform. The feature evaluation included the basic functions, service management, agile features, security management, and log management. Test results are summarized below. See Table 2 at the end of the document for the list of all verified items.

Basic Functions

Topology Management

Tolly engineers verified that eSight could use Link Layer Discovery Protocol (LLDP) and MAC tables of the network equipment to automatically discover the entire network topology including devices from third-party vendors.

The topology of the network shown in eSight is fully customizable to allow administrators to personalize the layout. Tolly engineers customized the size of the icons, the color, shape and width of the links, the background image, the displayed attributes in the devices’ and links’ labels. Typically, the numerous links in the network make the topology look messy. Huawei eSight supports link filters to allow administrators define certain types or statuses of links to be shown. See Figure 1.

The dashboard (portal homepage) is customizable. Administrators can choose the items (e.g. Top N average CPU usage, WLAN user statistics, top N SLA compliance, etc.) to be shown as well as the type of charts (bar, pie, lines, etc.). See Figure 2.

Alarm Management

Huawei eSight allows administrators to stop certain types of alarms from certain sources in a certain time period. For example, Tolly engineers stopped the link down alarms of the switches while making changes of the test bed topology to avoid being disrupted.

Administrators can define certain types of alarms to be sent out via email and text messages to certain people.

Certain types of alarms from certain sources in certain time can be consolidated into one alarm or alarms with an interval. So the administrators can be warned but not constantly disrupted.

Engineers were able to change the severity of certain type of alarm from the default one.

Huawei eSight has built-in guidance to remediate each type of alarm. It also allows administrators to add notes to the alarm. So experience can be shared to the administrator who handles the same type of alarm next time.
Performance Management

Different type of devices have different attributes to monitor. For example, compared to the aggregation/core devices, the numerous access devices in an enterprise network typically have longer monitoring period, lower alarm threshold and less monitoring indicators. Session information is important for firewalls while QoS information is critical for routers.

In addition to the built-in devices type groups, Huawei eSight also provides customizable grouping policies to allow users personalize their device groups. When a new device connects to the network, eSight could place it into the proper group automatically based on the grouping policies to achieve differentiated performance collection and alarm display. See Figure 3.
Also, users can save the most frequently monitored resources to My Favorites and sort by a certain attribute, for example, by group, for more efficient daily monitoring tasks.

In the test, Tolly engineers created two groups - aggregation device group and access device group using the device names as the filter.

Device Configuration File Management

Huawei eSight supports automatically backing up the configuration file of managed devices. It can compare the latest configuration file with the previous saved file to identify whether there are any configuration changes. The configuration change can trigger alarms.

With the saved files, Huawei eSight supports restoring the configuration of managed devices.

Secure Management

Huawei eSight supports assigning the rights, manageable object groups, and manageable time period for different users. For example, a temporary regional administrator can only monitor the performance of devices in the branch office in weekdays. See Figure 4.

Huawei eSight’s Web console supports HTTPS with secure connections.

Service Management

WLAN Management

Huawei eSight is able to manage Huawei wireless access controllers (ACs) and access points (APs) to deploy WLAN services.

Huawei eSight shows the unified topology of both wired and wireless networks. The wired switches, routers, firewalls, etc. were displayed together with the wireless ACs and APs.

The wireless service can be monitored by eSight. Information of online users, SSIDs, clients, access controllers and access points can all be monitored in eSight. See Figure 5.

As eSight can monitor the detailed information of all components in the wireless network, it is capable of helping administrators locate the faults. Administrator can diagnose the users, clients, SSIDs, access controllers and access points to locate the fault. See Figure 5.
Figure 5

Source: Tolly, November 2014
WLAN Environment Monitoring

Huawei eSight can also list the interference sources while they’ve been detected by the APs. It can also show the swept spectrogram and channel quality spectrogram of an AP to assist administrators to plan the wireless environment better. See Figure 6.

SLA Management

Huawei eSight can periodically monitor the network quality such as voice service quality, latency, jitter, etc. and export network quality (Service-level Agreement - SLA) reports. Engineers created one SLA task to monitor the ICMP jitter between two devices and generate the SLA compliance report periodically to send to the administrator’s email. While problems happen, administrators can use the SLA history or run the diagnose task to view the current network quality. See Figure 7.

Traffic Analysis

Huawei eSight supports collecting the traffic statistics using multiple protocols including NetStream, sFlow, NetFlow, etc. and then analyze the traffic from multiple dimensions including device, port, application, host, DSCP and session. The dashboard can show analysis in multiple dimensions - the top N application, host, conversation, DSCP, interface Traffic, etc. Drill down analysis is supported in each dimension to identify the performance of individual sessions. See Figure 8.

Also, eSight allows administrators to create personalized reports with customizable filters, report type, report layout, etc.

Terminal Access Management

Huawei eSight consider devices whose MAC or IP addresses are not in the MAC or IP address whitelist as unauthorized terminals. Administrators can run the discover tasks and find the unauthorized terminals.

QoS Management

With the QoS performance collection task, Huawei eSight is able to monitor the traffic statistics of each priority queue on each port.
Huawei eSight Service Level Agreement (SLA) Compliance Monitoring

Source: Tolly, November 2014  Figure 7

Huawei eSight Traffic Analysis

Source: Tolly, November 2014  Figure 8
Agile Features

iPCA
Packet Conservation Algorithm for Internet (iPCA) is Huawei’s proprietary technology to measure the frame loss ratio of the device level, link level as well as end-to-end and hop-by-hop network level in real-time directly using the service traffic. Huawei eSight can collect the frame loss ratio of the three levels and use the data to display the network quality history, trigger alarms and locate the network failure. See Figure 9.

SVF
Super Virtual Fabric (SVF) is Huawei’s vertical virtualization technology that allows wireless access points (APs) and low-cost fixed-configuration switches to act as remote interface cards of a parent switch for simplified management.

Huawei eSight can show an SVF instance as one network element. Administrators can also expand the SVF node to view the topology of the switches and APs in the SVF to achieve unified wired and wireless management. See Figure 10.

To simplify the configuration, Huawei eSight provides pre-defined configuration templates to configure all SVF members with one click for certain tasks.

Security Service

IPsec VPN
IPsec VPN service, topology and performance can be monitored by Huawei eSight. There is also a diagnose tool in eSight to help administrators locate IPsec VPN’s local side and remote side problems.

Security Service: Virtual Firewall Management
Huawei’s Next Generation Firewall (NGFW) can be configured into multiple virtual firewalls. Administrators can add the virtual firewalls to the authorization management list in eSight. Then eSight can manage and analyze the virtual firewalls’ policies.

Security Service: Intelligent Policy Analysis
Huawei eSight supports intelligent analysis for security rules.

Unmatched Rule Analysis - Identify the rules that are contradictory.

Risk Analysis - Analyze the potential risks (e.g. the destination address is set to any while the service includes Telnet and FTP).

Security Service: Group-based Policy Management
Typically, a security policy needs to be deployed to a few devices. Without the management application, administrators need to deploy the same policies multiple times. Huawei eSight supports deploy a security policy to a group of devices such as NGFW, virtual firewall devices, and AR routers to save administrators significant amount of time and avoid the chance of mistakes when doing duplication jobs.

The security policy created by eSight can be user-based and application-based. Huawei eSight also provides pre-defined applications for administrators to use.

Security Service: Centralized Management and Auditing of Policies

Huawei eSight can manage 802.1x authentication policies on multiple switches and audit the policy consistency to see whether the current running policy on the switch match the policy in eSight. If the policy does not match, administrators can deploy the policy to the switch with one click.

LogCenter

LogCenter is a component in Huawei eSight to store and query syslogs and binary logs. It supports intelligent log retrieving which can search certain logs with and/or/not conditions and time frames.

NAT translates multiple private IP addresses to the same number of or fewer public IP addresses. Huawei eSight’s LogCenter stores the NAT translation information and support NAT source tracing which allows administrators to search a time frame and identify the original source private IP address and the translated source public IP address and port.

Huawei eSight is capable of recording 7,000 events per second syslogs and 160,000 events per second binary logs with the help of the Huawei USG5530S collector for the syslogs and the E8000E collector for the binary logs.

The LogCenter application was installed on one physical server with one Intel Xeon E5-2640 hex-core CPU, 8GB RAM, 2TB hard drive and 4*GbE ports.
# Huawei eSight Unified Management Platform

## Tolly Verified Performance and Features

<table>
<thead>
<tr>
<th>Basic Functions</th>
<th>Traffic Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology Management</strong></td>
<td>✔️</td>
</tr>
<tr>
<td>✔️ Automatic Topology Discovery with LLDP and MAC Tables&lt;br&gt;Link discovery between third-party devices</td>
<td>✔️ Network Traffic Analysis for NetStream, sFlow, NetFlow, etc. Multiple Dimensions (application, interface, conversation, host device, DSCP, etc.) Supports drill down analysis to individual sessions</td>
</tr>
<tr>
<td>✔️ Topology Customization&lt;br&gt;Fully customizable icons, links, and labels</td>
<td>✔️ Terminal Access Management&lt;br&gt;Unauthenticated Terminal Location&lt;br&gt;Blacklist and whitelist</td>
</tr>
<tr>
<td>✔️ Dashboard (Portal Homepage) Customization&lt;br&gt;Customizable items and chart types</td>
<td>✔️ QoS Management&lt;br&gt;QoS Performance Monitoring for Each Priority</td>
</tr>
<tr>
<td>✔️ Alarm Management&lt;br&gt;Alarm Masking&lt;br&gt;Block certain types of alarms from certain sources in a certain time period</td>
<td>✔️ Agile Features&lt;br&gt;iPCA&lt;br&gt;Device-Level Packet Loss Measurement&lt;br&gt;Link-level Packet Loss Measurement&lt;br&gt;Network-level Packet Loss Measurement</td>
</tr>
<tr>
<td>✔️ Remote Alarm Notification&lt;br&gt;via email or text message</td>
<td>✔️ Security Management&lt;br&gt;IPsec VPN&lt;br&gt;IPsec VPN Service Monitoring&lt;br&gt;IPsec VPN Service Diagnosis</td>
</tr>
<tr>
<td>✔️ Alarm Consolidation</td>
<td>✔️ SVF&lt;br&gt;Manage Huawei Super Virtual Fabric (SVF)</td>
</tr>
<tr>
<td>✔️ Alarm Severity Redefinition</td>
<td>✔️ Security Policy&lt;br&gt;Virtual Firewall Management&lt;br&gt;Intelligent Policy Analysis&lt;br&gt;Redundancy Analysis, Unmatched Rule Analysis, Risk Analysis for security rules</td>
</tr>
<tr>
<td>✔️ Policy-based Automatic Performance Data Collection&lt;br&gt;Different policies for different types (groups) of devices</td>
<td>✔️ LogCenter&lt;br&gt;Intelligent Log Retrieving&lt;br&gt;NAT Source Tracing&lt;br&gt;High Performance Processing Capability&lt;br&gt;7,000 Events per Second Syslogs,&lt;br&gt;160,000 Events per Second Binary logs</td>
</tr>
<tr>
<td>✔️ Automatic Configuration Backup</td>
<td>✔️ Secure Management&lt;br&gt;Administrators' Permission Management by privilege, device domain, and time&lt;br&gt;Secure Connection Between the Client and Server (HTTPS)</td>
</tr>
<tr>
<td>✔️ Configuration File Comparison - current and the latest backup</td>
<td>✔️ Device Configuration File Management&lt;br&gt;Secure Connection Between the Client and Server (HTTPS)</td>
</tr>
<tr>
<td>✔️ Configuration File Restoration</td>
<td>✔️ Secure Management&lt;br&gt;Integrated Wired and Wireless Topology&lt;br&gt;WLAN Network-wide Status Monitoring&lt;br&gt;WLAN Quick Fault Location</td>
</tr>
<tr>
<td>✔️ Administrators’ Permission Management by privilege, device domain, and time</td>
<td>✔️ Service Management&lt;br&gt;WLAN Management&lt;br&gt;WLAN Service Deployment&lt;br&gt;Integrated Wired and Wireless Topology&lt;br&gt;WLAN Network-wide Status Monitoring&lt;br&gt;WLAN Quick Fault Location</td>
</tr>
<tr>
<td>✔️ Secure Connection Between the Client and Server (HTTPS)</td>
<td>✔️ Secure Management&lt;br&gt;SLA Management&lt;br&gt;SLA Compliance Assessment</td>
</tr>
</tbody>
</table>
About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

About Huawei eSight

The eSight Unified Management Platform is a new-generation comprehensive Operation and Management (O&M) solution developed by Huawei for enterprise campus networks, branch networks, data center networks, unified communications, video conferencing, and video surveillance. Huawei eSight provides lifecycle management with automated deployment, comprehensive monitoring, intelligent diagnostics and fast fault recovery. Huawei eSight helps enterprises improve network resource utilization, reduce operation costs, and guarantee stability of the enterprise ICT system.

You can reach the Huawei eSight team by E-mail at network@huawei.com

Visit eSight on the Internet at:

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided “as is,” and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.