NMS Basics

www.huawei.com

HUAWEI

Foreword

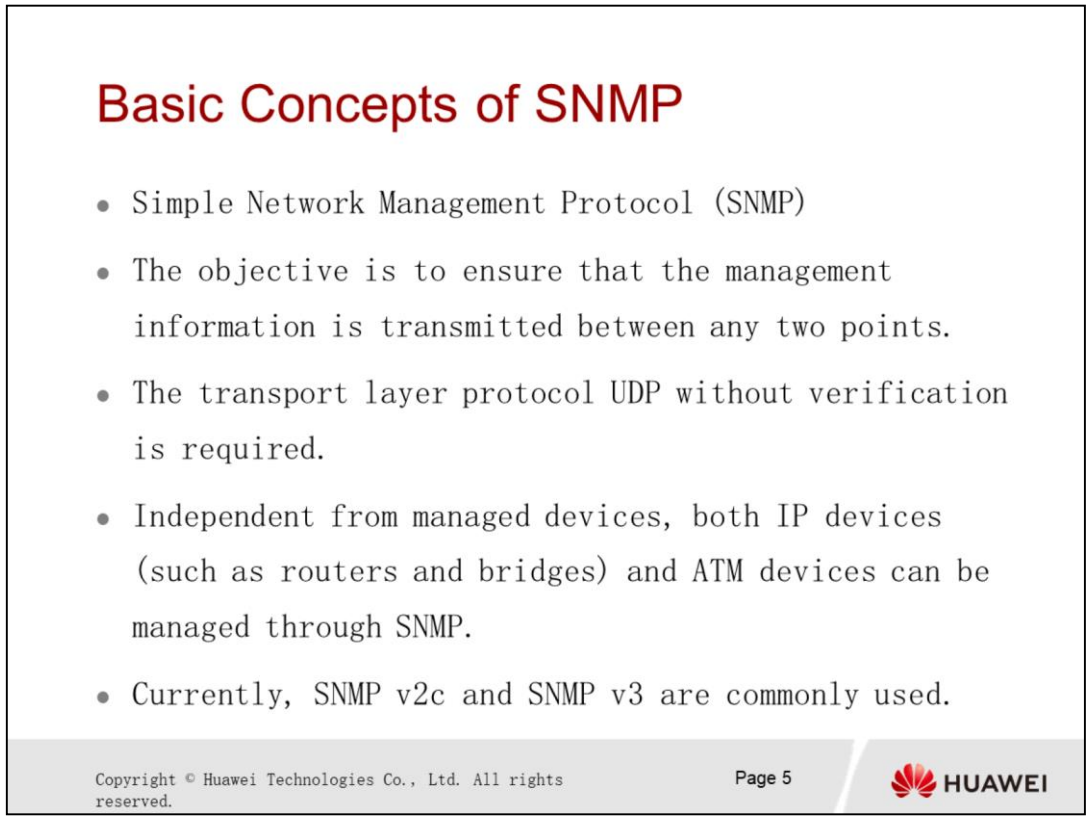
- The eSight PON components can be used to manage and monitor PON network devices.
- This course describes eSight_PON network management, including the typical process of eSight deployment and basic operations. Before learning this course, you should be familiar with the basic knowledge about the PON network.

Objectives

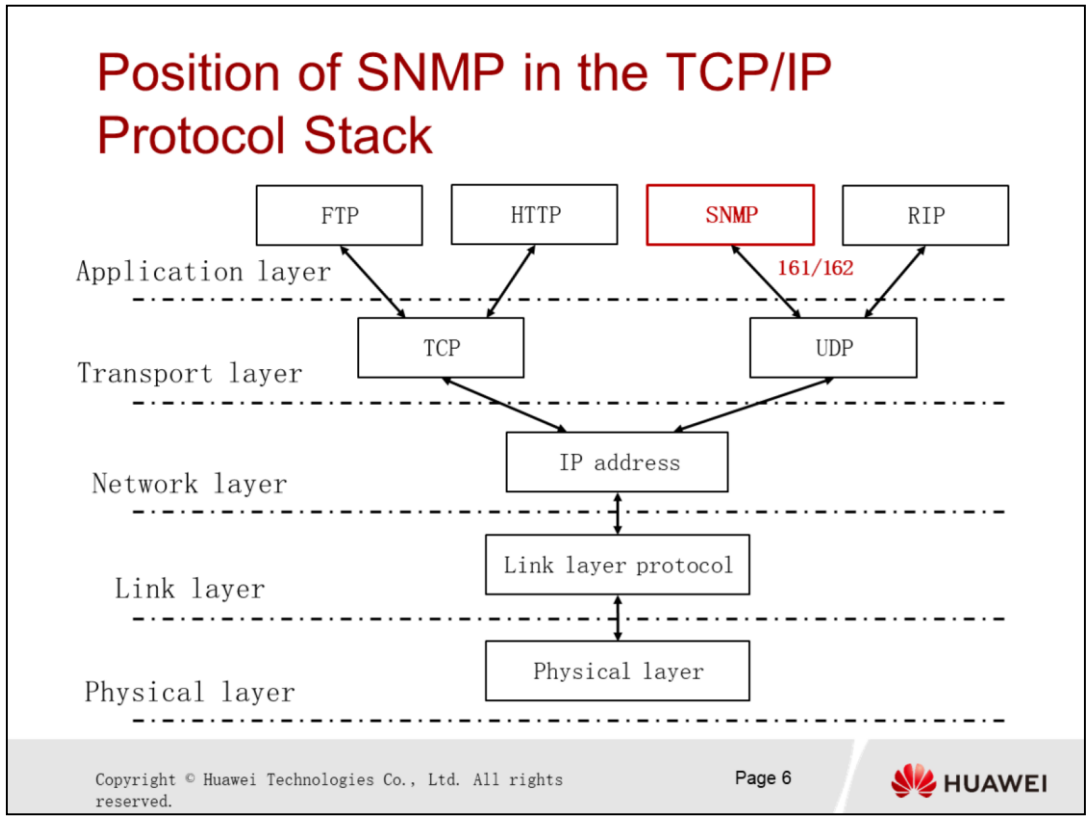
- Upon completion of this course, you will be able to:
  - Understand the principles of the SNMP protocol.
  - Understand the basic functions and features of the eSight for PON network device management.
  - Master basic operations on the eSight.

Contents

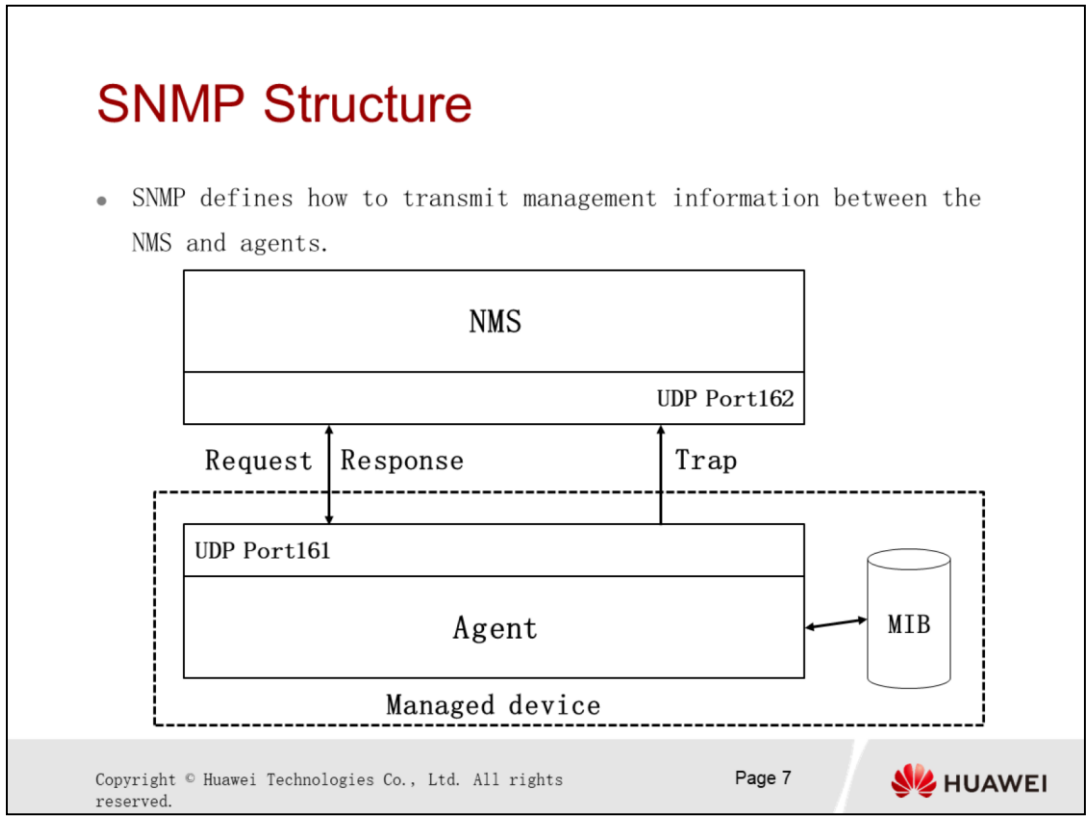
HUAWEI



- The Simple Network Management Protocol (SNMP) is a network management protocol widely used on the TCP/IP network. It provides a method for managing network resources by using a central computer (that is, the network management workstation) that runs the network management software.
- SNMP version:
  - SNMPv1: Easy to implement and weak in security
  - SNMPv2c: More secure and currently widely used
  - SNMPv3: Defines a management framework and introduces the user security model (USM) to provide a secure access mechanism for users.

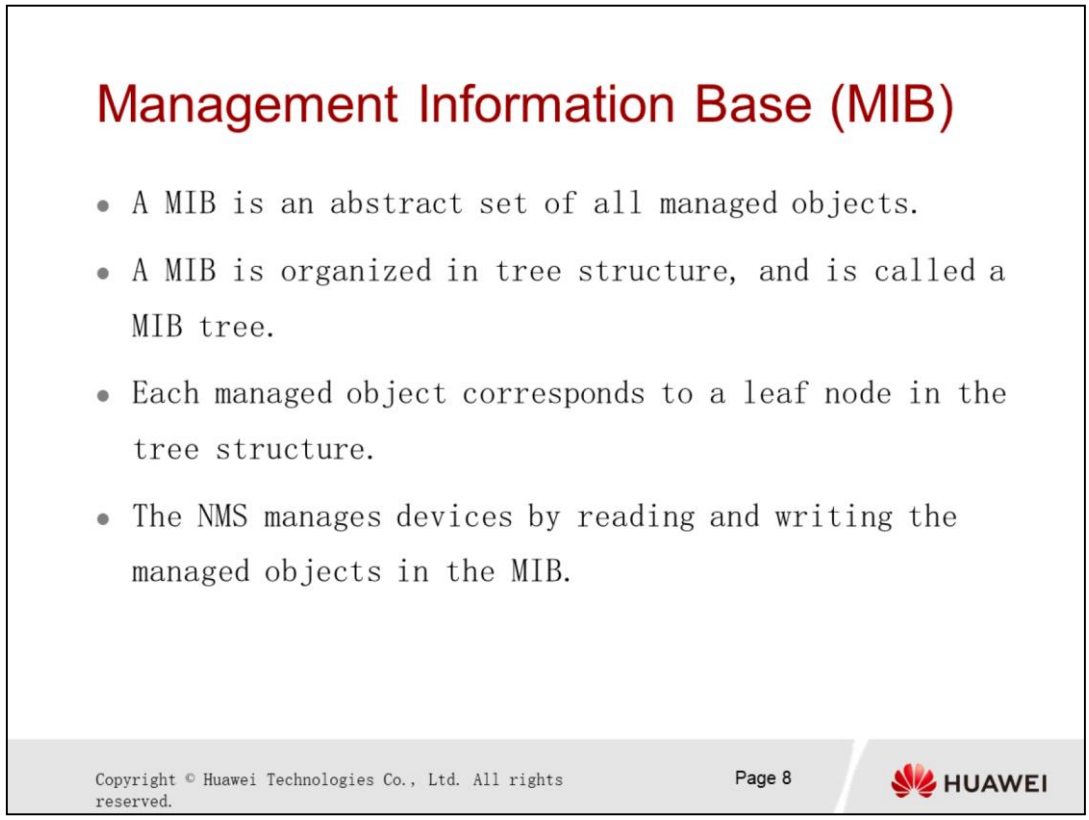


- The SNMP protocol is an application layer protocol of the TCP/IP network. It is the carrier for exchanging information between the NMS and agents using protocol data units (PDUs). SNMP is not responsible for data transmission. Data exchange is implemented through transport layer protocols such as UDP.

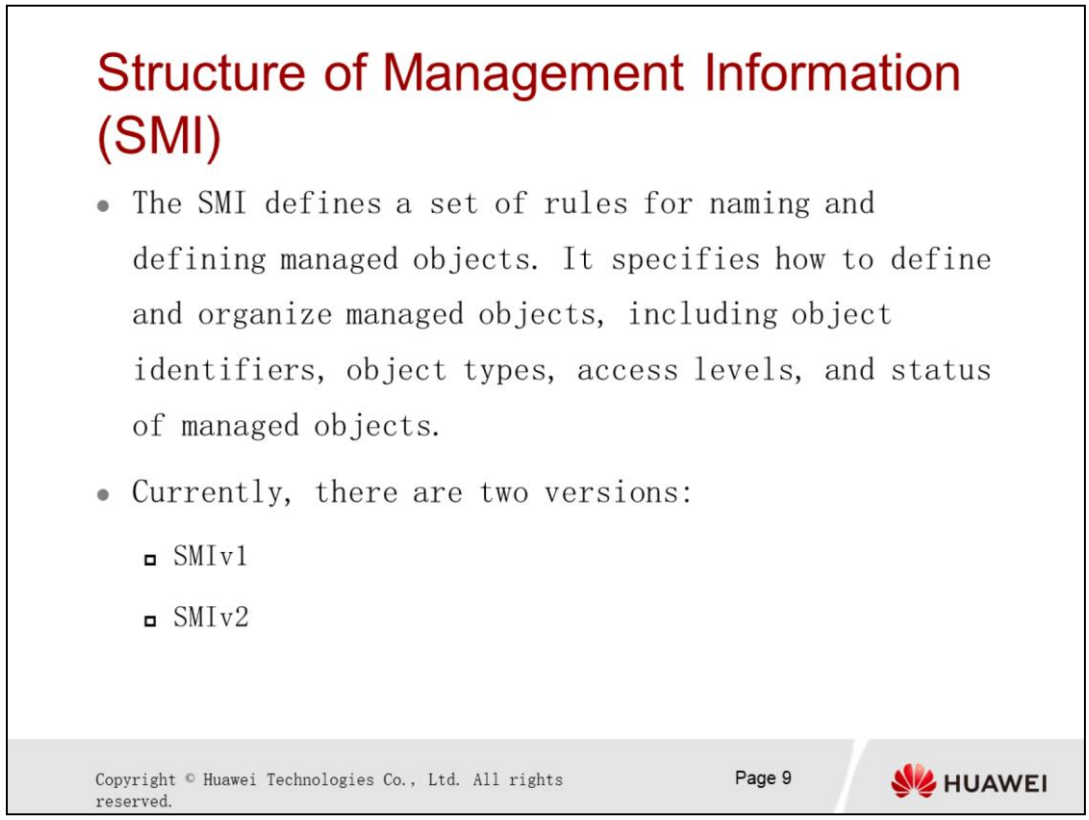


- The SNMP protocol exchanges signaling between the network management workstation and agents.
  - The network management system (NMS) is the network management software running on the NMS workstation. A network administrator performs operations on the NMS, and sends request packets to the managed devices to monitor and configure network devices.
  - The Agent is a proxy process running on a managed device. After receiving a request from the NMS, the managed device responds to the request through the Agent. The main functions of the Agent include collecting the device status, responding to remote operation requests from the NMS, and sending alarm information to the NMS
  - A management information base (MIB) is a virtual database which contains a device status information set and is maintained on a managed device. The Agent collects device status information by searching the MIB. The MIB organizes managed devices according to the hierarchical tree structure and describes the devices in the ASN.1 format.
  - If a module status of a managed device is abnormal, the Agent sends a trap message to the NMS to notify the NMS of the fault. This helps network administrators handle network problems in a timely manner.
- The implementation of SNMP network management consists of three parts: management information base (MIB), structure management information (SMI),

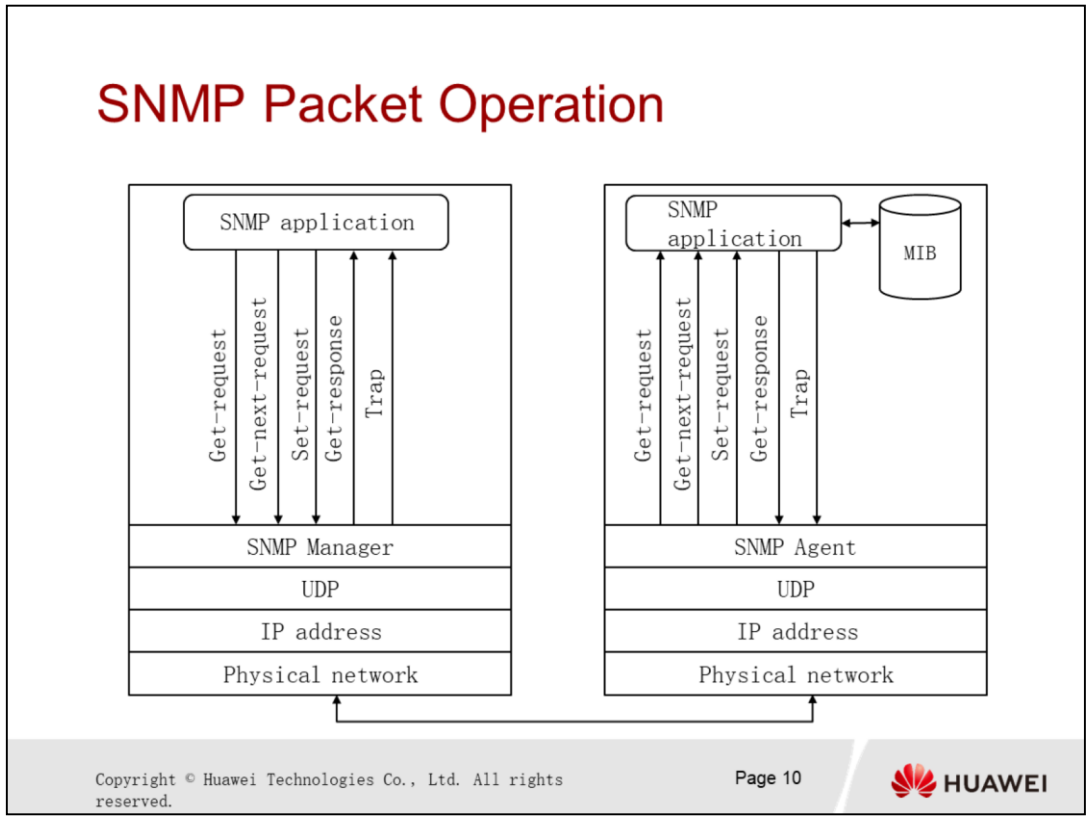
and SNMP.



- A MIB is an abstract set of all managed objects. It is a device status information set maintained on a managed device. Each Agent maintains such a MIB. The NMS can read or set the values of objects in the MIB.
- A MIB is a set of managed objects. It defines a series of attributes of managed objects, including:
  - Name of an object
  - Object access permission
  - Data type of an object



- The SMI defines a set of rules for naming and defining managed objects. It defines the types of data that can be used by MIBs, such as Conter and Gauge. It enables talk between SNMP objects.



- SNMPv1 defines 5 PDUs (also called SNMP packets), which are used for the interaction between the NMS and agents.
- The operations of various packets are as follows:
  - get-request: Extracts one or more parameter values from an agent process.
  - get-next-request: Extracts the next parameter value that follows the current parameter value from an agent process.
  - set-request: Sets one or more parameter values of an agent process.
  - get-response: Returns one or more parameter values. This operation is triggered by an agent process and is the response to the preceding 3 operations.
  - Trap: The agent process sends a trap packet to notify the management process that an event has occurred.
- The following 2 protocol operations are added to SNMPv2c:
  - get-bulk request: This operation is equivalent to multiple getnext operations performed consecutively, and used by the NMS to read information from managed devices in batches.
  - Inform: A managed device sends an alarm to the NMS. The NMS replies with an Inform response message to acknowledge the receipt.

Comparison Between SNMP Versions

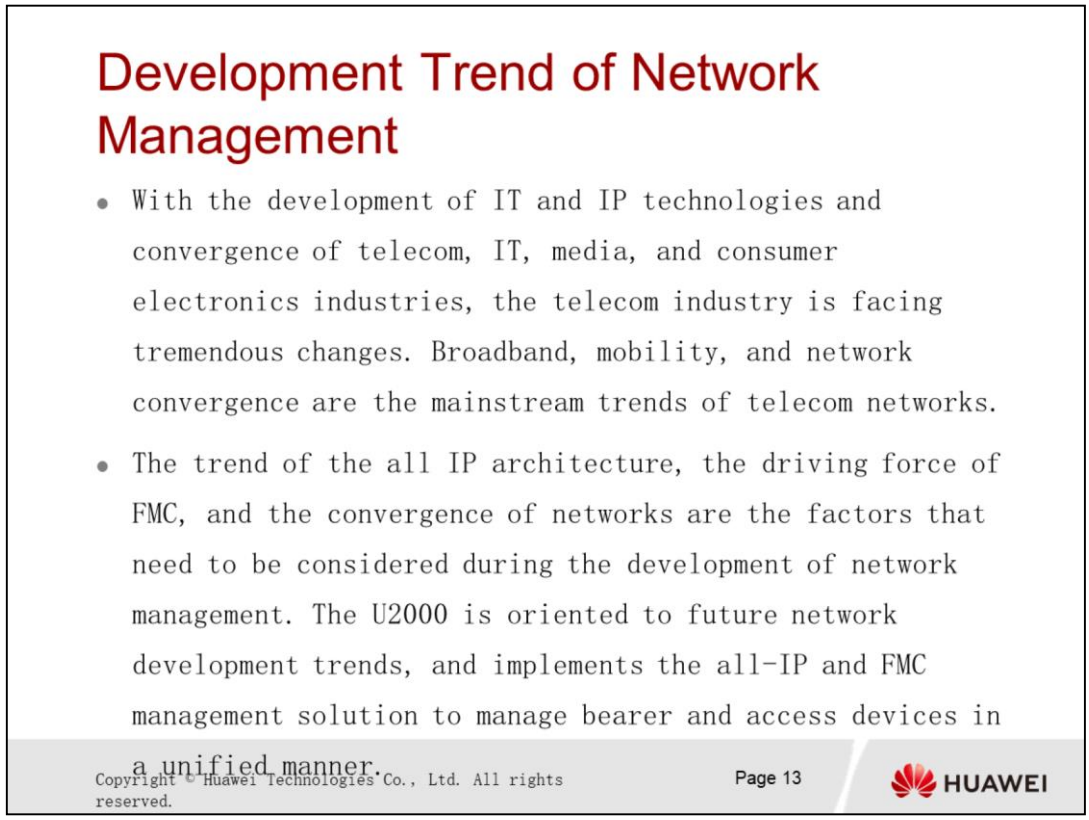
- The SNMP versions include SNMPv1, SNMPv2c, and SNMPv3.
- The implementation principle of SNMPv3 is similar to that of SNMPv1/SNMPv2c. The difference is that identity authentication and encryption are added in SNMPv3.

Protocol Version	User Verification	Encryption	Authentication
V1	No; community name is used.	No	No
V2c	No; community name is used.	No	No
V3	Yes; verification based on the user name	Yes	Yes

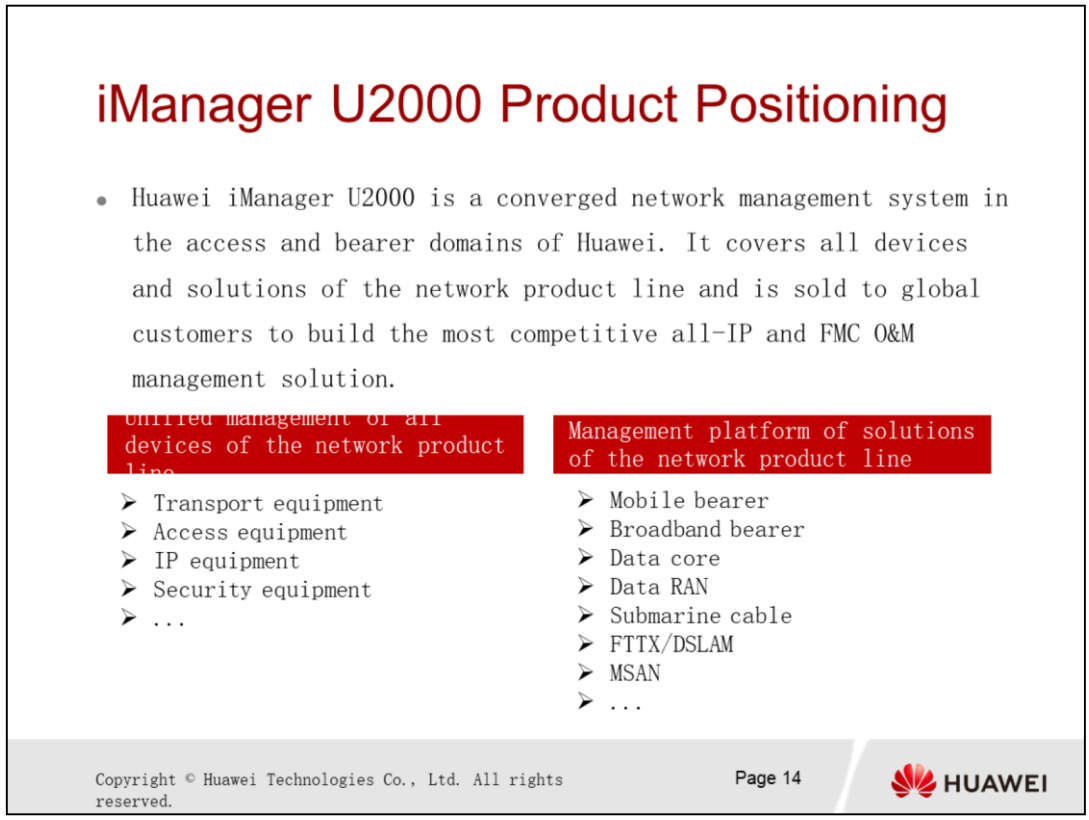
- The SNMP versions include SNMPv1, SNMPv2c, and SNMPv3.
- SNMPv1 and SNMPv2c use community name-based authentication. The NMS controls the device access permission based on a community name list. An agent does not check whether a sender uses an authorized community name. In addition, SNMP messages are not encrypted before transmission. Therefore, the authentication and privacy protection measures are inadequate.
- Based on SNMPv1, SNMPv2c enhances the following functions: Supports more operations, supports more data types, provides richer error processing codes, and supports multiple transmission protocols.
- SNMPv3 security is mainly reflected in data security and access control.
  - SNMPv3 provides message-level data security, including data integrity check, data source verification, and data verification.
  - SNMPv3 access control is a security check based on protocol operations and controls access to managed objects.

Contents

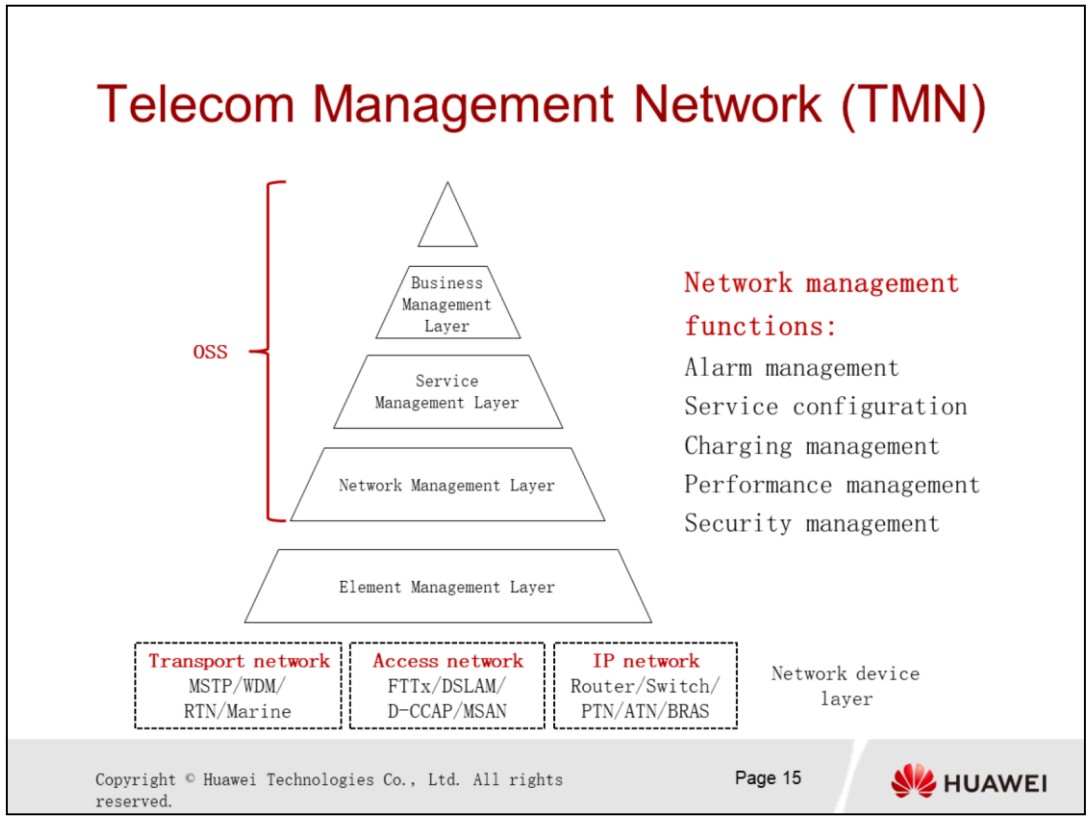
HUAWEI



- Network development and O&M management:
  - The trend of the All IP architecture drives vertical networks that are divided by technologies and services to transfer to a flat horizontal network.
  - The driving force of the fixed-mobile convergence (FMC) comes from improving user experience, reducing OPEX, and improving efficiency.
  - Network convergence brings O&M management convergence.
- To meet the future network development trend, the U2000 implements the all-IP and FMC management solution to centrally manage the bearer and access devices.
  - The U2000 integrates not only the management of devices in multiple domains, but also the management of the NE layer and the network layer, breaking the hierarchical management mode and better meeting the transition management requirements of "vertical network" to "flat horizontal network".
  - The U2000 integrates multiple domains, reducing O&M costs and improving network values.

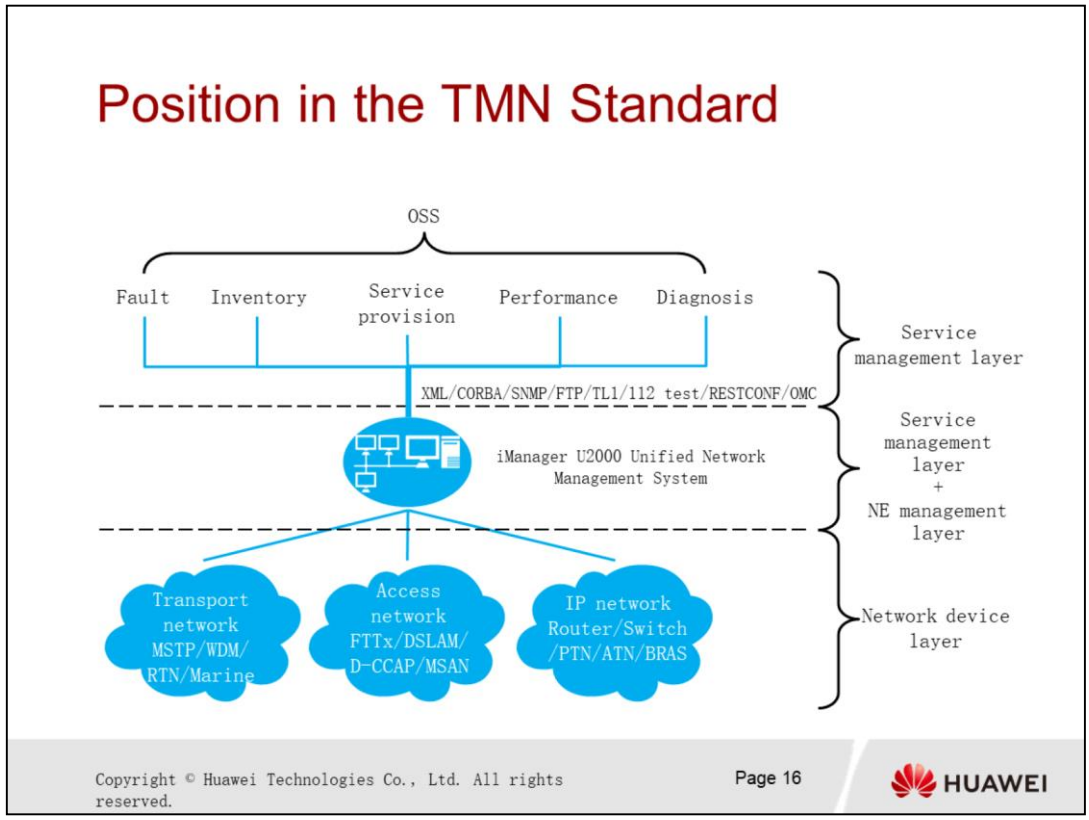


- The U2000 is positioned as the equipment management system of Huawei. It is the main product and solution of Huawei for future network management. It provides powerful management functions at the NE and network layers.

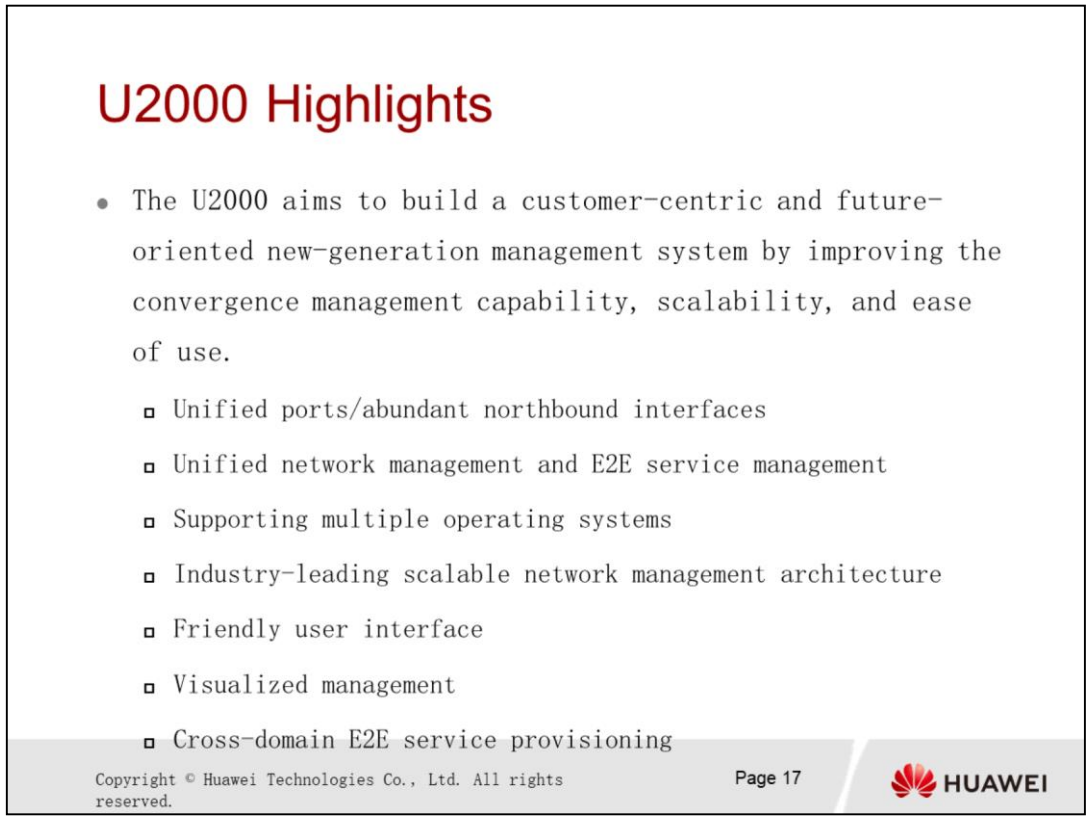


- TMN: telecommunication management network
  - With the increase in the scale and complexity of telecommunication networks, the network management system plays an increasingly important role in improving network service quality, managing network resources, and reducing network management costs.
  - To achieve unified, simple, and standardized management, ITU-T proposes the concept of TMN to support the planning, configuration, installation, operation, and organization of telecom networks and telecom services.
- The functions of the TMN can be classified into the following levels in ascending order:
  - Network device layer: Includes some physical NEs. The management software is the Local Craff Terminal (LCT).
  - NE management layer: Configures and manages a single NE in a centralized manner.
  - Network management layer: Manages all NEs in the managed domain, and is applicable to large-scale and geographically dispersed network management, such as T2100. The main functions include: coordinating and controlling the activities of all NEs from the perspective of the entire network; provisioning, modifying, or terminating network services; and interacting with the upper service management layer in terms of network performance and availability.
  - Service management layer: Provides complete service operation management, including service leasing, broadband wholesale, and VPN.
  - Transaction management layer: Implements transaction related functions, analyzes development trends such as quality issues, and provides

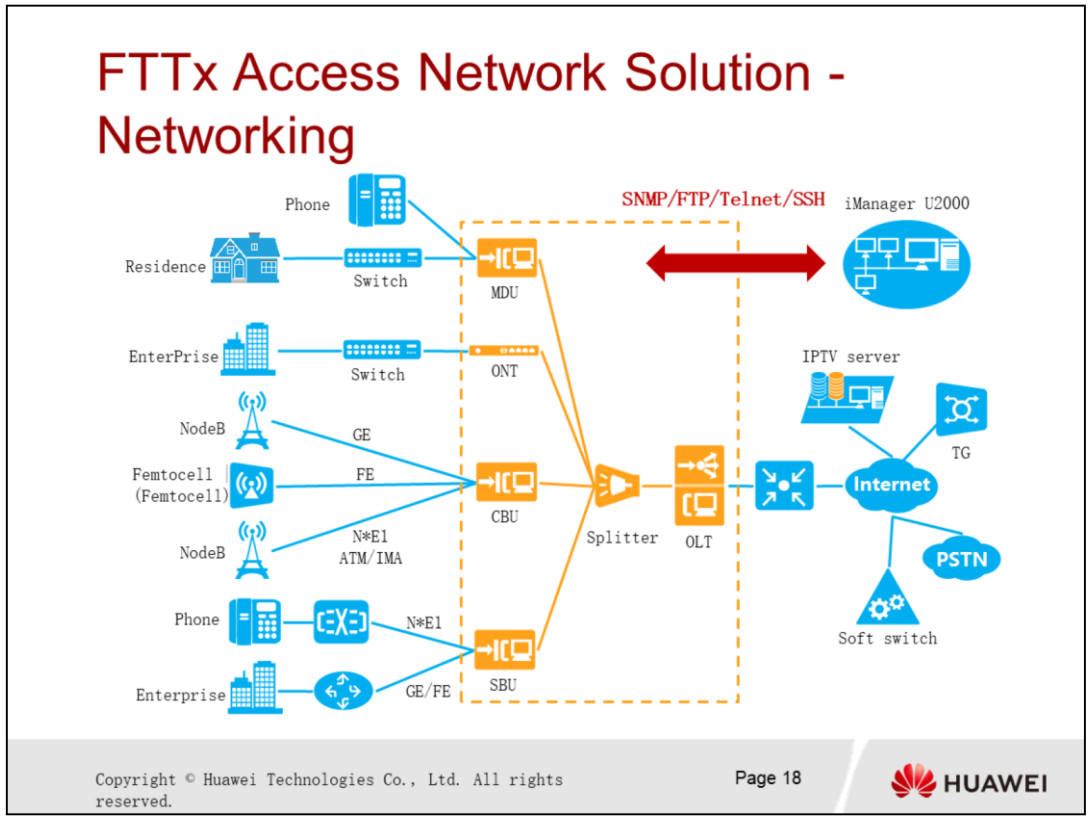
accounting basics and other financial reports.



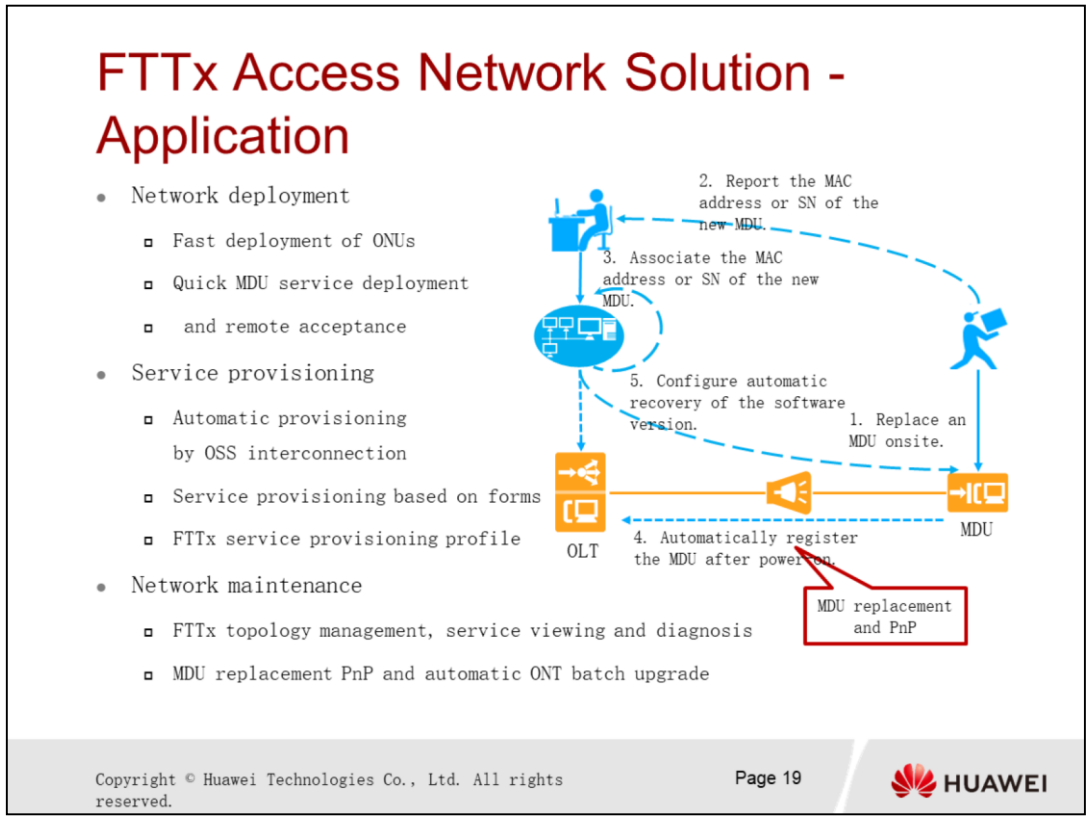
- The U2000 is located between the NE management layer and network management layer in the TMN structure. It has all NE- and network-level functions.
- The U2000 is a typical solution that converges network management applications.
  - The U2000 provides a unified management platform for access, transport, and IP equipment. It not only realizes the convergent management of cross-domain equipment, but also breaks the vertical management mode and realizes the convergent management of the network and NE layers. It supports rights- and domain-based management to separately manage different domains and avoid interference between different departments.
  - The U2000 adapts to the network convergence trend and provides management solutions for multiple networking scenarios. It provides a unified GUI, simple and convenient service provisioning, quick and efficient service monitoring and service assurance, creating excellent user experience and saving network O&M costs
  - The unified northbound interface reduces a large amount of OSS integration work.



- Unified ports/abundant northbound interfaces:
  - The U2000 provides northbound interfaces (NBIs) with unified ports, leading standards, and various types of NBIs to meet customers' OSS integration requirements.
- Unified network management and E2E service management
  - The U2000 manages transport, access, and IP devices in a unified manner, provides E2E service management capabilities, supports management of third-party routers, and supports ICMP and SNMP protocols.
- The following operating systems are supported:
  - The U2000 is based on the Huawei unified management application platform (iMAP). The U2000 is an independent application that can be installed on different operating systems and databases, showing excellent compatibility with multiple operating systems.
- Industry-leading scalable network management architecture:
  - The U2000 uses the client/server (C/S) structure that is mature and widely used. It supports distributed and hierarchical database systems, service processing systems, and client application systems. It adopts a scalable modular architecture and can be split and co-deployed to meet the management requirements of complex and large-scale networks.
- User-friendly GUI:
  - Provides a unified GUI for alarms, topology, performance, security, and configuration management. In addition, it provides user-friendly error messages, indicating the cause of an error and the method of rectifying the fault.
- Visualized management
- Cross-domain E2E service provisioning



- The FTTx access network solution is a large-capacity, long-distance, and high-bandwidth optical fiber access solution provided by Huawei. The U2000 provides a complete solution for managing and maintaining FTTx access network devices, including the OLT, ONU, SBU, and CBU in a unified manner.
- The FTTx access network solution uses a single fiber to provide voice, data, and video services, meeting the fiber to the curb (FTTC), fiber to the building (FTTB), fiber to the home (FTTH), fiber to the office (FTTO), fiber to the mobile base station (FTTM), fiber to the door (Fiber To The Door), fiber to the service area (FTTS), IP private line interconnection, and wholesale networking requirements.
- The figure shows the networking application of the FTTx access NMS.



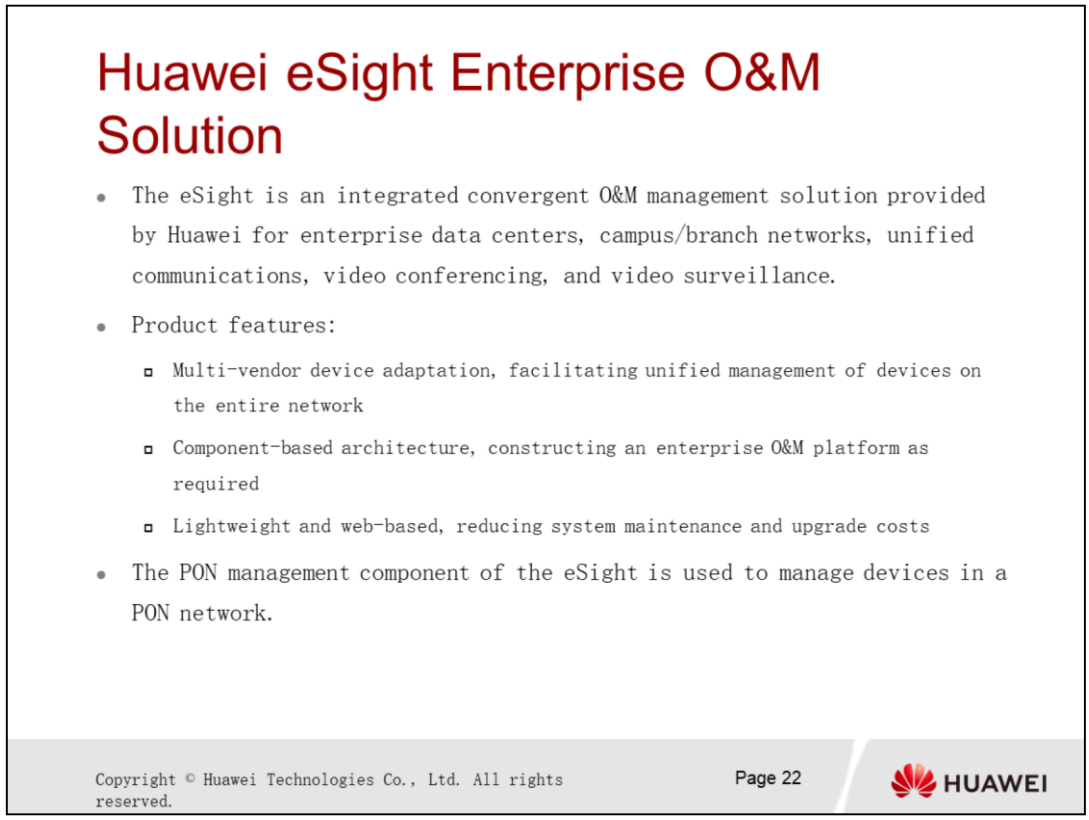
- In the FTTx access NMS networking application, the U2000 provides the 3 functions: network deployment, service provisioning, and network maintenance.
- Network deployment:
  - Fast deployment of ONUs: Supports automatic ONU deployment and remote software commissioning based on the ONU plug-and-play policy.
  - MDU service fast deployment and remote acceptance: Pre-configures services based on Excel sheets to implement MDU plug-and-play for PON upstream transmission. Manual site visits are not required, and results are automatically reported, reducing O&M costs.
- Flexible and efficient FTTx service provisioning:
  - Automatic provisioning by OSS interconnection
  - Batch provisioning of forms
  - FTTx service provisioning profiles, enabling one-click GUI provisioning
- Network maintenance:
  - FTTx topology management and hierarchical service assurance
  - E2E service query and diagnosis for FTTB & FTTH
  - Fast service recovery: MDU replacement and plug-and-play, and PON port service cutover
  - Automatic batch ONT upgrade

Contents

HUAWEI

Enterprise Network Management Requirements

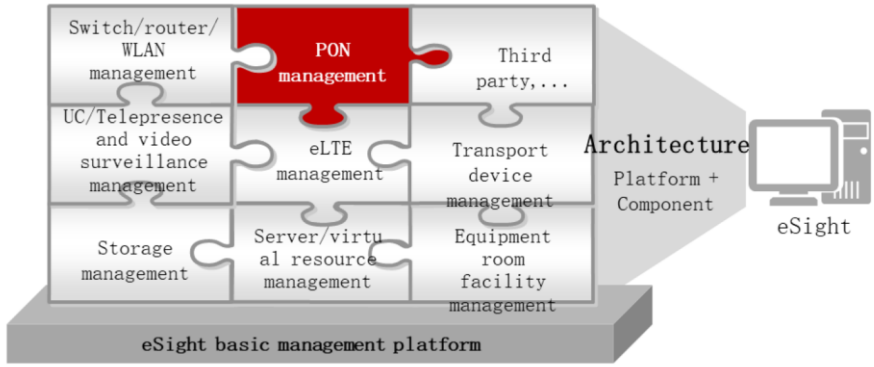
- The number of devices increases.
  - As the number of devices increases, the complexity of network management increases. This means that more maintenance support personnel are required, which increases the equipment maintenance cost.
- Unified management of devices from multiple vendors
  - Each time a network device of a vendor is introduced, the NMS of the corresponding vendor needs to be introduced, and only the devices of the vendor can be managed. The operation interface and management contents of the NMSs are different.
- A network management platform that supports large-scale and portable management is required. Standard and universal network management protocols should be used to implement efficient and unified management of the entire network.



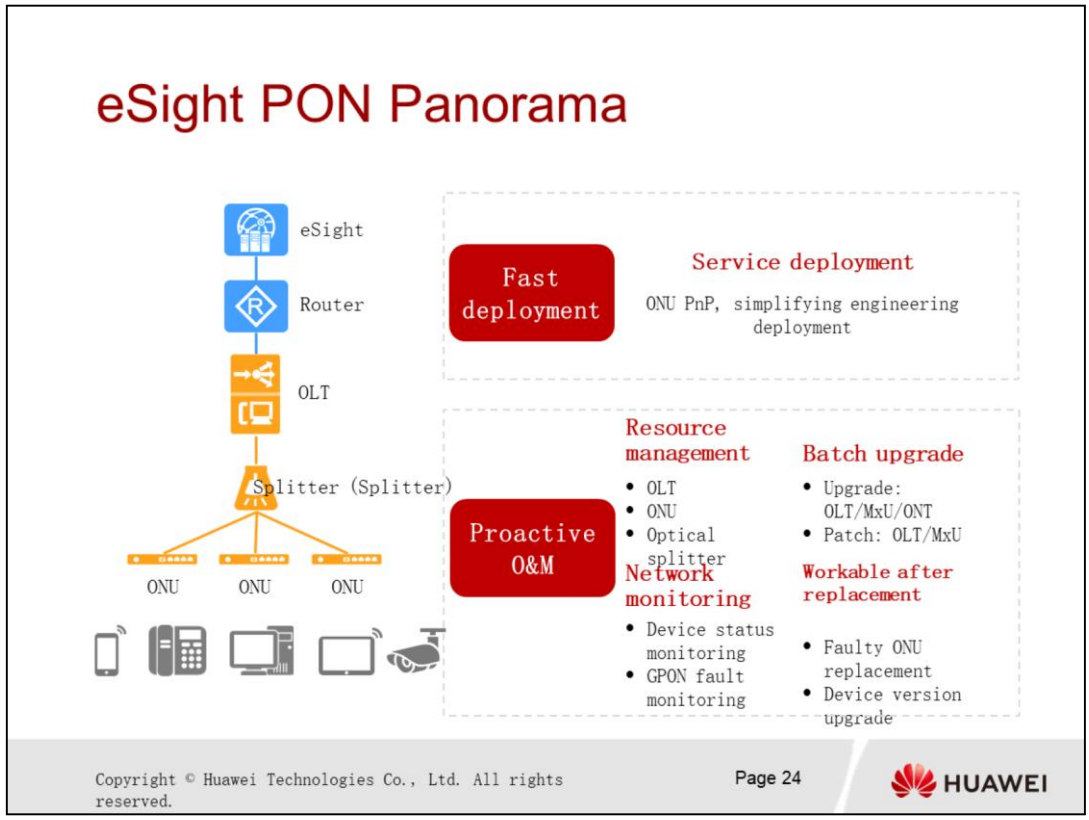
- Product features:
- Multi-vendor device adaptation facilitates unified management of devices on the entire network.
  - The eSight provides open interfaces that can be integrated to support unified management of Huawei servers, storage devices, virtualization devices, switches, routers, WLAN devices, firewalls, PON devices, eLTE devices, unified communications devices, telepresence devices, video surveillance devices, application systems, and equipment room facilities. It is also pre-integrated with capabilities for managing devices from mainstream third parties, such as HP, Cisco, and H3C.
- The componentized architecture can be used to construct an enterprise O&M platform as required.
  - The eSight uses a componentized architecture and provides various components on the unified eSight management platform. Customers can select components based on site requirements.
- Lightweight and web-based structure reduces system maintenance and upgrade costs.
  - The eSight uses the B/S architecture. Clients do not need to install any plug-ins and can access the eSight anytime anywhere. During system upgrade or maintenance, you only need to update the server software, reducing the system maintenance and upgrade costs.
  - Visualized diagnosis and centralized O&M improve O&M efficiency.

eSight PON Network Management

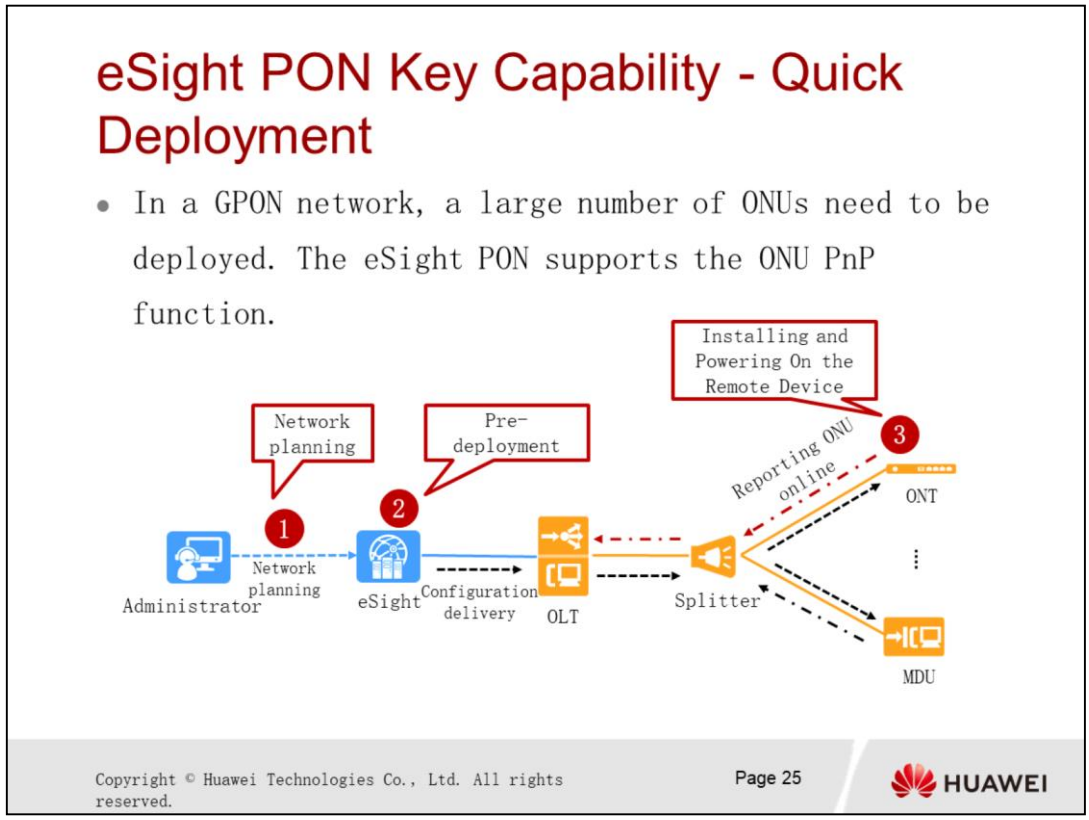
- The PON management component of the eSight is used to manage devices in a PON network. It manages PON device resources (OLTs, optical splitters, and ONUs) and related services, and monitors PON network quality and device running status.



- The eSight uses a componentized architecture and provides various components on the unified eSight management platform. The preceding figure shows the eSight componentized architecture view. The PON management component is a component that manages PON network devices.

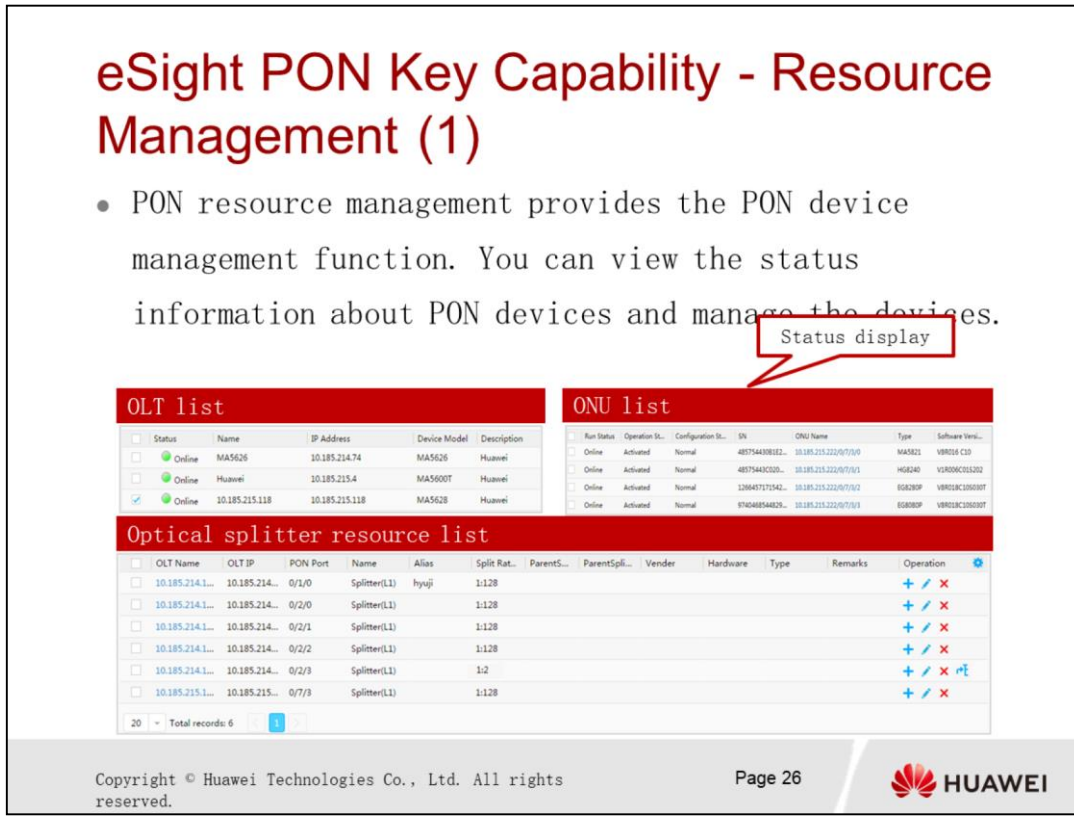


- Main functions:
  - Service deployment: ONUs support plug-and-play, simplifying engineering deployment.
  - Resource management: Manages device resources such as OLTs, ONUs, and optical splitters.
  - Network monitoring: Monitors the device status and GPON fault.
  - Batch upgrade: Upgrade the OLT/MxU/ONT and install the OLT/MxU patches.
  - Workable after replacement: Faulty ONUs can be replaced and the device version can be upgraded.



- In a GPON network, a large number of ONUs need to be deployed. The eSight PON supports the ONU plug-and-play function. That is, after the OLT is deployed, the PON terminal devices (including the MxU and ONT) can be deployed on the network. A network administrator does not need to commission the software on the installation site. After a PON terminal is powered on, services can be configured according to the preset plug-and-play policy, improving the deployment efficiency.
- Network planning:
  - Plan the device location, upstream interface, management IP address, management VLAN, and other network and service parameters.
- Pre-deployment:
  - Configure the ONU plug-and-play policy.
  - Set the parameters related to the OLT and associate the ONU plug-and-play policy.
- Install and power on a remote device.
  - After an ONU is installed and powered on onsite, the ONU automatically sends a go-online notification to the OLT. The eSight verifies the device and selects deployment configurations based on the pre-deployment policy, and delivers the pre-deployment configurations to the ONU through the OMCI channel. After the configurations take effect,

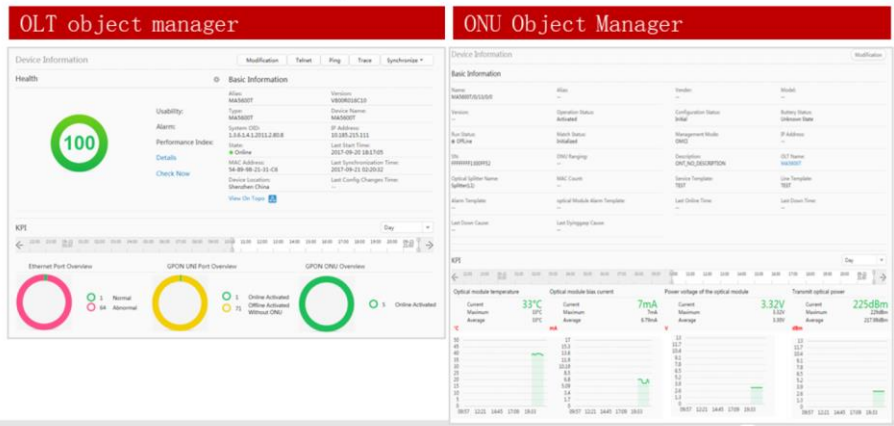
services are automatically enabled.



- The eSight PON resource management function centrally manages PON device resources on the entire network, including optical splitter resource management, OLT resource management, and ONU resource management. Key service data is displayed in a centralized manner to show the network quality in real time.
- OLT resource management
  - Provides a list of OLTs managed by the system in a resource table. The OLT basic information can be viewed and filtered.
  - Allows users to synchronize and jump to the physical topology, switch to the OLT device manager by name, and view detailed information.
- ONU resource management
  - Provides a list of ONUs managed by the system in a resource table. The basic ONU information can be viewed and filtered.
  - Allows users to move ONUs, replace ONUs, modify ONU aliases, set polling parameters, jump to an ONU manager by the ONU name, and view detailed information.
- Optical splitter resource management
  - Provides a list of optical splitters managed by the system in a resource table. The basic optical splitter information can be viewed and filtered.
  - Allows users to add, move, modify, and delete optical splitters, and import optical splitters in batches.

eSight PON Key Capability - Resource Management (2)

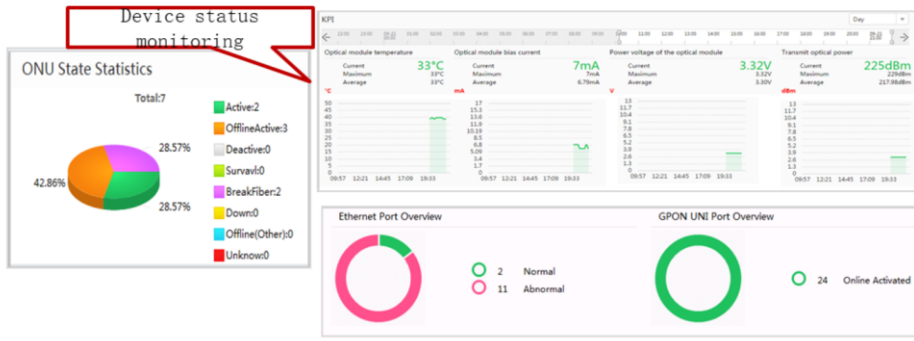
- In the Object Manager, you can view the detailed information about the OLT/ONU/optical splitter, such as the basic information, health status, and KPIs.



- More abundant KPIs are provided, making the object manager a 360-degree view of network maintenance.
- PON electronic label
  - Displays the list of PON device electronic labels in a resource table and supports the export function.
- Device software version management
  - Allows users to view, upload, modify, and delete device software versions.
  - Creates device software upgrade tasks based on the selected upgrade options and uploaded software version files. Provides a list of created tasks in a table, and displays the task progress and status.
- Backup task for device configuration file management
  - Backs up the running configuration files of the devices in tasks by day, week, or month at a specified time.
  - Backs up the configuration of a specified device, or restores the configuration files of a selected device.

eSight PON Key Capability - Network Monitoring (1)

- The GPON network monitoring function monitors device status and collects statistics on device performance indicators, such as CPU usage, memory usage, Ethernet port usage, and GPON UNI port usage. When a PON network is faulty, O&M personnel can locate the fault based on the reported alarm information.

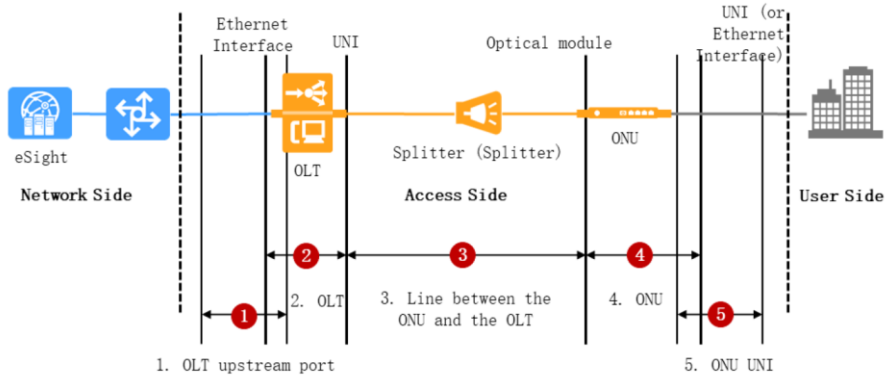


HUAWEI

- GPON network monitoring helps quick fault locating.
  - Lists and displays the OLTs, ONUs, and optical splitters in a centralized manner. Users can obtain device information in one-stop mode.
  - Displays device alarm information in a centralized manner. Users can analyze and determine the fault type and quickly locate the node where a fault has occurred based on the alarm name, alarm source, and location information.

eSight PON Key Capability - Network Monitoring (2)

- The eSight provides various monitoring methods for the GPON network. If any problem occurs on the network, alarms are displayed. It is recommended that you monitor the GPON network according to the following principles:

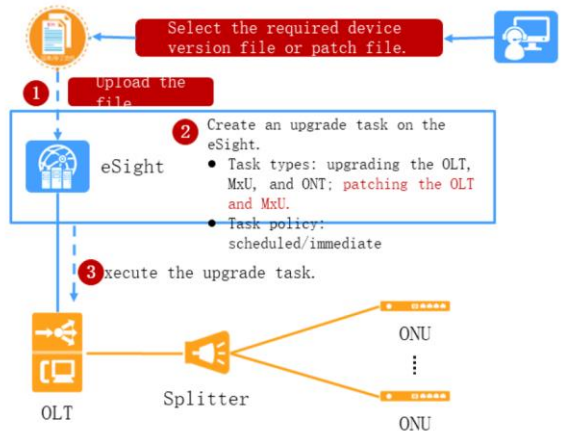


HUAWEI

- Monitoring the upstream port of the OLT
  - Monitors the status of the link between the OLT and upstream devices, the transmit/receive packet loss rate of the OLT upstream port, and the broadband usage.
- Monitoring the OLT
  - Generally, the OLT is located in an equipment room and less likely to become faulty. An OLT fault is commonly caused by a board fault which is directly reflected on the interface. You are advised to monitor the status of the interfaces.
- Monitoring the line between an ONU and the OLT
  - The line profile is a common cause of faults on a GPON network. You are advised to check the status of each monitoring point and take preventive measures accordingly.
- Monitoring the ONU
  - Common faults of an ONU are caused by power failures and board faults. Power failures can be monitored by the ONU status. Board faults are directly reflected on the ONU user network interfaces (UNIs).
- Monitoring ONU UNI
  - Faults in customer terminals account for 50% of the entire GPON network faults, but eSight cannot directly monitor the status of terminal devices. The communication status between a client terminal and the ONU can be indirectly monitored by the status of the ONU UNI.
  - The eSight checks the ONU UNI status using the ONU NE explorer or ONU topology.

eSight PON Key Capability - Batch Upgrade

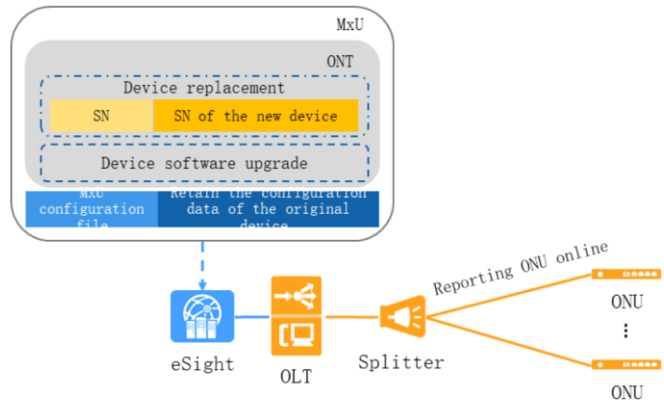
- The eSight PON supports wizard-based device software upgrade to implement fast and batch remote upgrade of PON devices.



- Manually upgrading communication devices to the same version in batches
  - Add, modify, and delete versions by configuring a version upgrade task.
  - Configure the upgrade object, upgrade type, and upgrade version using the upgrade wizard. The eSight supports immediate upgrade and scheduled upgrade.
  - Monitor and manage the entire device upgrade process to view the upgrade progress, structure, and version of the devices.
  - Query the detailed history records of the device upgrade.

eSight PON Key Capability - Workable After Replacement

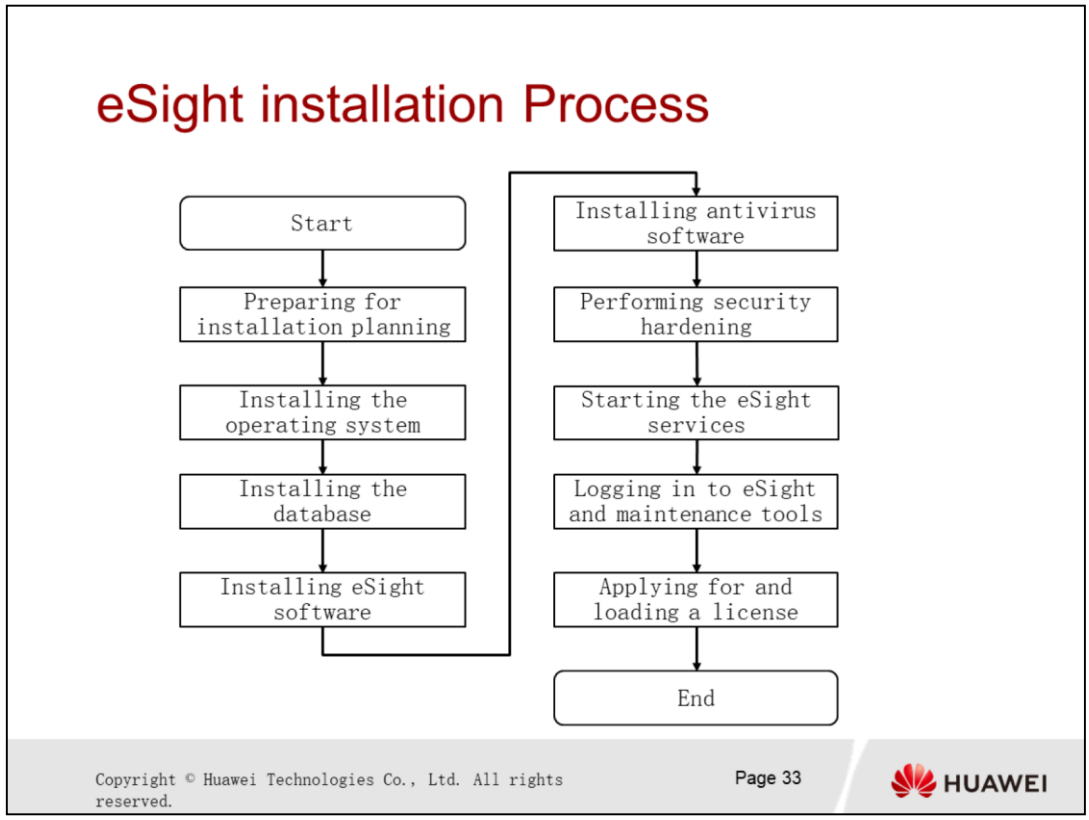
- The eSight PON supports ONU replacement. A device that fails or cannot meet new service requirements can be replaced in time.



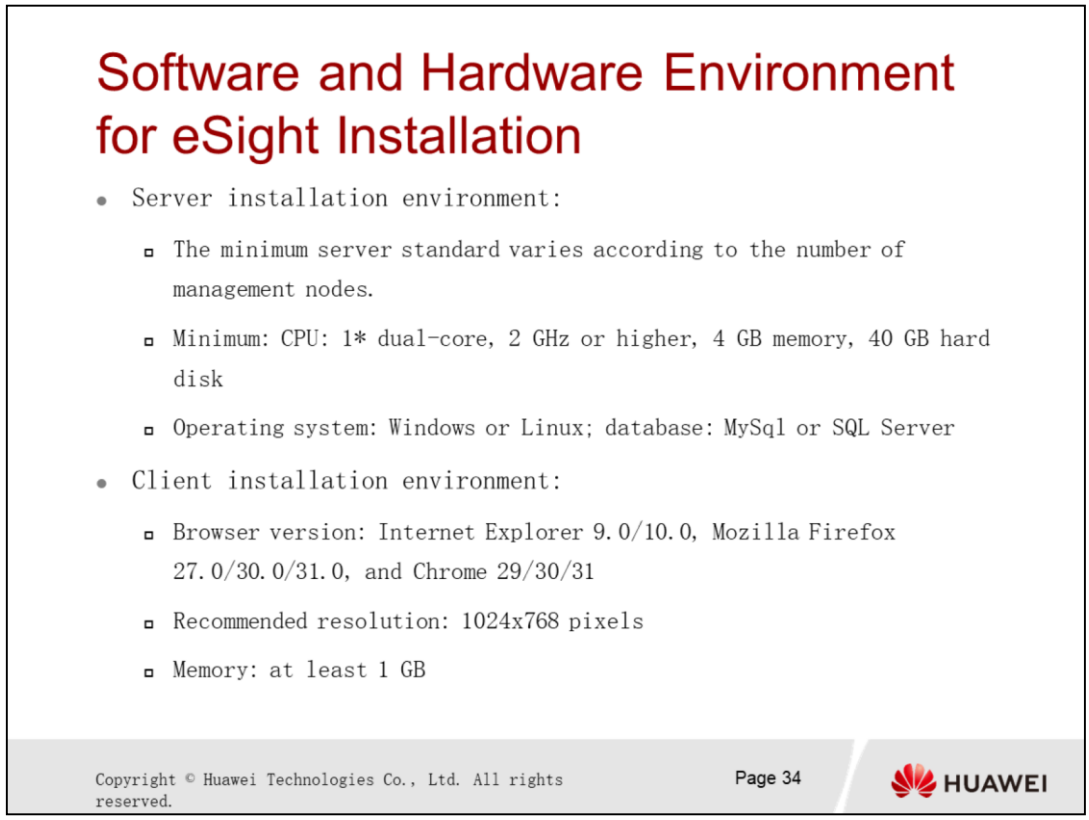
- Fast network recovery:
  - Devices can be upgraded remotely in batches. As many as 300 ONTs can be upgraded per hour, greatly improving the upgrade efficiency.
  - If an ONU needs to be replaced, the MxU configuration file can be backed up in advance so that the new device inherits the configuration data of the original device. In this way, the network can be quickly restored to meet service requirements.

Contents

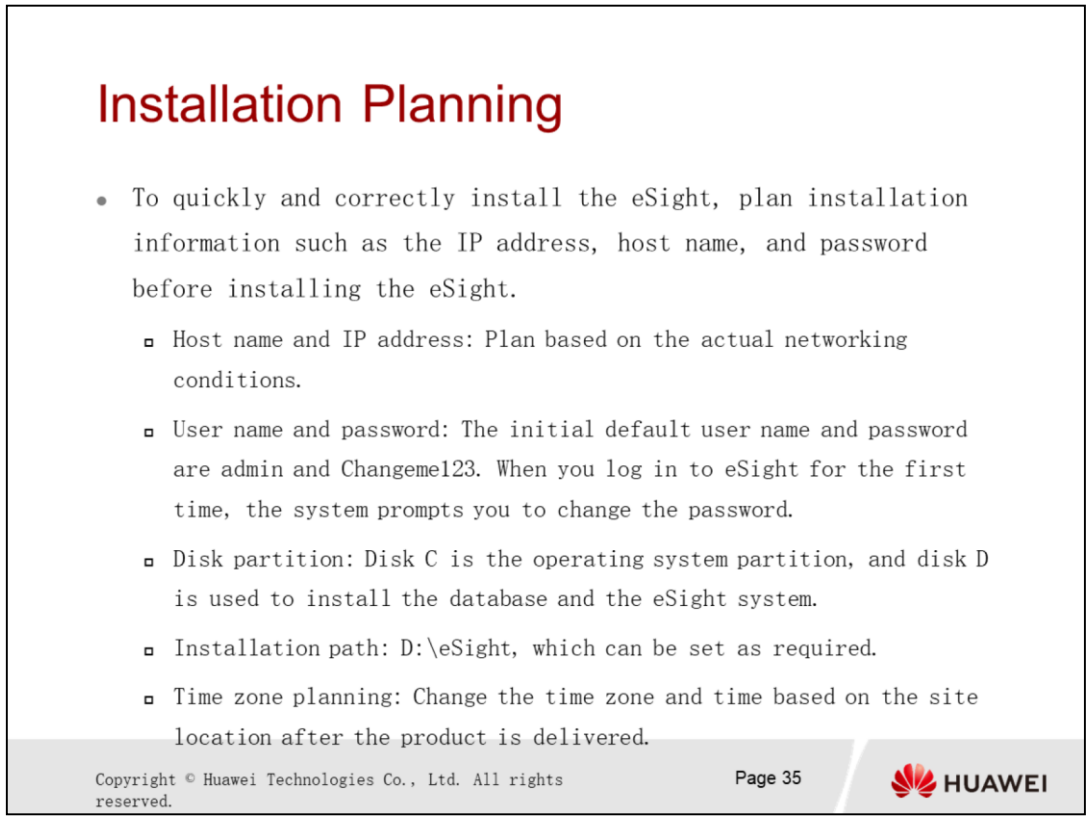
HUAWEI



- Pre-installation scheme: The servers delivered by Huawei have been pre-installed with an operating system and the eSight system.
- New installation scheme: If a server is purchased from another vendor or the eSight system needs to be reinstalled, refer to the installation process shown in the figure.



- Recommended operating system and database versions for the server installation environment:
  - Configuration 1: Windows Server 2008 R2 Standard (64-bit) (Chinese simplified or English version), Windows Server 2012 R1 Standard (64-bit) (Chinese simplified or English version) + MySql 5.5 (included in the standard NMS software package) /Microsoft SQL Server 2008 R2-Standard Edition
  - Configuration 2: Novell SuSE LINUX Enterprise Server-Multi-language version -Enterprise version -11.0 SP3 (Chinese simplified or English version) + Oracle Database Standard Edition 11g R2
  - Note: Configuration 2 is recommended if there are more than 20,000 management nodes.
- There is no special operating system requirement on the client installation environment. The browser version and internal storage must meet certain requirements.



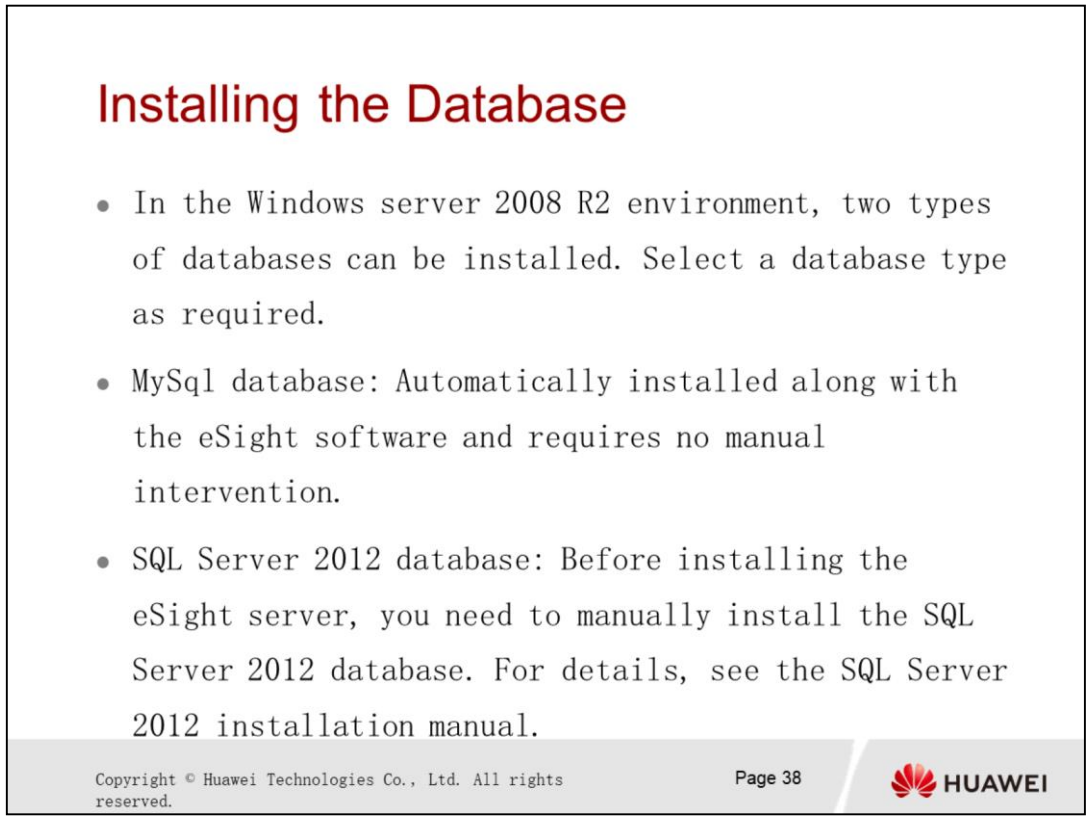
- eSight server host names:
  - Must be unique on the network.
  - Consists of letters (case sensitive), digits, and hyphens (-). The first character must be a letter.
  - Contains 2 to 24 characters
- eSight server IP address:
  - Static IP addresses must be used.
  - The eSight supports IPv4, IPv6, and IPv4/IPv6 dual stacks. Plan the IP address based on the actual networking.
  - The server can communicate with the managed devices properly.
  - The server communicates with clients properly.
- eSight installation path:
  - The eSight software cannot be installed in the root directory.
  - It is not recommended that eSight be installed in the system partition.

Obtaining Software

- The eSight can be installed in either of the following ways:
  - Using the CD-ROM
  - Using the software package
- To obtain the software:
  - Log in to the Huawei enterprise technical support website. (http://support.huawei.com/enterprise)
  - Browse or search for eSight.
  - On the Software tab page, download the eSight software and digital signature.

Contents

HUAWEI



- When installing the SQL Server 2012 database, you need to specify the password of the SQL Server system administrator account sa.
  - The password can contain only uppercase and lowercase letters, digits, and the following special characters:

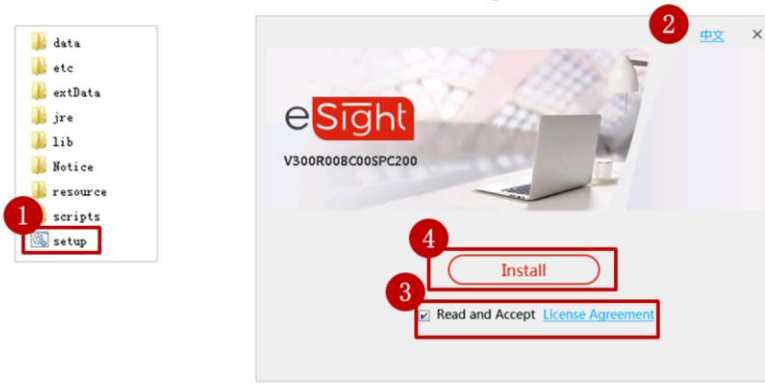
    ~@#^*()-_+|[{}];,/?
  - The password must contain 8 to 32 characters.
- After installing the SQL Server 2012 database, you can check whether the installation is successful by viewing the information in the SQL Server Configuration Manager.
  - In addition, you need to make network configurations for the SQL Server. Otherwise, the eSight cannot access the database.

Contents

HUAWEI

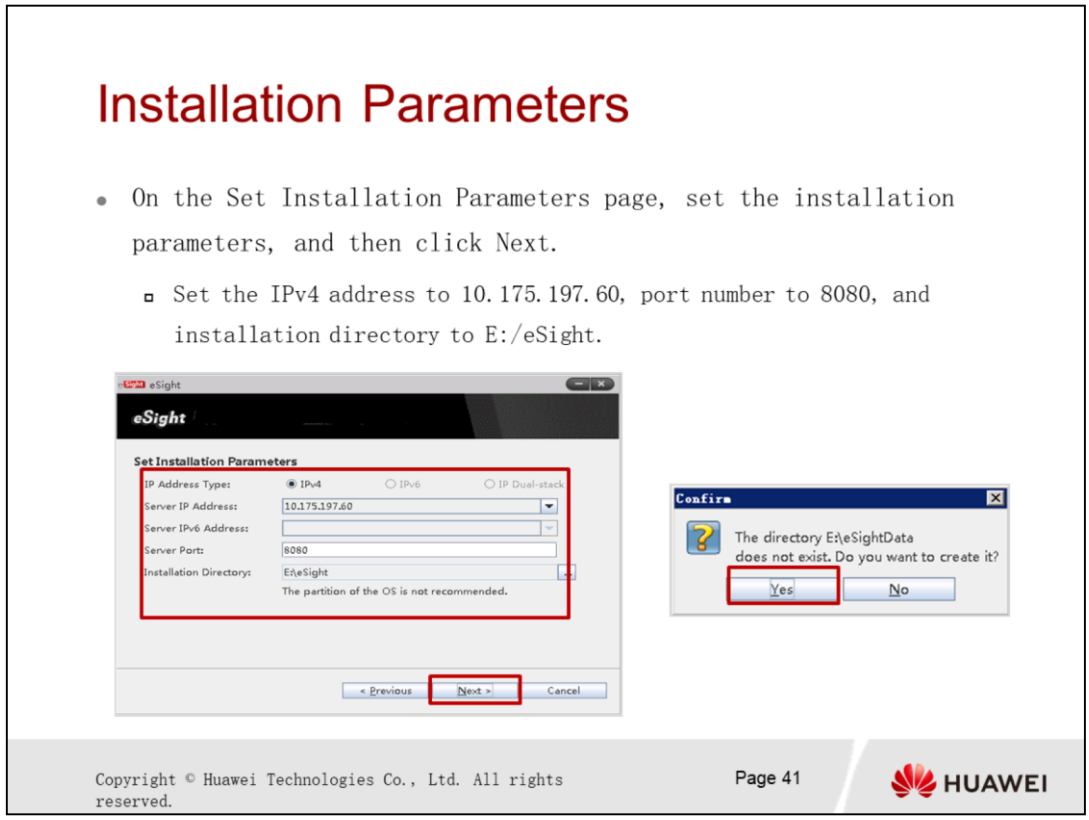
Starting eSight Installation

- Run setup.bat to enter the installation process. Select the language of the installation CD-ROM and the NMS. Select Read and Accept and click Install.

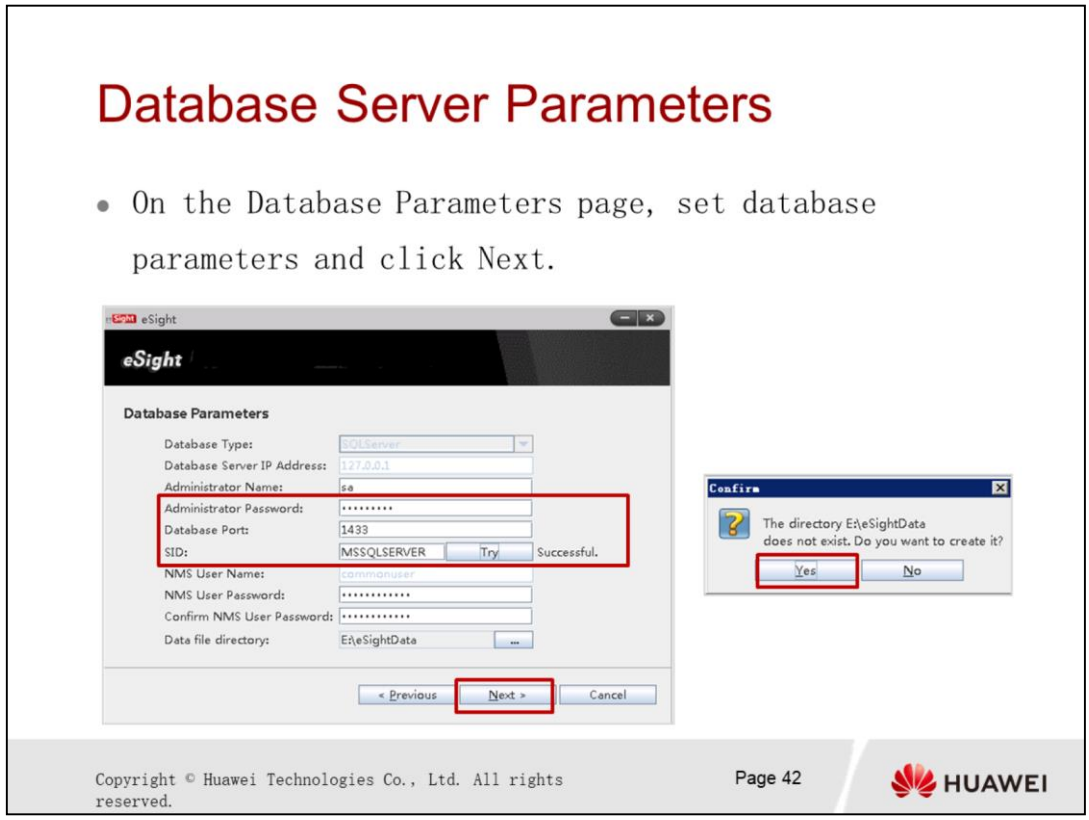


HUAWEI

- Double-click **setup** in the installation package directory to start the installation program. In this case, select to install the eSight V300R008C00SPC200 software and select **English** as the language. Read the license agreement, select **Read and Accept**, and click **Install**.
- The system automatically checks whether the current environment meets the eSight installation requirements. If the current environment does not meet the eSight installation requirements, the system displays a message. After the fault is rectified, reinstall the eSight.
- Once the installation language is selected, the language cannot be changed after the installation is complete. You can only reinstall the eSight to change the language.



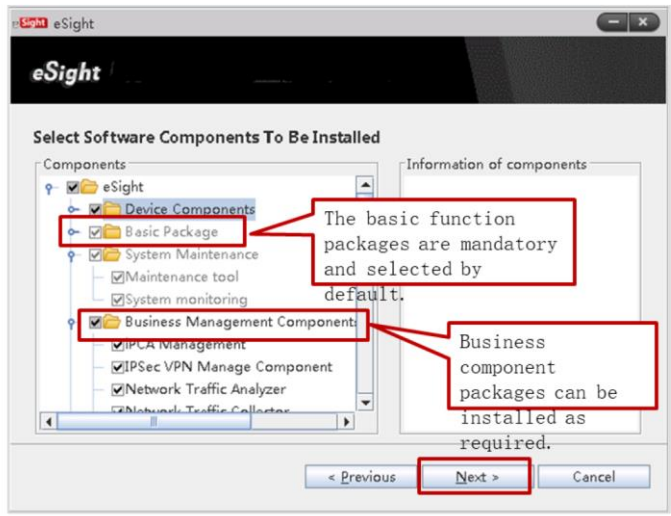
- Ensure that the eSight software installation path is empty. Otherwise, eSight cannot be installed.
- If the installation directory does not exist, the system asks you whether to create a directory. Click **Yes**. The system automatically creates the directory.
- Installation parameter settings:
  - IP address type: indicates IP address type of the eSight server. The eSight supports IPv4, IPv6, and IP dual-stack. Select a proper type based on network planning.
  - IP address: indicates the default IP address of the current server. If the server has multiple IP addresses, select an available IP address that can be used by the eSight to communicate with external entities from the drop-down list box.
  - Port: The default port number is 8080. If the port number is occupied, change it to another port number.
  - Installation path: Indicates the eSight installation path. You can manually change the path, for example, E:\eSight. The default value is D:\eSight. The eSight software cannot be installed in the root directory.



- If the database type is SQL Server and the eSight is installed for the first time, enter the user name **sa** and password **Changeme123.**
- Database server parameter settings:
  - Administrator Name: The default user name is **sa**, which is the default administrator account of the SQL Server database and has the highest permission on the database. You can set a user with the same rights as the **sa** user if necessary.
  - Administrator Password: The default value is **Changeme123.** If the database password is different from the default password, enter the password of the database administrator.
  - Database Port: The default port is 1433. If the database port number is different from the default port number, enter the database port number manually.
  - SID: Indicates the database instance name. The default value is **MSSQLSERVER.** If the actual database instance name is different from the default value, enter the actual database instance name.
  - NMS User Password: The default password of the database NMS user is **Changeme_123.**
  - Data file directory: indicates the path for storing data files. The default path is D:\eSightData. You can change the path manually. If the specified directory does not exist, the system asks you whether to create a directory. Click **Yes.** The system automatically creates the

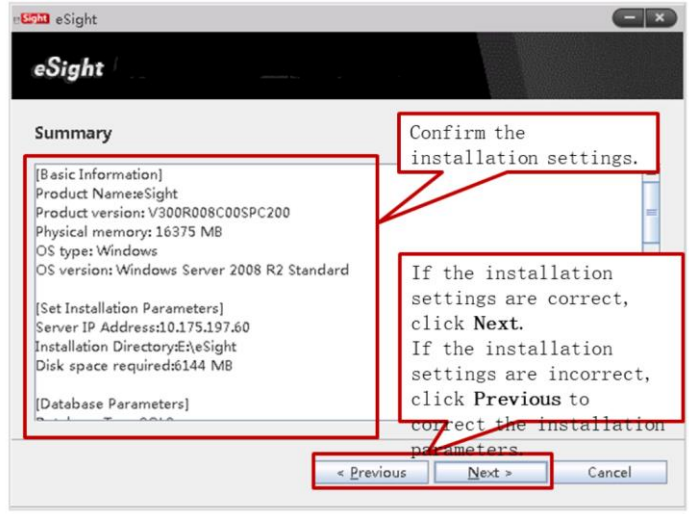
directory.

Selecting Components to Be Installed



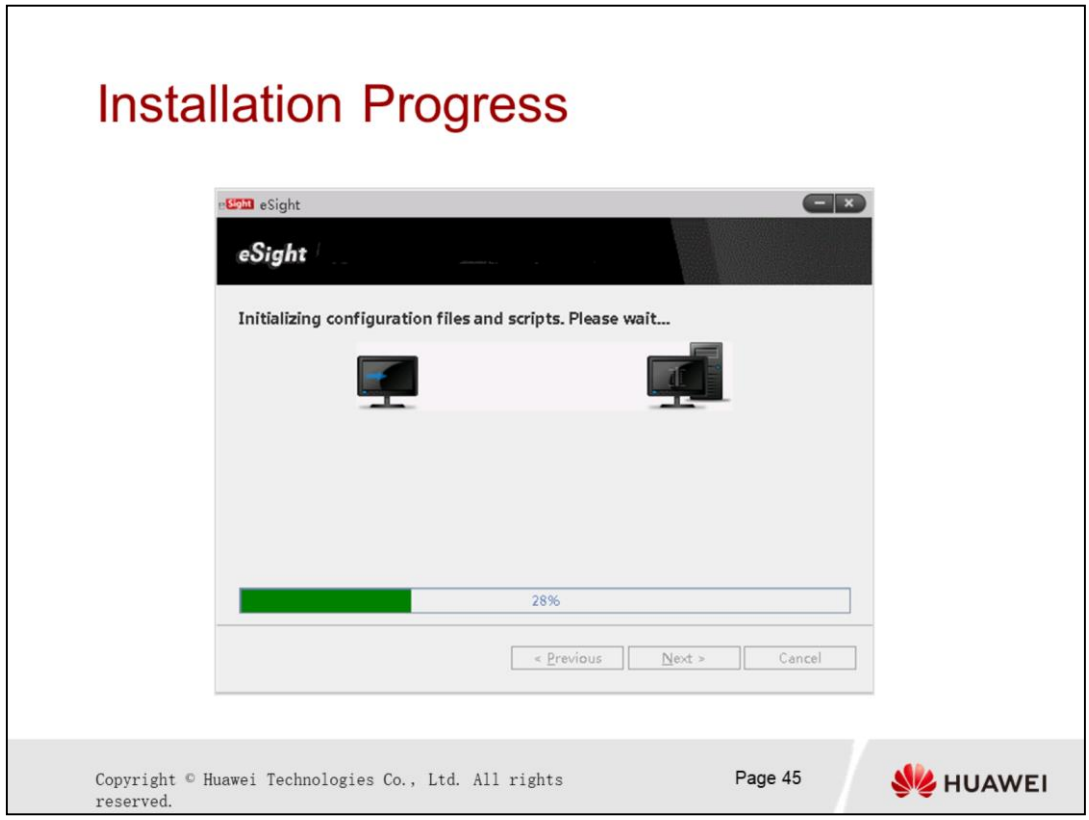
- In the **Select Software Components To Be Installed dialog** box, select the components to be installed and click **Next**.
- The functions of the components are controlled by licenses. If a license is not purchased, the corresponding function cannot be used after the installation. Different licenses enable different components.
- The components under **Basic Package** are mandatory and dimmed by default. Select to install components under **Business Management Component** according to the actual situation.
- The **eSight** supports incremental component installation. That is, if a component is not installed during the first installation of the eSight, you can continue to install the component when installing the eSight for the second time. Ensure that the version number of the installation package during incremental installation is the same as that of the eSight.

Confirm the Summary Information

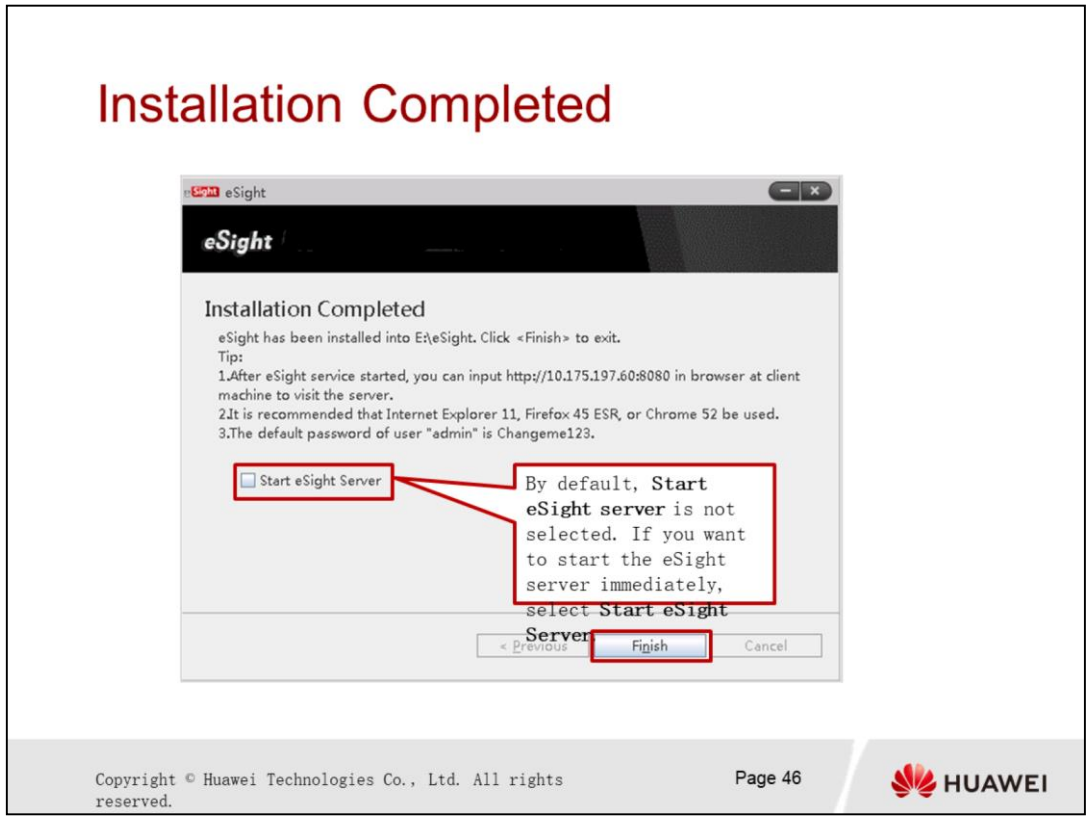


HUAWEI

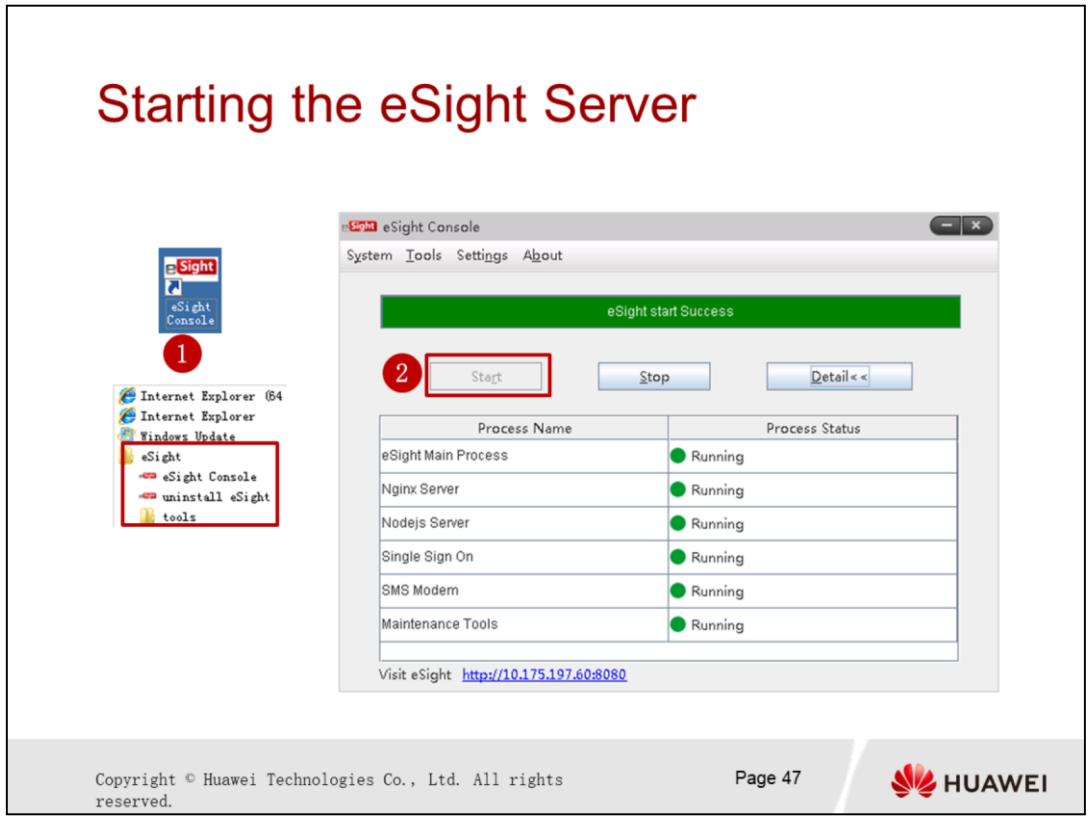
- On the **Summary** page, confirm the installation settings and click **Next**. If the installation setting is incorrect, click **Previous** to set the installation parameters again.



- The system starts to install eSight. The installation takes about 15 minutes. After the installation is complete, click **Finish** in the **Installation Completed** dialog box.



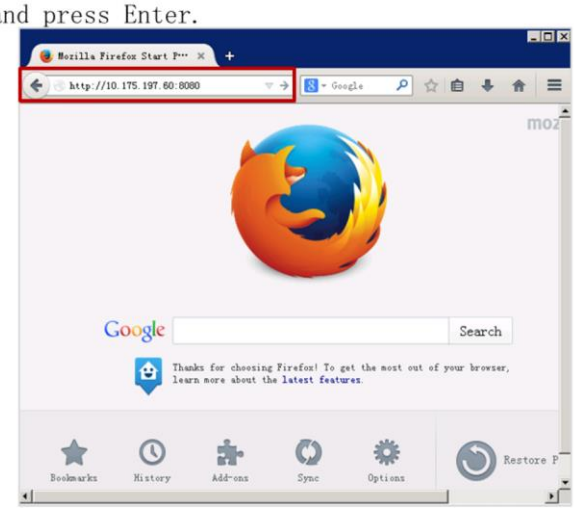
- After the installation is complete, the system does not select **Start eSight Server** by default. To start the eSight server immediately, select **Start eSight Server** and click **Finish**.



- To start the eSight server, perform the following steps:
  - Double-click the eSight Console shortcut icon on the desktop and click **Start** to start the eSight server.
  - Choose **Start** > **All Programs** > **eSight** > **eSight Console**, and click **Start** to start the eSight server.
- On the **eSight Console** page, click **Start**. Wait for several minutes. The console is successfully started.
- If the eSight server needs to be automatically started when the operating system restarts, perform the following steps: On the main menu, choose **Settings** > **Automatic Startup**.

Logging In to eSight Using a Browser

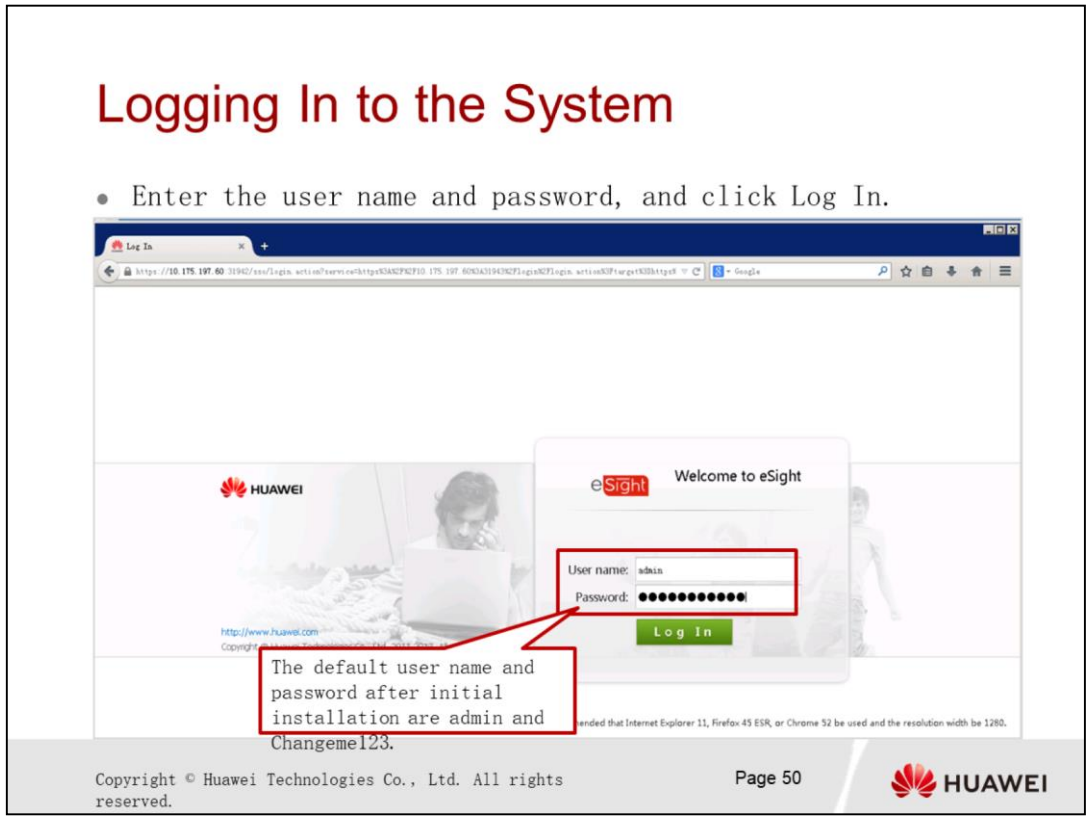
- Enter http://10.175.197.60:8080/ in the address box of the browser and press Enter.



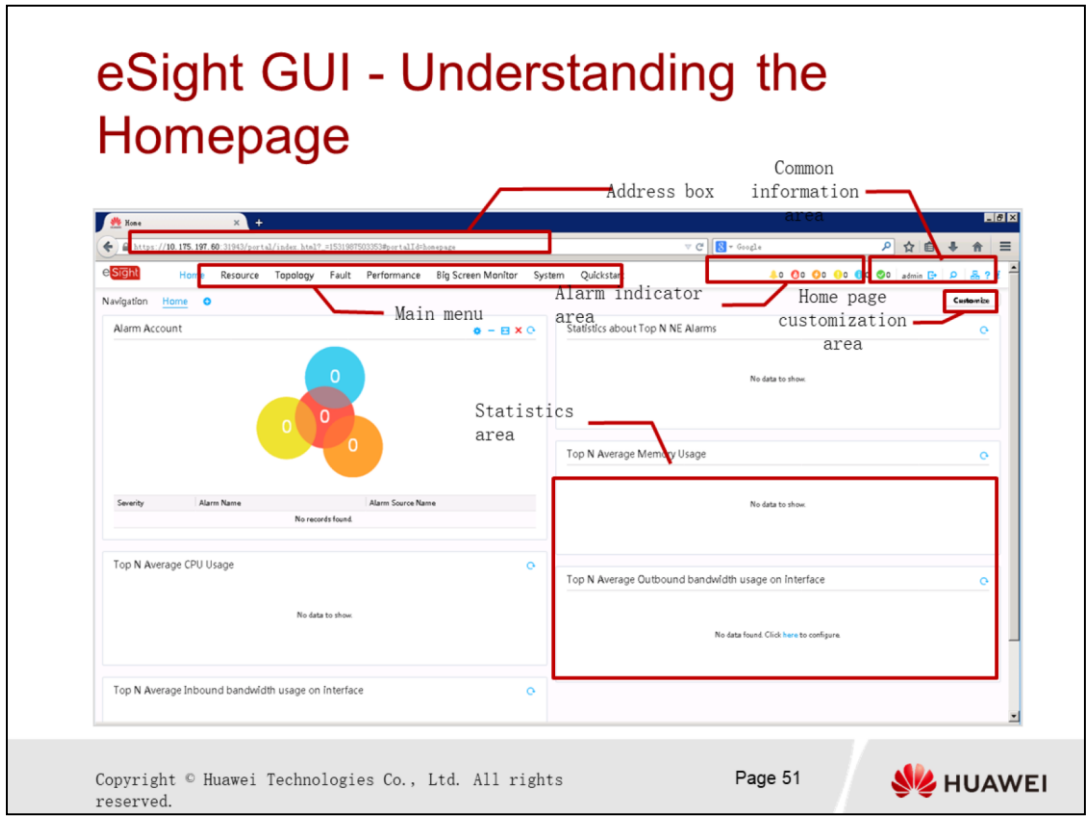
HUAWEI

- Log in to the eSight from a client browser and check whether the eSight version and functions are normal.
  - Open a browser, enter http://*eSight server IP address*:port number in the address box, and press **Enter**.
  - In this example, the IP address is **10.175.197.60**, and the default eSight port number is **8080**.
  - If the server has multiple IP addresses, enter the IP address selected during eSight software installation. Otherwise, you cannot log in to the eSight.
  - If a message is displayed indicating that the website security certificate is incorrect, install the security certificate first.
  - If the server IP address entered in the address box is localhost or 127.0.0.1, the security certificate cannot be installed.
- The Windows Internet Explorer 11, Firefox 45 ESR, and Chrome 52 browsers are recommended.

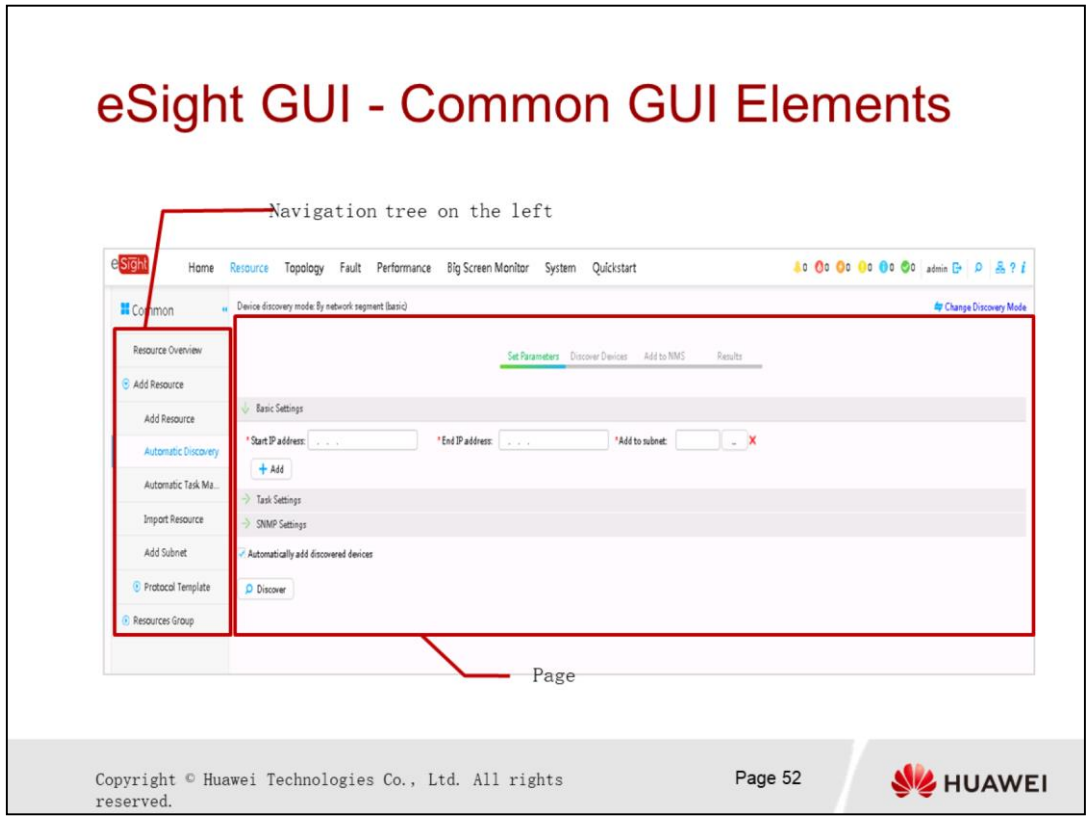
- If Firefox browser displays a message indicating that the security certificate is incorrect, the possible causes are as follows:
  - The security certificate is incorrect or the eSight security certificate is not installed. Install a valid security certificate.
- Handling method:
  - Method 1: Deploy a certificate issued by a CA to eSight.
  - Method 2: Set the eSight built-in certificate as a browser trusted certificate.
  - You are advised to use method 1 to deploy the certificate issued by a CA to eSight. Method 2 may not take effect in some scenarios due to browser version differences.
- In the preceding figure, if a security certificate error occurs in the Firefox browser, you need to set the browser trust certificate. On the page that is displayed, click **Add Exception**. On the **Add Security Exception** page that is displayed, click **Get Certificate** to obtain the certificate, and then click **Confirm Security Exception** to confirm the security certificate.



- After logging in to eSight for the first time, change the password as prompted. For example, change the password to Huawei123 and keep the new password secure. If the password of the admin user is lost, you need to reinstall the eSight to restore the default password.
- When logging in to the eSight, enter the correct user name and password.
  - If an admin user attempts to log in to the eSight and enters incorrect passwords for 5 consecutive times within 10 minutes, the login IP address is locked for 10 minutes.
  - If a common user attempts to log into the system and enters incorrect passwords for a number of times reaching the account restriction conditions, the account is locked for 30 minutes by default.
  - A user can log in to the system again after the lockout duration expires. A common user can also contact the administrator to unlock the account and then log in to the system again.
- If a password is about to expire, the eSight prompts you to change the password within the validity period.



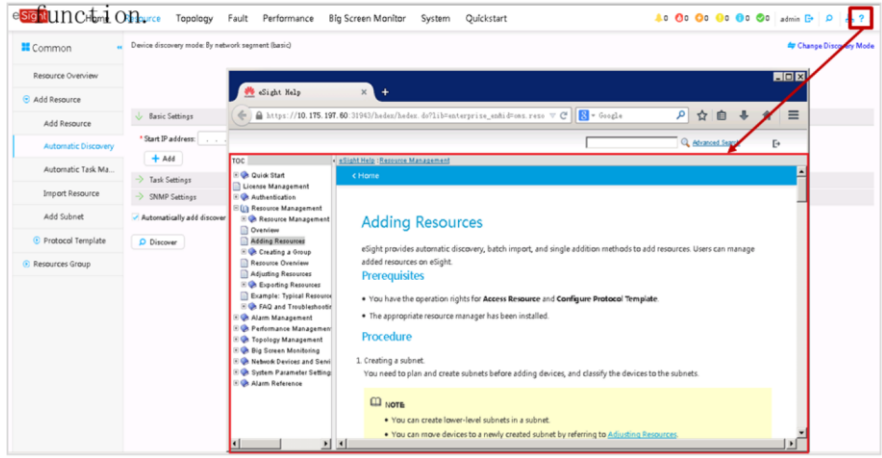
- Main menu: Displays main entries for eSight functions.
- Alarm indicator area: Displays the total number of alarms, uncleared critical alarms, uncleared major alarms, uncleared minor alarms, uncleared warning alarms, and cleared alarms from left to right.
- Common information area: Displays the following common eSight information from left to right: user name, logout, global search, website map, help, and about.
- Home page customization area: Displays the device data status using the protlet. This feature enables users to detect and handle abnormal device status in a timely manner and ensure normal device running.
    - The portlet displays the device status and network-wide status in a list, curve chart, or bar chart in each area on the home page.
- Statistics area: Displays device status and service statistics based on the customized status, including top N average CPU usage, top N average memory usage, and so on.



- Navigation tree on the left: Access the main menu and select a specific function from the navigation tree to access the operation page of the function.
- Page: This area is used to perform specific operations on the eSight.

eSight GUI - Online Help

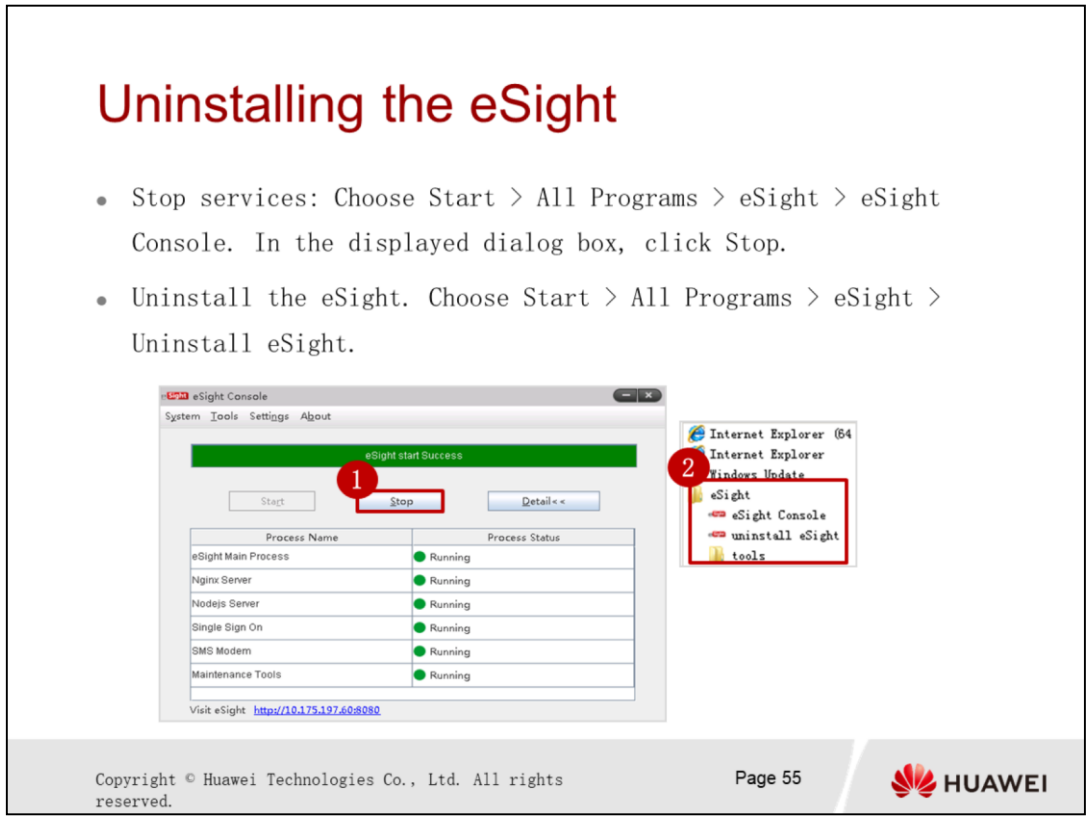
- On any operation page of the eSight, click Help. The eSight automatically switches to the help information of the current function.



HUAWEI

Contents

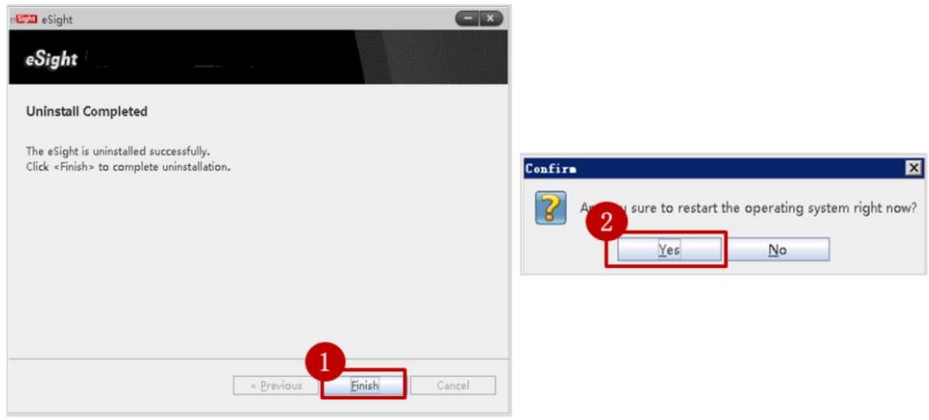
HUAWEI



- Choose **Start > All Programs > eSight > eSight Console**. In the dialog box that is displayed, click **Stop**.
  - When the system displays a message indicating that the status of each process is stopped and the message **stopping eSight system succeeded** is displayed, the services are stopped.
- Choose **Start > All Programs > eSight > Uninstall eSight** to start the uninstallation program.
  - In the displayed eSight uninstallation wizard, click **Next**.
  - In the displayed Confirm dialog box, click **Yes**.
  - The system starts uninstalling the eSight. The uninstallation takes about 10 minutes.

Uninstallation Completed

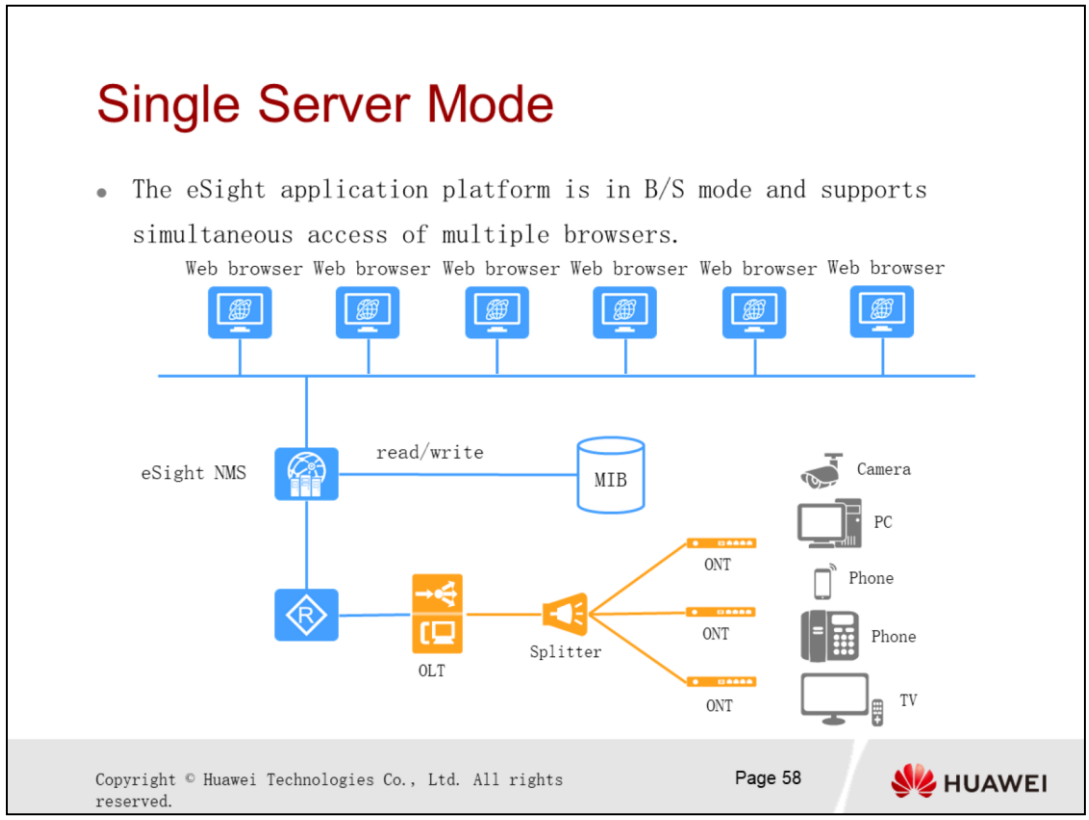
- Click Next as prompted to complete the uninstallation and restart the operating system.



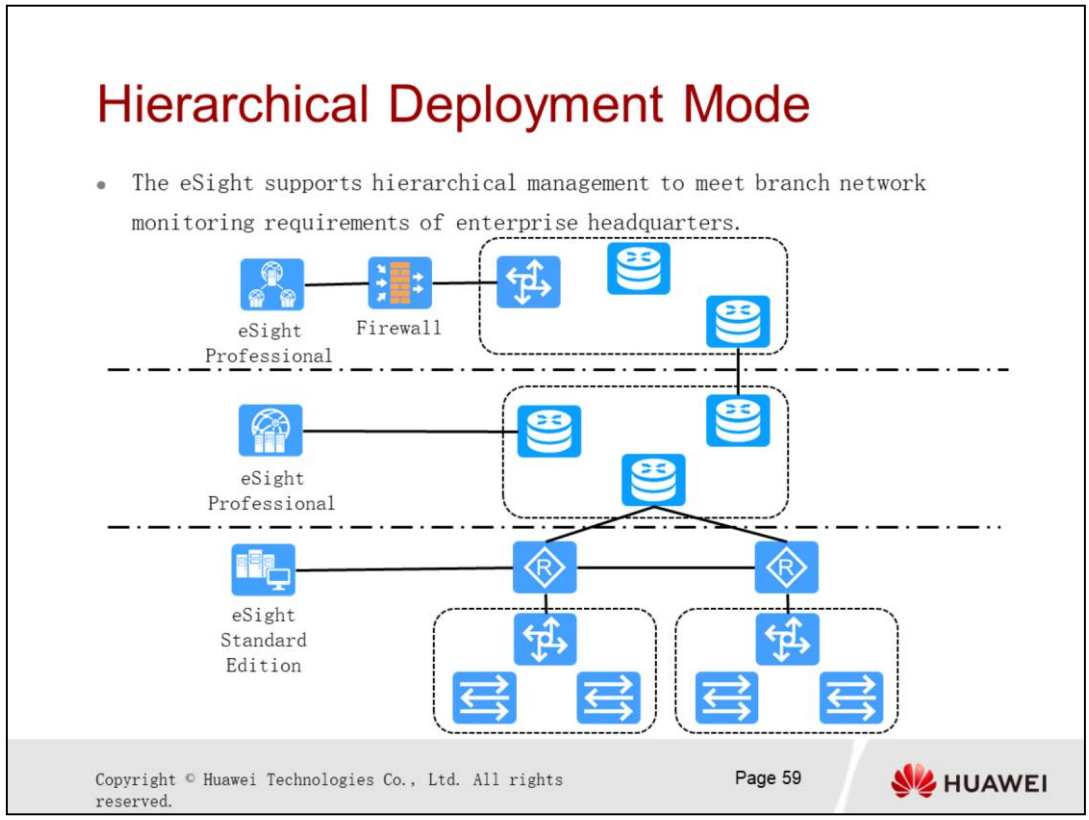
- After the uninstallation is complete, click **Finish** in the **Uninstall Completed** dialog box.
- In the displayed **Confirm** dialog box, click **Yes** to restart the operating system.

Contents

HUAWEI



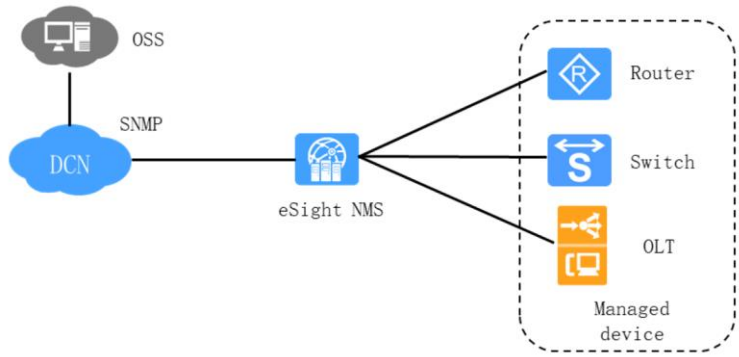
- The eSight deployment modes include single server deployment, hierarchical deployment, and integration with the OSS system.
- The eSight Infrastructure Management Maintenance Tool uses the browser/server (B/S) working mode..
  - The single-server system uses multiple web clients and a single server. Web clients and the eSight server are connected through a LAN or WAN.
  - After logging in to the eSight Infrastructure Management Maintenance Tool using a web browser on a PC, you can manage and maintain the infrastructure management system server.
  - The single-server system deployment solution applies to scenarios where the network scale is small and reliability requirements are not high.



- The eSight supports hierarchical management to meet branch network monitoring requirements of enterprise headquarters.
- In hierarchical deployment mode, a user can add lower-layer NMSs to the upper-layer NMS. The system provides links to the lower-layer NMSs. When a user clicks a lower-layer NMS link, a new browser window is displayed, showing the home page of the lower-layer NMS.

Integration with the OSS

- The eSight application platform can be integrated with the upper-layer OSS, report network alarms through SNMP, and interconnect with the OSS alarm system.

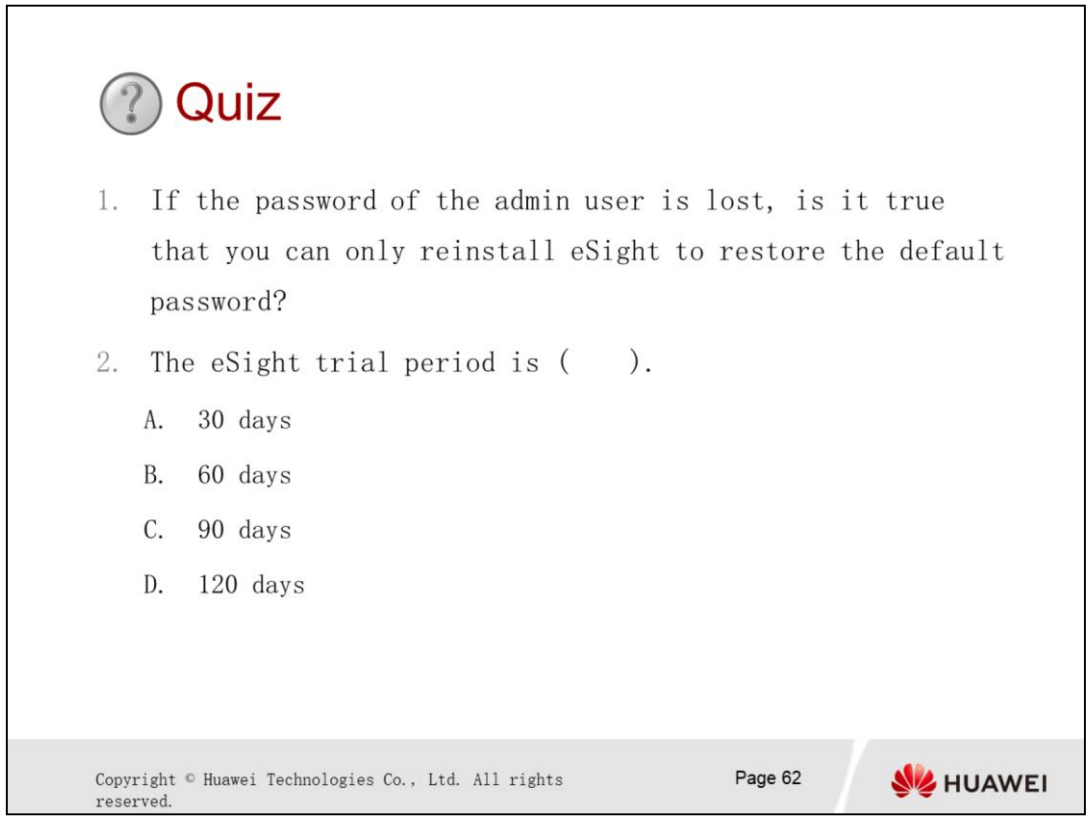


HUAWEI

- Operation support system (OSS) is the network management software running on the network management center workstation. Network administrators can operate the OSS to send requests to managed devices to monitor and configure network devices.
- The advantages of integration with the OSS are as follows:
  - Improve the network management capability through the OSS.
  - Separate NE management functions from the network management functions.
  - Meet the requirements of the enterprise O&M.

Summary

- Principles of the SNMP protocol
- eSight_PON network device management overview
- eSight installation and uninstallation



- Answers:
  - 1. Yes
  - 2. C

Thank You

www.huawei.com