Network Management and O&M



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. 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.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



Contents

[1 Network Management and O&M 1](#_Toc60149323)

[1.1 Foreword 1](#_Toc60149324)

[1.2 Objectives 1](#_Toc60149325)

[1.3 Basic Concepts of Network Management and O&M 1](#_Toc60149326)

[1.3.1 What Is Network Management and O&M? 1](#_Toc60149327)

[1.3.2 Basic Network Management Functions 2](#_Toc60149328)

[1.3.3 Network Management Modes 3](#_Toc60149329)

[1.4 Traditional Network Management 4](#_Toc60149330)

[1.4.1 Management Through the CLI or Web System 4](#_Toc60149331)

[1.4.2 SNMP-based Centralized Management 5](#_Toc60149332)

[1.4.3 Typical SNMP Architecture 6](#_Toc60149333)

[1.4.4 SNMP Message Exchange 7](#_Toc60149334)

[1.4.5 MIB 8](#_Toc60149335)

[1.4.6 Common MIB Objects 9](#_Toc60149336)

[1.4.7 SNMP Management Model 10](#_Toc60149337)

[1.4.8 SNMPv1 10](#_Toc60149338)

[1.4.9 SNMPv2c 11](#_Toc60149339)

[1.4.10 SNMPv3 11](#_Toc60149340)

[1.4.11 SNMP Summary 12](#_Toc60149341)

[1.4.12 Basic SNMP Configuration 12](#_Toc60149342)

[1.4.13 SNMP Configuration Example (Network Device Side) 14](#_Toc60149343)

[1.5 Network Management Based on Huawei iMaster NCE 14](#_Toc60149344)

[1.5.1 Transformation and Challenges of the Network Industry 14](#_Toc60149345)

[1.5.2 Huawei iMaster NCE 15](#_Toc60149346)

[1.5.3 NETCONF Overview 16](#_Toc60149347)

[1.5.4 Typical NETCONF Interaction 18](#_Toc60149348)

[1.5.5 YANG Language Overview 18](#_Toc60149349)

[1.5.6 YANG and XML 19](#_Toc60149350)

[1.5.7 Telemetry Overview 19](#_Toc60149351)

[1.6 Quiz 20](#_Toc60149352)

[1.7 Summary 21](#_Toc60149353)

# Network Management and O&M

## Foreword

The ever expanding network and increasing network devices present a significant challenge in managing networks effectively and providing high-quality network services.

There are many network management and O&M methods, of which this course describes some of the most common.

## Objectives

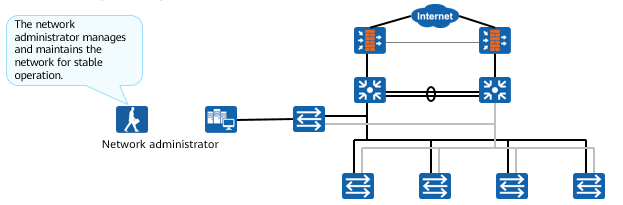
On completion of this course, you will be able to:

* Understand basic concepts of network management and O&M.
* Master common network management and O&M methods.
* Describe basic functions of network management and O&M.
* Understand the fundamentals of SNMP.
* Understand Huawei iMaster NCE and related technologies.

## Basic Concepts of Network Management and O&M

### What Is Network Management and O&M?

Network management and O&M plays an important role on a communications network. It ensures that devices work properly and the communications network runs properly to provide efficient, reliable, and secure communications services.



Common enterprise network architecture

Network management and O&M is classified as software management or hardware management.

* Software management: management of network applications, user accounts (such as accounts for using files), and read and write permissions. This course does not describe software management in detail.
* Hardware management: management of network elements (NEs) that constitute the network, including firewalls, switches, routers, and other devices. This course mainly describes hardware management.

Generally, an enterprise network has dedicated departments or personnel responsible for network management and O&M.

Note:

* A network element (NE) refers to a hardware device and software running on the hardware device. An NE has at least one main control board that manages and monitors the entire NE. The NE software runs on the main control board.

### Basic Network Management Functions

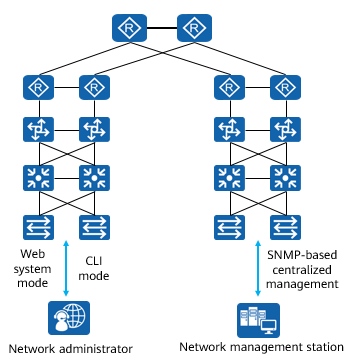


Basic Network Management Functions

OSI defines five functional models for network management:

* Configuration management: monitors network configuration information so that network administrators can generate, query, and modify hardware and software running parameters and conditions, and configure services.
* Performance management: manages network performance so that the network can provide reliable, continuous, and low-latency communication capabilities with as few network resources as possible.
* Fault management: ensures that the network is always available and rectifies faults as soon as possible.
* Security management: protects networks and systems from unauthorized access and attacks.
* Accounting management: records the network resource usage of users, charges users, and collects statistics on network resource usage.

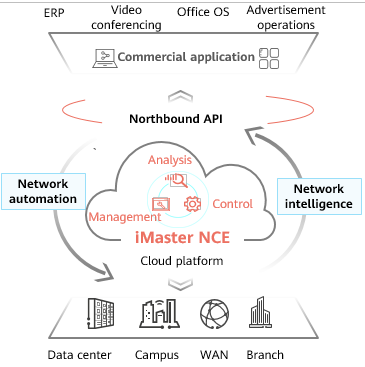
### Network Management Modes



Traditional Network Management and O&M

Traditional network management:

* Web system: The built-in web server of the device provides a graphical user interface (GUI). You need to log in to the device to be managed from a terminal through Hypertext Transfer Protocol Secure (HTTPS).
* CLI mode: You can log in to a device through the console port, Telnet, or SSH to manage and maintain the device. This mode provides refined device management but requires that users be familiar with command lines.
* SNMP-based centralized management: The Simple Network Management Protocol (SNMP) provides a method for managing NEs (such as routers and switches) by using a central computer (that is, a network management station) that runs network management software. This mode provides centralized and unified management of devices on the entire network, greatly improving management efficiency.



iMaster NCE-based Network Management and O&M

iMaster NCE-based network management:

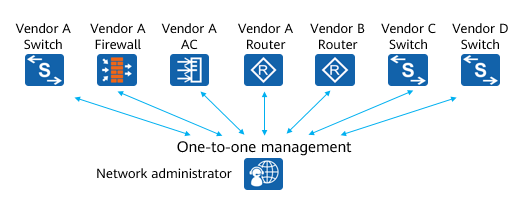
* iMaster NCE is a network automation and intelligence platform that integrates management, control, analysis, and AI functions. It provides four key capabilities: full-lifecycle automation, intelligent closed-loop management based on big data and AI, scenario-specific app ecosystem enabled by open programmability, and all-cloud platform with ultra-large system capacity.
* iMaster NCE uses protocols such as Network Configuration Protocol (NETCONF) and RESTCONF to deliver configurations to devices and uses telemetry to monitor network traffic.

## Traditional Network Management

### Management Through the CLI or Web System

When the network scale is small, the CLI and web system are generally used for network management.

* Network administrators can log in to a device through HTTPS, Telnet, or the console port to manage the device.
* These network management modes do not require any program or server to be installed on the network, and the cost is low.
* Network administrators must have a good master of network knowledge and vendor-specific network configuration commands.
* These modes have great limitations when the network scale is large and the network topology is complex.



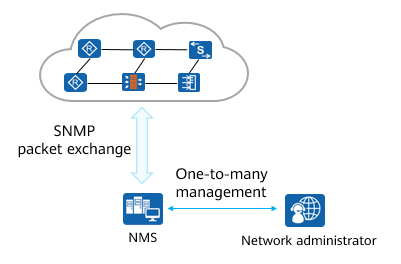
Management Through the CLI or Web System

As networks rapidly expand and applications become more diversified, network administrators face the following problems:

* The fast growth of network devices increases network administrators' workloads. In addition, networks' coverage areas are constantly being expanded, making real-time monitoring and fault locating of network devices difficult.
* There are various types of network devices and the management interfaces (such as command line interfaces) provided by different vendors vary from each other, making network management more complex.

### SNMP-based Centralized Management

SNMP is a standard network management protocol widely used on TCP/IP networks. It provides a method for managing NEs through a central computer that runs network management software, that is, a network management station.



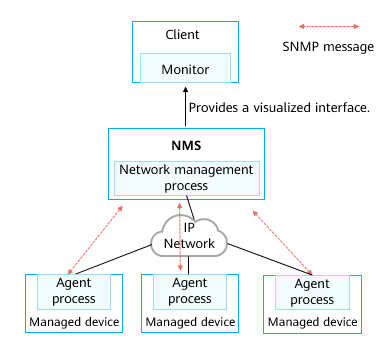
SNMP-based Centralized Management

* Network administrators can use the NMS to query information, modify information, and troubleshoot faults on any node on the network, improving work efficiency.
* Network devices of different types and vendors are managed in a unified manner.

There are three SNMP versions: SNMPv1, SNMPv2c, and SNMPv3.

* In May 1990, RFC 1157 defined the first SNMP version: SNMPv1. RFC 1157 provides a systematic method for monitoring and managing networks. SNMPv1 implements community name-based authentication, failing to provide high security. In addition, only a few error codes are returned in SNMPv1 packets.
* In 1996, the Internet Engineering Task Force (IETF) released RFC 1901 in which SNMPv2c is defined. SNMPv2c provides enhancements to standard error codes, data types (Counter 64 and Counter 32), and operations including GetBulk and Inform.
* SNMPv2c still lacks security protection measures, so IETF released SNMPv3. SNMPv3 provides user security module (USM)-based encryption and authentication and a view-based access control model (VACM).

### Typical SNMP Architecture



Typical SNMP Architecture

On a network where SNMP is used for network management, a network management system (NMS) functions as a network management center and runs management processes. Each managed device needs to run an agent process. The management process and agent process communicate with each other through SNMP messages.

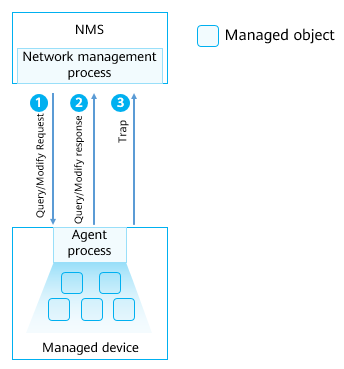
An NMS is a system that uses SNMP to manage and monitor network devices. The NMS software runs on NMS servers.

Managed devices are devices that are managed by the NMS on the network.

The agent process runs on managed devices to maintain the information data of the managed devices, respond to the request from the NMS, and report the management data to the NMS that sends the request.

An NMS is an independent device that runs network management programs. The network management programs provide at least one man-machine interface for network administrators to perform network management operations. Web page interaction is a common man-machine interaction mode. That is, a network administrator uses a terminal with a monitor to access the web page provided by the NMS through HTTP/HTTPS.

### SNMP Message Exchange



SNMP Message Exchange

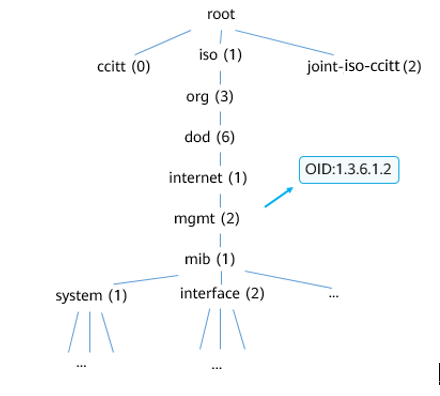
The NMS and managed devices exchange messages in the following modes:

* The NMS sends a request for modifying or querying configuration information to a managed device through SNMP. The agent process running on the managed device responds to the request from the NMS.
* The managed device can proactively report traps to the NMS so that the network administrator can detect faults in a timely manner.

Managed object: Each device may contain multiple managed objects. A managed object can be a hardware component or a set of parameters configured on the hardware or software (such as a routing protocol).

SNMP uses management information bases (MIBs) to describe a group of objects of a manageable entity.

### MIB



MIB

A MIB is a database containing the variables that are maintained by managed devices. (The variables can be queried or set by the agent processes.) The MIB defines the attributes of managed devices in the database.

* Object identifier (OID) of an object
* Status of an object
* Access permission of an object
* Data types of an object

A MIB provides a structure that contains data on all NEs that may be managed on the network. Because the data structure is similar to the tree structure, a MIB is also called an object naming tree.

MIB is defined independently of a network management protocol. Device vendors can integrate SNMP agent software into their products (for example, routers), but they must ensure that this software complies with relevant standards after new MIBs are defined. You can use the same network management software to manage routers containing MIBs of different versions. However, the network management software cannot manage a router that does not support the MIB function.

There are public MIBs and private MIBs.

* Public MIBs: defined by RFCs and used for structure design of public protocols and standardization of interfaces. Most vendors need to provide SNMP interfaces according to the specifications defined in RFCs.
* Private MIBs: They are the supplement of the public MIBs. Some enterprises need to develop private protocols or special functions. The private MIBs are designed to enable the SNMP interface to manage such protocols or functions. They also help the NMS provided by the third party to manage devices. For example, the MIB object of Huawei is 1.3.6.1.4.1.2011.

### Common MIB Objects

Objects used for query or modification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OID | Object Name | Data Type | Maximum Access | Description |
| 1.3.6.1.2.1.2.1 | ifNumber | Integer | read-only | Number of network interfaces in the system (regardless of the current interface status) |
| 1.3.6.1.4.1.2011.5.25.41.1.2.1.1.3 | hwIpAdEntNetMask | IpAddress | read-create | Subnet mask of an IP address |

Objects used for alarm notification

|  |  |  |  |
| --- | --- | --- | --- |
| OID | Object Name | Bound Variable | Description |
| 3.6.1.6.3.1.1.5.3 | linkDown | ifIndex  ifAdminStatus  ifOperStatus  ifDesc | It is detected that one of the communication links in the ifOperStatus object has entered the down state from another state (but not the notPresent state). The original state is indicated by the value of ifOperStatus. |

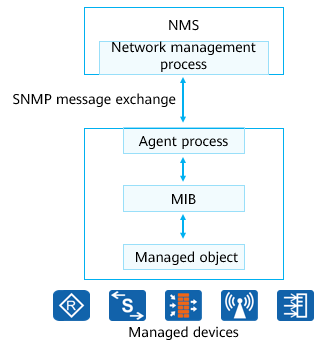
The maximum access permission of a MIB object indicates the operations that the NMS can perform on the device through the MIB object.

* not-accessible: No operation can be performed.
* read-only: reads information.
* read-write: reads information and modifies configurations.
* read-create: reads information, modifies configurations, adds configurations, and deletes configurations.

When generating a trap, the device reports the type of the current trap together with some variables. For example, when sending a linkDown trap, the device also sends variables such as the interface index and current configuration status of the involved interface.

* ifIndex: interface index (number)
* ifAdminStatus: indicates the administrative status, that is, whether the interface is shut down. 1 indicates that the interface is not shut down, and 2 indicates that the interface is shut down.
* ifOperStasuts: indicates the current operating status of the interface, that is, the link layer protocol status of the interface. The value 1 indicates Up, 2 indicates Down.
* ifDesc: interface description

### SNMP Management Model



SNMP Management Model

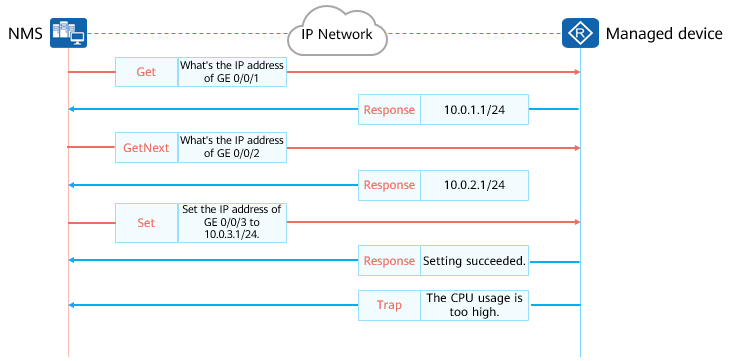
Query/Modify operation:

* The NMS sends an SNMP request message to an agent process.
* The agent process searches the MIB on the device for information to be queried or modified and sends an SNMP response message to the NMS.

Trap operation:

* If the trap triggering conditions defined for a module are met, the agent process sends a message to notify the NMS that an event or trap has occurred on a managed object. This helps network administrators promptly process network faults.

### SNMPv1

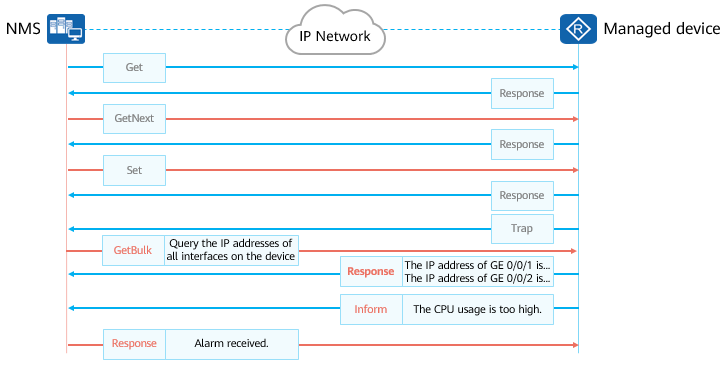


SNMPv1

SNMPv1 defines five protocol operations.

* Get-Request: The NMS extracts one or more parameter values from the MIB of the agent process on the managed device.
* Get-Next-Request: The NMS obtains the next parameter value from the MIB of the agent process in lexicographical order.
* Set-Request: The NMS sets one or more parameter values in the MIB of the agent process.
* Response: The agent process returns one or more parameter values. It is the response to the first three operations.
* Trap: The agent process sends messages to the NMS to notify the NMS of critical or major events.

### SNMPv2c



SNMPv2c

SNMPv2c supports the following operations:

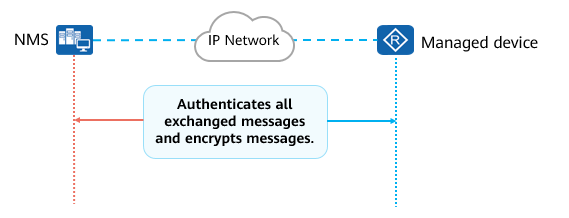
* GetBulk: equals to multiple GetNext operations. You can set the number of GetNext operations to be included in one GetBulk operation.
* Inform: A managed device proactively sends traps to the NMS. In contrast to the trap operation, the inform operation requires an acknowledgement. After a managed device sends an InformRequest message to the NMS, the NMS returns an InformResponse message. If the managed device does not receive the acknowledgment message, it temporarily saves the trap in the Inform buffer and resends the trap until the NMS receives the trap or the number of retransmission times reaches the maximum.

### SNMPv3

SNMPv3 has the same working mechanism as SNMPv1 and SNMPv2c, but adds header data and security parameters.

SNMPv3 messages can be authenticated and encrypted.

SNMPv3 is applicable to networks of various scales and has high security.



SNMPv3

SNMPv3 supports identity authentication and encryption.

* Identity authentication: A process in which the agent process (or NMS) confirms whether the received message is from an authorized NMS (or agent process) and whether the message is changed during transmission.
* Encryption: The header data and security parameter fields are added to SNMPv3 messages. For example, when the management process sends an SNMPv3 Get-Request message carrying security parameters such as the username, key, and encryption parameters, the agent process also uses an encrypted response message to respond to the Get-Request message. This security encryption mechanism is especially applicable to a scenario in which data needs to be transmitted through a public network between the management process and agent process.

### SNMP Summary

SNMP has the following advantages:

* Simplicity: SNMP is applicable to networks that require high speed and low cost because it uses a polling mechanism and provides basic network management functions. Moreover, SNMP uses UDP to exchange data and therefore is supported by most products.
* Convenience: SNMP allows management information exchange between arbitrary devices on a network, so that a network administrator can query information and locate faults on any device.

SNMPv1 applies to small-scale networks where security requirements are not high or the network environment is safe and stable, such as campus networks and small-sized enterprise networks.

SNMPv2c applies to medium- and large-sized networks where security requirements are not high or the network environment is safe, but a large volume of traffic exists and traffic congestion may occur.

SNMPv3 is the recommended version and applies to networks of various scales, especially those networks that have high security requirements and allow only authorized administrators to manage network devices.

### Basic SNMP Configuration

Enable the SNMP agent function.

[Huawei] **snmp-agent**

Set the SNMP version.

[Huawei] **snmp-agent sys-info version [v1 | v2c | v3]**

You can configure the SNMP version as required. However, the protocol version used on the device must be the same as that used on the NMS.

Create or update MIB view information.

[Huawei] **snmp-agent mib-view** *view-name* { **exclude** | **include** } *subtree-name* [**mask** *mask*]

Add a new SNMP group and map users in this group to the SNMP view.

[Huawei] **snmp-agent group v3** *group-name* **{ authentication | noauth | privacy } [ read-view** *view-name* | **write-view** *view-name* **| notify-view** *view-name* ]

This command is used to create an SNMP group of the SNMPv3 version and specify the authentication and encryption mode and one or more of read-only view, read-write view, and notification view. It is a mandatory command on networks that require high security.

Add a user to the SNMP group.

[Huawei] **snmp-agent usm-user v3** *user-name* **group** *group-name*

Configure an authentication password for an SNMPv3 user.

[Huawei] **snmp-agent usm-user v3** *user-name*  **authentication-mode { md5 | sha | sha2-256 }**

Configure the SNMPv3 user encryption password.

[Huawei] **snmp-agent usm-user v3** *user-name* **privacy-mode { aes128 | des56 }**

Set parameters for the device to send traps.

[Huawei] **snmp-agent target-host trap-paramsname** *paramsname* **v3 securityname** *securityname* **{ authentication | noauthnopriv | privacy }**

Configure the target host of traps.

[Huawei] **snmp-agent target-host trap-hostname** *hostname* **address** *ipv4-address* **trap-paramsname** *paramsname*

Enable all trap functions.

[Huawei] **snmp-agent trap enable**

Note that this command is used only to enable the device to send traps. This command must be used together with the **snmp-agent target-host** command. The **snmp-agent target-host** command specifies the device to which traps are sent.

Configure the source interface that sends traps.

[Huawei] **snmp-agent trap source** *interface-type* *interface-number*

Note that a source IP address must have been configured for the interface that sends traps.

### SNMP Configuration Example (Network Device Side)



SNMP Configuration Example (Network Device Side)

Enable SNMP on R1and set the SNMP version to SNMPv3.

Set the SNMPv3 group name to test and encryption authentication mode to privacy.

Create an SNMPv3 user named R1 and set the authentication and encryption passwords to HCIA-Datacom123.

Create a trap parameter named param and set securityname to sec.

Set the IP address of the SNMP target host to 192.168.1.10.

Enable the trap function and specify GE 0/0/1 as the source interface that sends traps.

R1configuration:

[R1]snmp-agent

[R1]snmp-agent sys-info version v3

[R1]snmp-agent group v3 test privacy

[R1]snmp-agent usm-user v3 R1 test authentication-mode md5 HCIA@Datacom123 privacy-mode aes128 HCIA-Datacom123

[R1]snmp-agent target-host trap-paramsname param v3 securityname sec privacy

[R1]snmp-agent target-host trap-hostname nms address 192.168.1.10 trap-paramsname param

[R1]snmp-agent trap source GigabitEthernet 0/0/1

[R1]snmp-agent trap enable

Info: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y

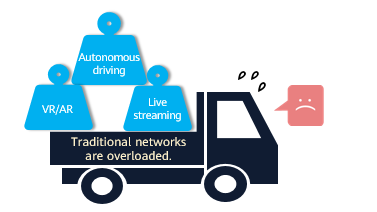
## Network Management Based on Huawei iMaster NCE

### Transformation and Challenges of the Network Industry

With the advent of the 5G and cloud era, innovative services such as VR/AR, live streaming, and autonomous driving are emerging, and the entire ICT industry is booming. At the same time, the traffic of the entire network also increases explosively. Huawei Global Industry Vision (GIV) predicts that the amount of new data will reach 180 ZB by 2025. Moreover, the dynamic complexity of services makes the entire network more complex.

Such challenges can only be overcome by constructing automated and intelligent network systems centered on user experience.

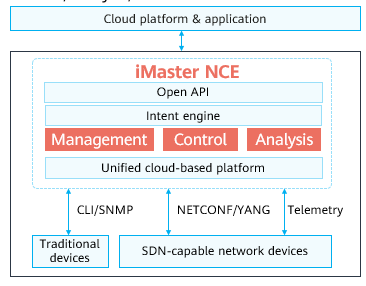
* One zettabyte (abbreviated "ZB") is equal to 1012 GB.



Transformation and Challenges of the Network Industry

### Huawei iMaster NCE

Huawei iMaster NCE is a network automation and intelligence platform that integrates management, control, analysis, and AI functions.



Huawei iMaster NCE

In terms of management and control, iMaster NCE allows you to:

* Manage and control traditional devices through traditional technologies such as CLI and SNMP.
* Manage and control SDN-capable networks through NETCONF (based on the YANG model).

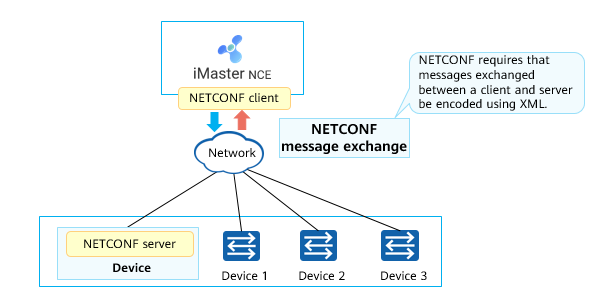
iMaster NCE collects network data through protocols such as SNMP and telemetry, performs intelligent big data analysis based on AI algorithms, and displays device and network status in multiple dimensions through dashboards and reports, helping O&M personnel quickly detect and handle device and network exceptions and ensuring normal running of devices and networks.

iMaster NCE provides the following key capabilities:

* Full-lifecycle automation: iMaster NCE provides full-lifecycle automation across multiple network technologies and domains based on unified resource modeling and data sharing, enabling device plug-and-play, immediate network availability after migration, on-demand service provisioning, fault self-healing, and risk warning.
* Intelligent closed-loop management based on big data and AI: iMaster NCE constructs a complete intelligent closed-loop system based on its intent engine, automation engine, analytics engine, and intelligence engine. It also uses telemetry to collect and aggregate massive volumes of network data. This allows it to determine the network status in real time. iMaster NCE provides big data-based global network analysis and insights through unified data modeling, and is equipped with Huawei's sophisticated AI algorithms accumulated during its 30 years in the telecom industry. It provides automated closed-loop analysis, forecast, and decision-making based on customers' intents. This helps improve user experience and continuously enhance network intelligence.
* Open programmability-enabled scenario-based application ecosystem: In the southbound direction, iMaster NCE provides a programmable integrated development environment — Design Studio — and a developer community for integration with third-party network controllers and devices; in the northbound direction, it provides cloud-based AI training platforms and IT applications. iMaster NCE allows customers to purchase Huawei native apps on demand, develop their own apps, and turn to third-party system integrators for app development.
* Large-capacity cloud platform: iMaster NCE, with cloud-native architecture, supports both on-premises deployment and cloud-based deployment. With elastic scalability, it can provide large system capacity to allow a large number of access users. With online data sharing and process streamlining, it avoids scattered data distribution and multi-level O&M in offline mode.

### NETCONF Overview

NETCONF provides a network device management mechanism. You can use NETCONF to add, modify, or delete configurations of network devices, and obtain configurations and status of network devices.



NETCONF Overview

NETCONF has three objects:

* NETCONF client
* NETCONF server
* NETCONF message

NETCONF client: manages network devices using NETCONF. Generally, the NMS functions as the NETCONF client. It sends <rpc> elements to a NETCONF server to query or modify configuration data. The client can learn the status of a managed device based on the traps and events reported by the server.

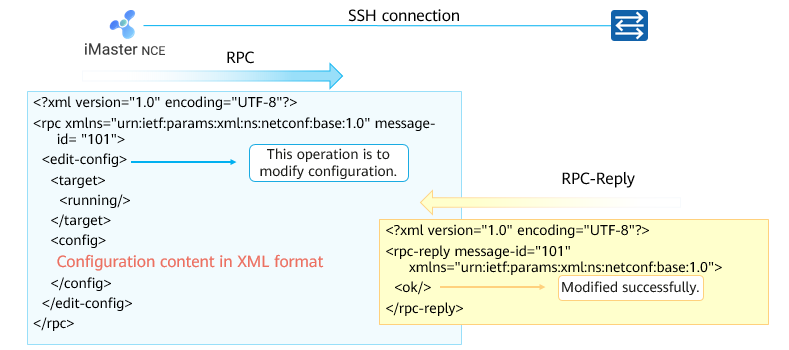
NETCONF server: maintains information about managed devices, responds to requests from clients, and reports management data to the clients. NETCONF servers are typically network devices, for example, switches and routers. After receiving a request from a client, a server parses data, processes the request with the assistance of the Configuration Manager Frame (CMF), and then returns a response to the client. If a trap is generated or an event occurs on a managed device, the NETCONF server reports the trap or event to the client through the Notification mechanism, so the client can learn the status change of the managed device.

A client and a server establish a connection based on a secure transmission protocol such as Secure Shell (SSH) or Transport Layer Security (TLS), and establish a NETCONF session after exchanging capabilities supported by the two parties using Hello packets. In this way, the client and the server can exchange messages. A network device must support at least one NETCONF session. The data that a NETCONF client obtains from a NETCONF server can be configuration data or status data.

NETCONF Advantages

|  |  |  |  |
| --- | --- | --- | --- |
| Function | NETCONF | SNMP | CLI |
| Interface type | Machine-machine interface: The interface definition is complete and standard, and the interface is easy to control and use. | Machine-to-machine interface | Man-machine interface |
| Operation efficiency | High: Object-based modeling is supported. Only one interaction is required for object operations. Operations such as filtering and batch processing are supported. | Medium | Low |
| Scalability | Proprietary protocol capabilities can be extended. | Weak | Moderate |
| Transaction | Supports transaction processing mechanisms such as trial running, rollback upon errors, and configuration rollback. | Not supported | Partially supported |
| Secure transmission | Multiple security protocols: SSH, TLS, BEEP/TLS, and SOAP/HTTP/TLS | Only SNMPv3 supports secure transmission. | SSH |

### Typical NETCONF Interaction



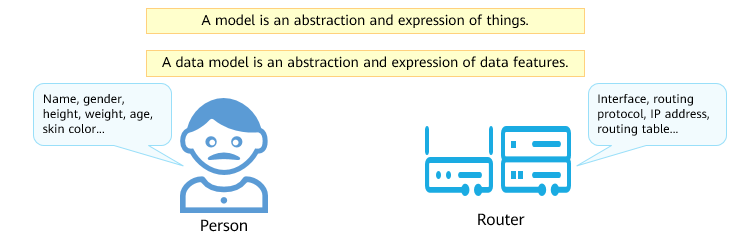
Typical NETCONF Interaction

NETCONF uses SSH to implement secure transmission and uses Remote Procedure Call (RPC) to implement communication between the client and server.

### YANG Language Overview

Yet Another Next Generation (YANG) is a data modeling language that standardizes NETCONF data content.

The YANG model defines the hierarchical structure of data and can be used for NETCONF-based operations. Modeling objects include configuration, status data, remote procedure calls, and notifications. This allows a complete description of all data exchanged between a NETCONF client and server.



YANG Language Overview

YANG originates from NETCONF but is not only used for NETCONF. Although the YANG modeling language is unified, YANG files are not unified.

YANG files can be classified into the following types:

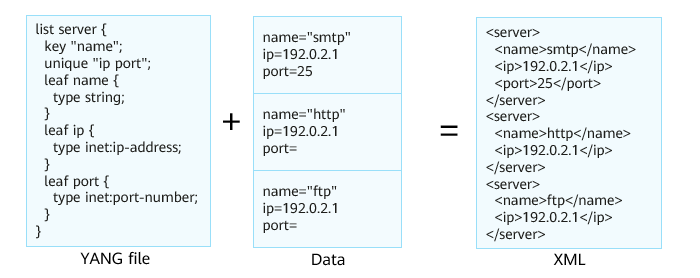
* Vendor's proprietary YANG file
* IETF standard YANG
* OpenConfig YANG

The YANG model is presented as a .yang file.

The YANG model has the following characteristics:

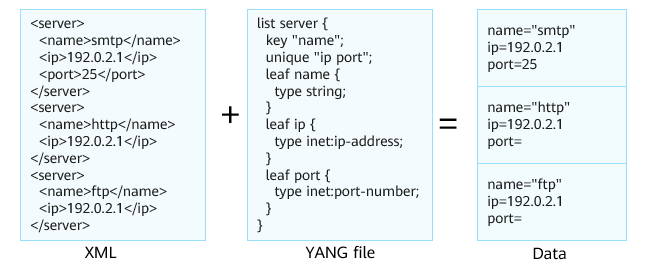
* Hierarchical tree-like structure modeling.
* Data models are presented as modules and sub-modules.
* It can be converted to the YANG Independent Notation (YIN) model based on the XML syntax without any loss.
* Defines built-in data types and extensible types.

### YANG and XML



YANG and XML (1)

* A YANG file is loaded on the NETCONF client (such as the NMS or SDN controller).
* The YANG file is used to convert data into XML-format NETCONF messages before they are sent to the device.



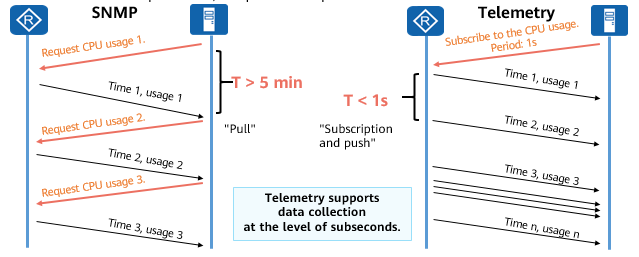
YANG and XML (2)

* A YANG file is loaded on the NETCONF server (such as a router or switch).
* The YANG file is used to convert received XML-format NETCONF messages into data for subsequent processing.

### Telemetry Overview

Telemetry, also called network telemetry, is a technology that remotely collects data from physical or virtual devices at a high speed.

Devices periodically send interface traffic statistics, CPU usage, and memory usage to collectors in push mode. Compared with the traditional pull mode, the push mode provides faster and more real-time data collection.



Telemetry Overview

There is also a view in the industry that SNMP is considered as a traditional telemetry technology, and the current telemetry is referred to as streaming telemetry or model-driven telemetry.

Telemetry packs the data to be sent, improving transmission efficiency.

## Quiz

1. (Single) Which of the following operations is used by the managed device to report alarms in SNMPv1? ( )
2. Get
3. Set
4. Inform
5. Trap
6. (Single) On an SNMP-based network, what is used to indicate information that can be queried and set by the agent process? ( )
7. NMS
8. Agent process
9. MIB
10. Managed devices
11. (Multiple) Which of the following are key capabilities of NCE? ( )
12. Full-lifecycle automation
13. Intelligent closed-loop based on big data and AI
14. Open Programmable Enables Scenario-based App Ecosystem
15. Large-capacity full-cloud platform
16. (True or false) SNMPv3 has the same working mechanism as SNMPv1 and SNMPv2c, but adds header data and security parameters. ( )
17. True
18. False
19. (True or false) YANG is a data modeling language that standardizes NETCONF data content. ( )
20. True
21. False
22. (Single) In SNMPv1, which of the following operations is used by a managed device to report traps? ( )
23. Get-Request
24. Set-Request
25. Trap
26. Response

## Summary

With the development of network technologies, more and more network management and O&M methods are available. The common methods are as follows:

* CLI mode or web system
* SNMP
* Huawei iMaster NCE's intelligent O&M platform (covering management, control, and analysis)