Fondamenti di Internet

Network Management and O&M

Prof. Gianluca Reali

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.

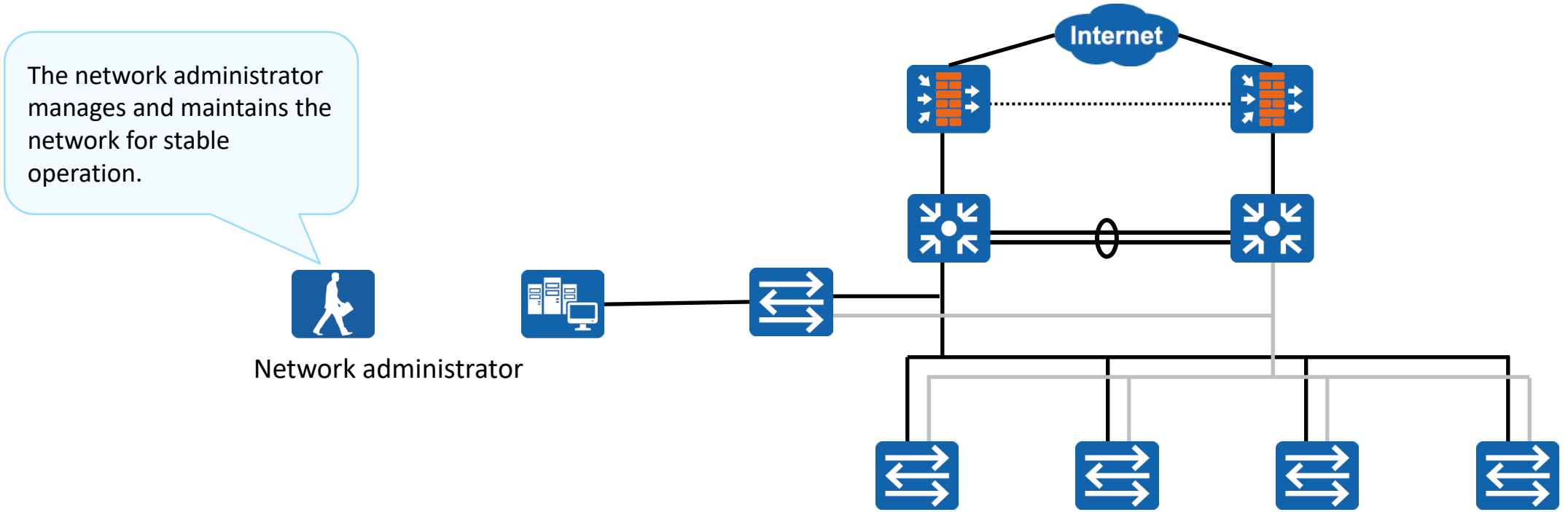
Objectives

- 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.

Contents

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

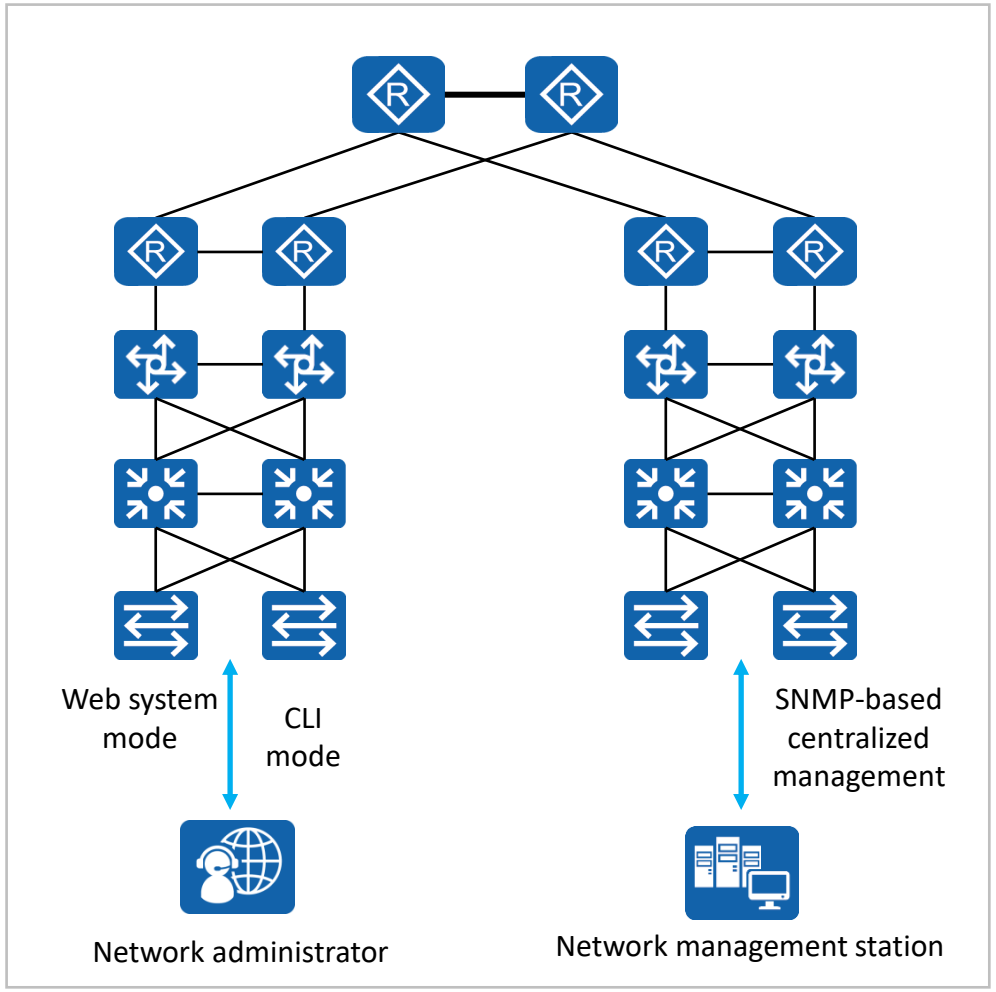
Basic Network Management Functions

OSI defines five functional models for network management:

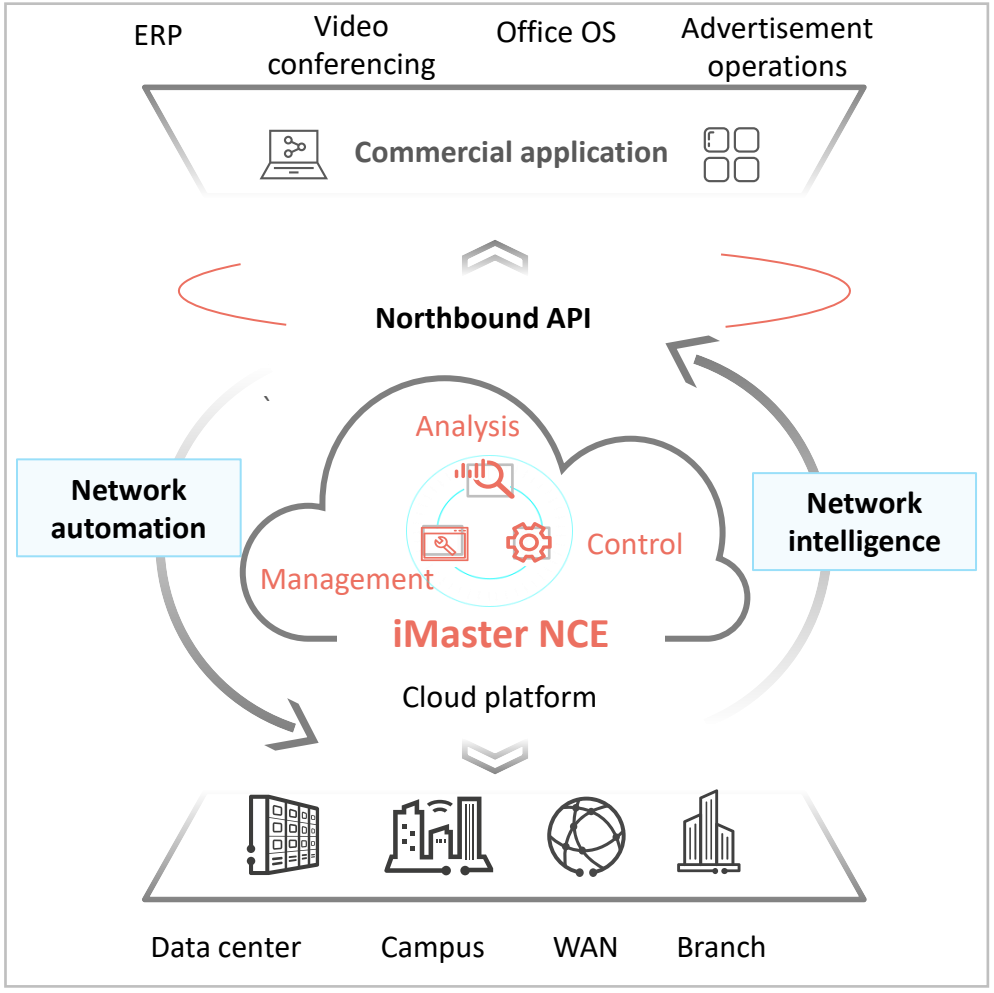
- Configuration management: monitors network configuration information so that network administrators can generate, query, and modify hardware and software running **parameters and conditions**, and **configure services**.
- Performance management: manages **network performance** so that the network 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



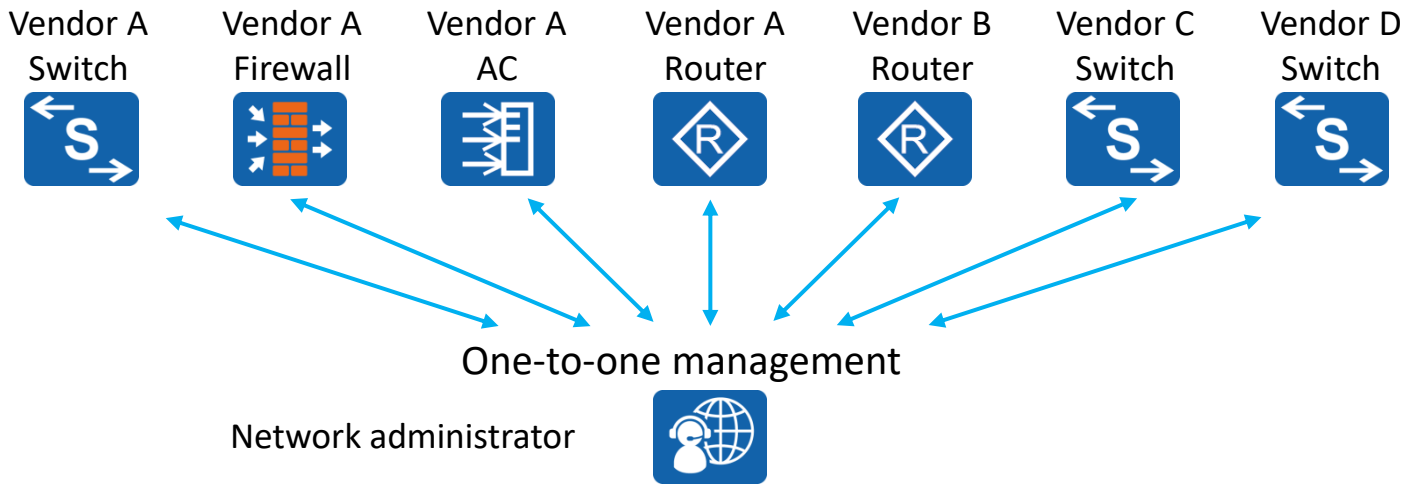
iMaster NCE-based Network Management and O&M



Contents

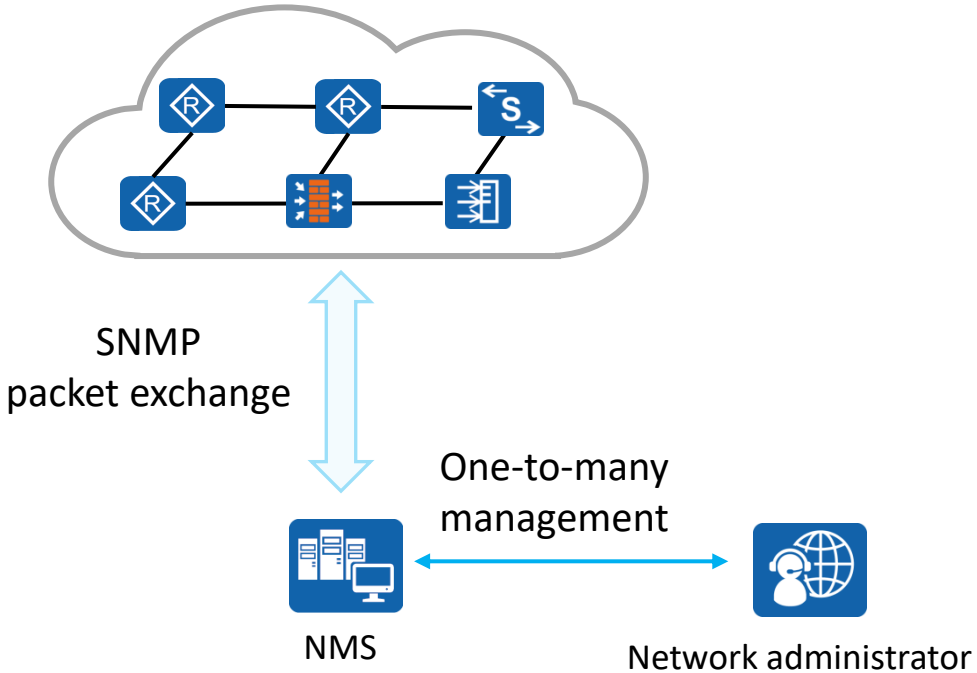
Management Through the CLI or Web System

- 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.



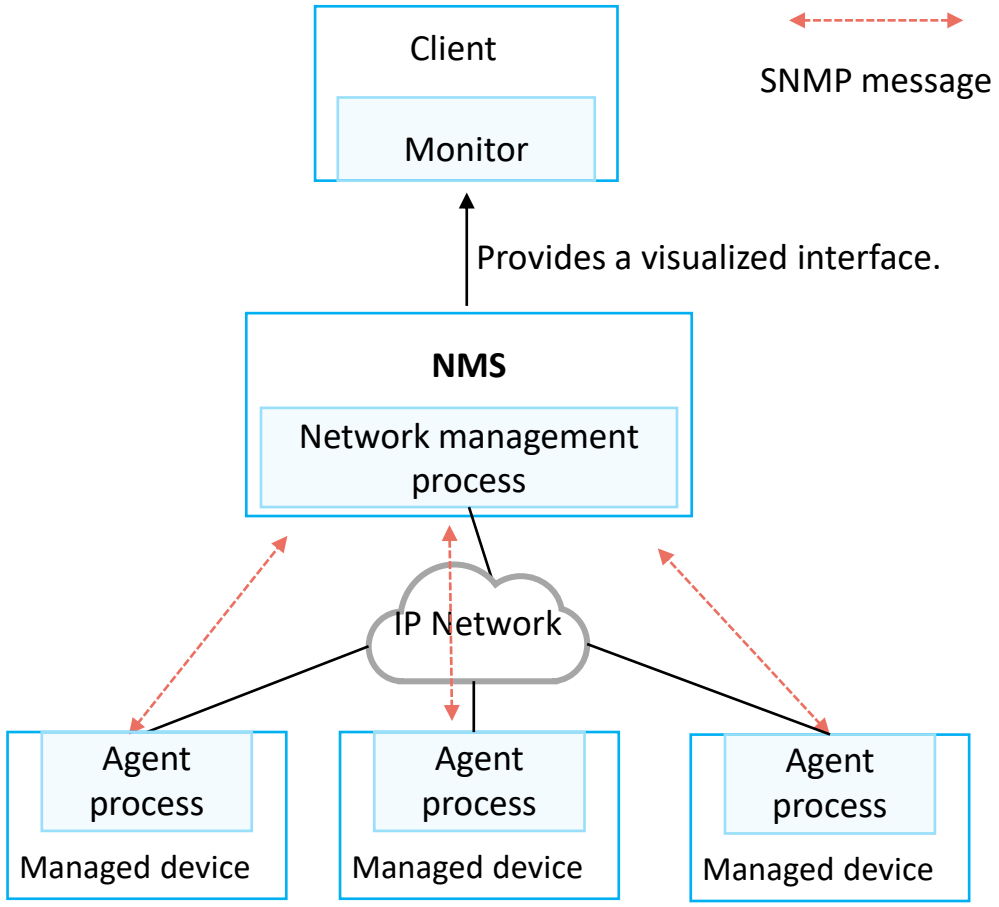
SNMP-based Centralized Management

- 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**.



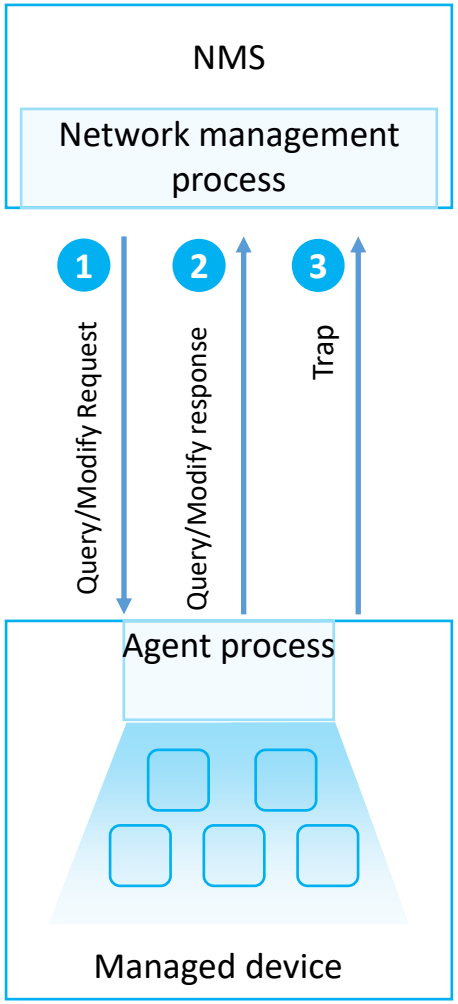
- Network administrators can use the NMS to **query** information, **modify** information, and **troubleshoot** faults on any node on the network, improving work efficiency.
- Network devices of different types and vendors are managed in a unified manner.
- SNMPv1, SNMPv2c, and SNMPv3

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.

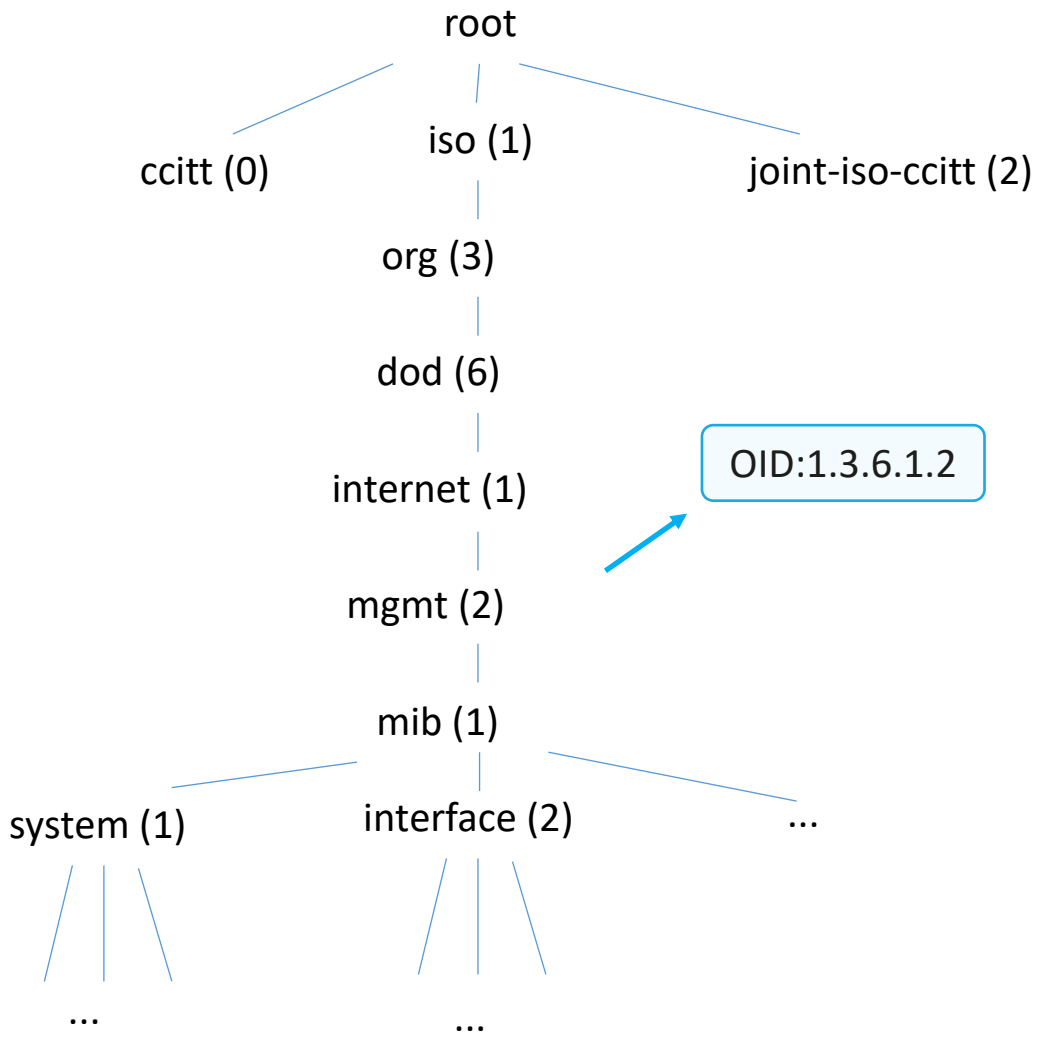
SNMP Message Exchange



Managed object

- 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



- 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.

Common MIB Objects

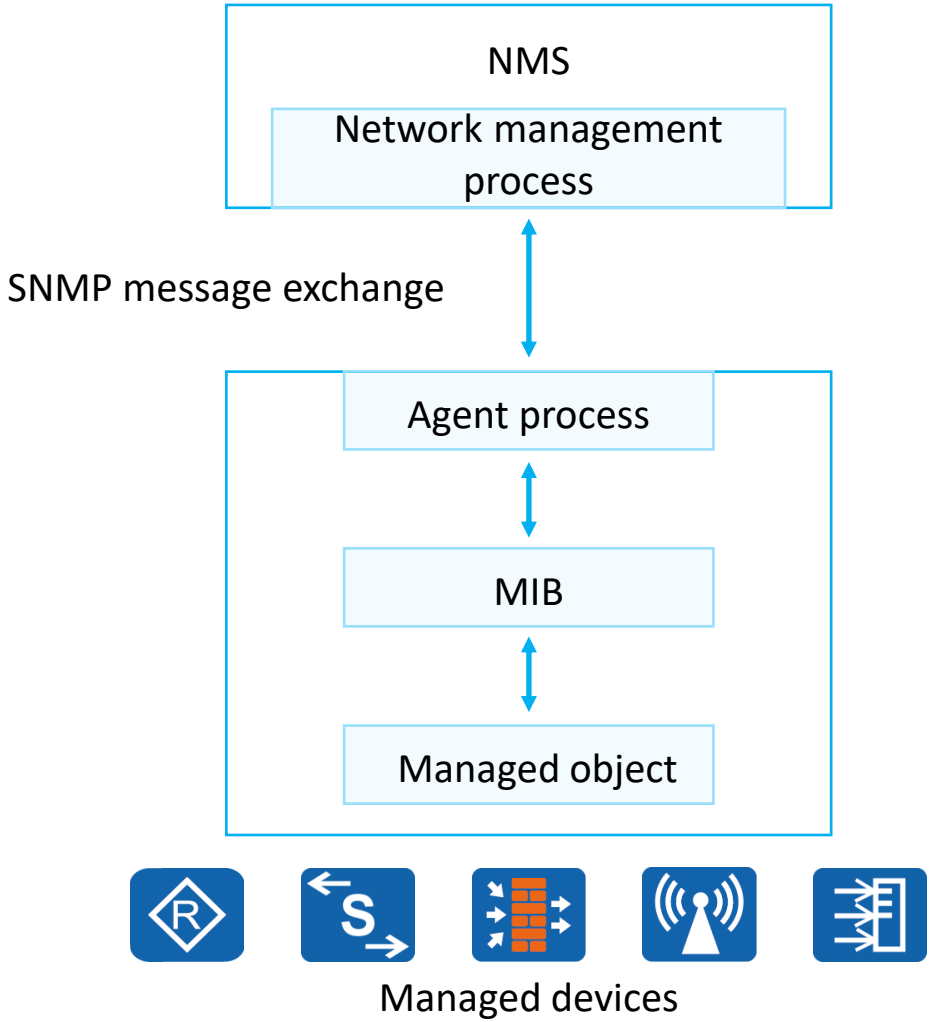
- Objects used for query or modification:

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:

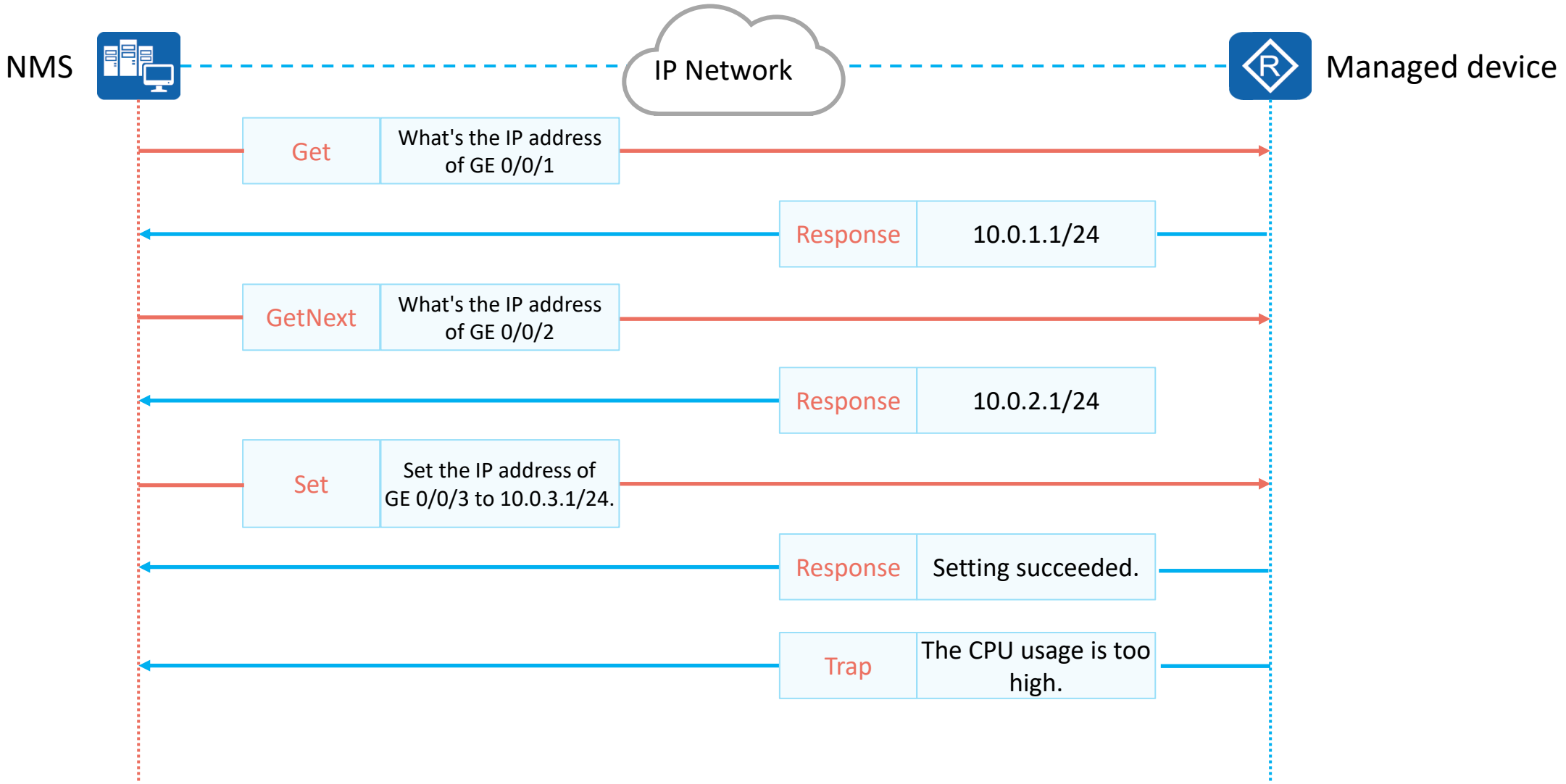
OID	Object Name	Bound Variable	Description
3.6.1.6.3.1.1.5.3	linkDown	ifIndex ifAdminStatus ifOperStatus ifDesc	It is detected that one of the communication links in the ifOperStatus object has entered the down state from another state (but not the notPresent state). The original state is indicated by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

SNMP Management Model

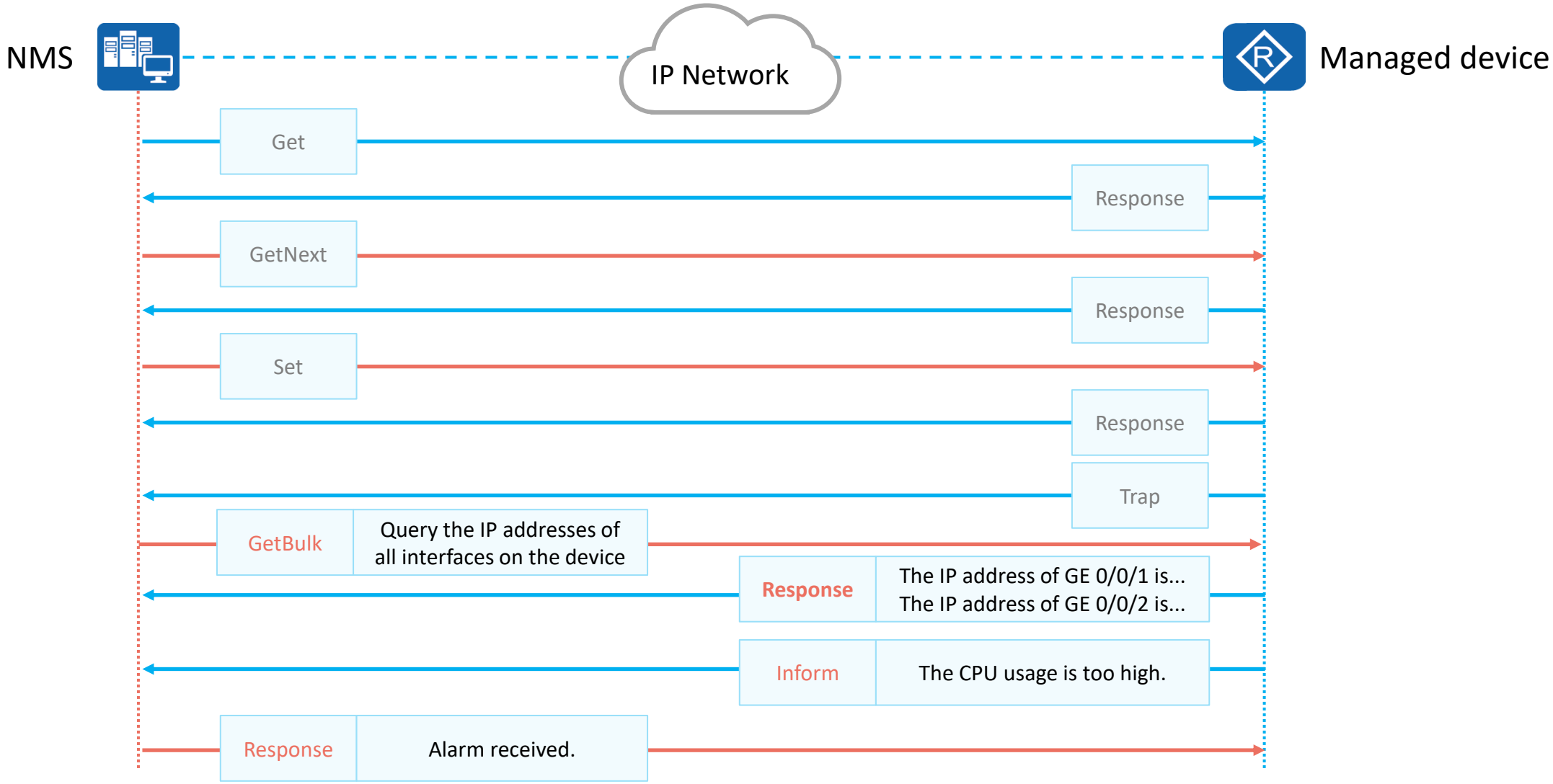


- Query/Modify operation:
  - The NMS sends an SNMP request message to an agent process.
  - The agent process searches the MIB on the device for information to be queried or modified and sends an SNMP response message to the NMS.
- Trap operation:
  - If the trap triggering conditions defined for a 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

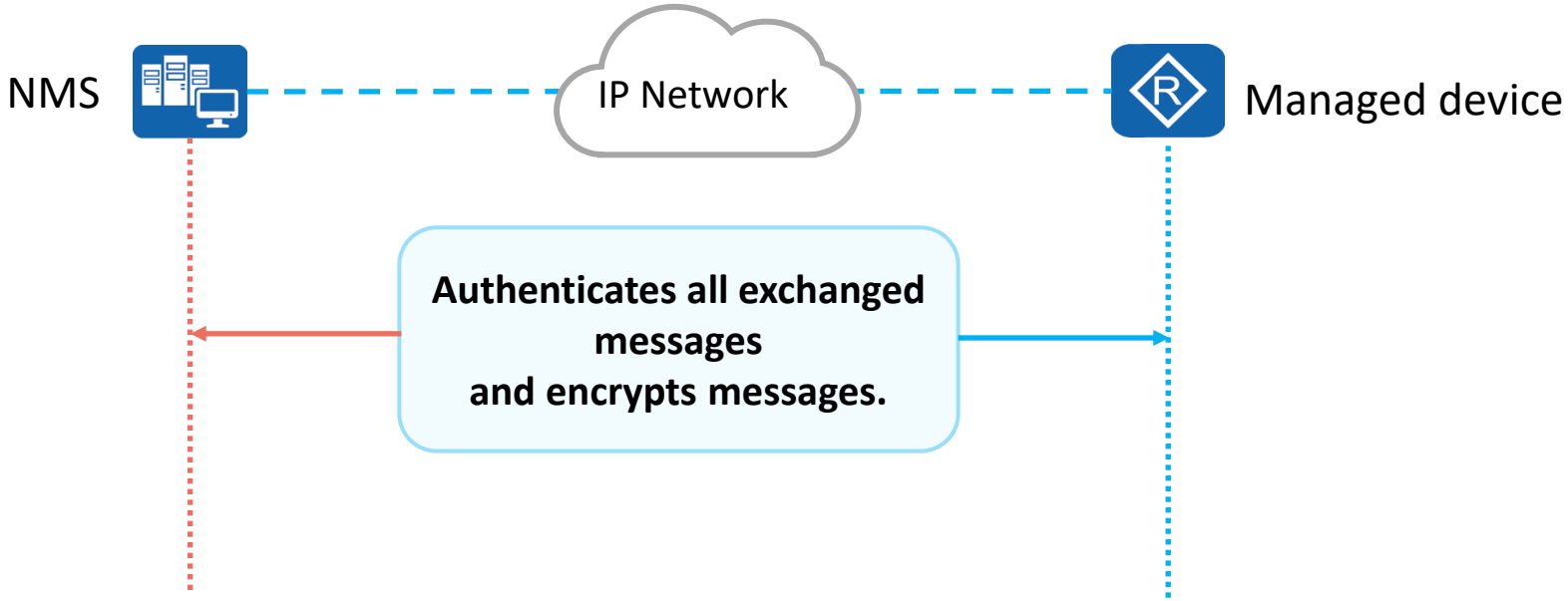


SNMPv2c



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.



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 (1)

1. Enable the SNMP agent function.

   [Huawei] **snmp-agent**

2. 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.

3. Create or update MIB view information.

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

4. 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.

Basic SNMP Configuration (2)

5. Add a user to the SNMP group.

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

6. Configure an authentication mode for an SNMPv3 user.

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

7. Configure the SNMPv3 user encryption mode.

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

8. Set parameters for sending trap messages.

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

Basic SNMP Configuration (3)

9. Configure the target host of traps.

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

10. Enable all trap functions.

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

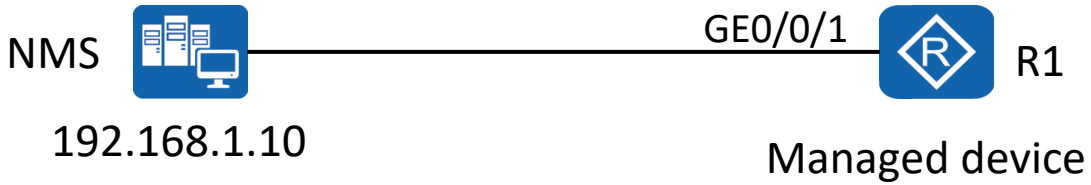
Note that this command is used only to enable the device to send traps. This command must be used together with the **snmp-agent target-host** command. The **snmp-agent target-host** command specifies the device to which traps are sent.

11. 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)



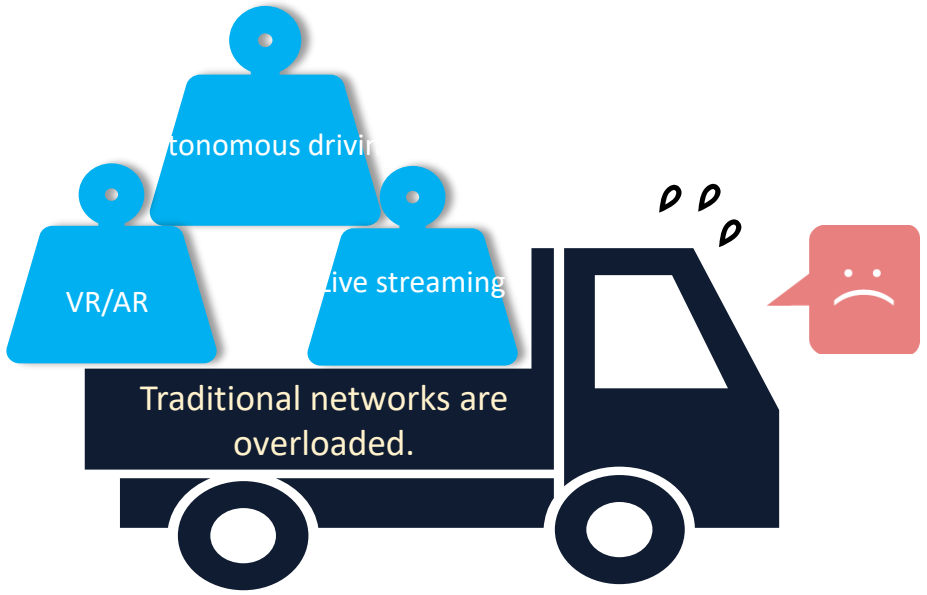
- Enable SNMP on R1and set the SNMP version to SNMPv3.
- Set the SNMPv3 group name to **test** and encryption authentication mode to **privacy**.
- Create an SNMPv3 user named **R1** and set the authentication and encryption passwords to **HCIA-Datacom123**.
- Create a trap parameter named **param** 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

Contents

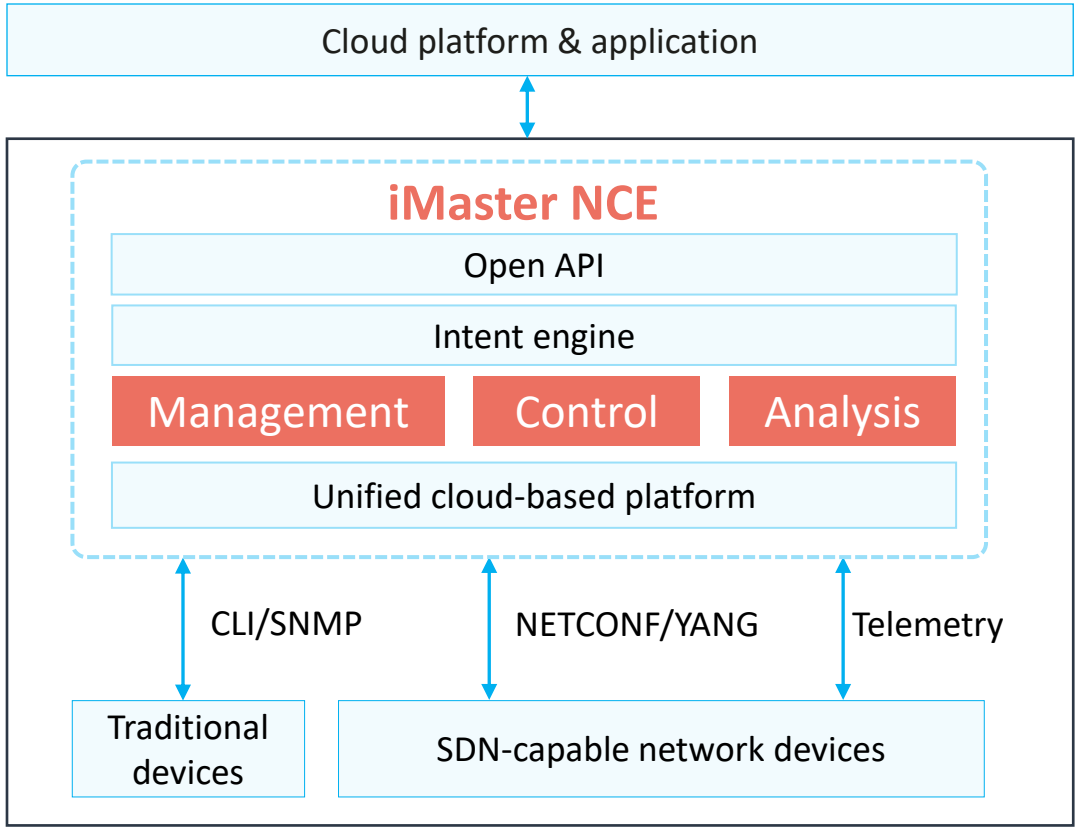
Transformation and Challenges of the Network Industry

- 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.



Huawei iMaster NCE

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



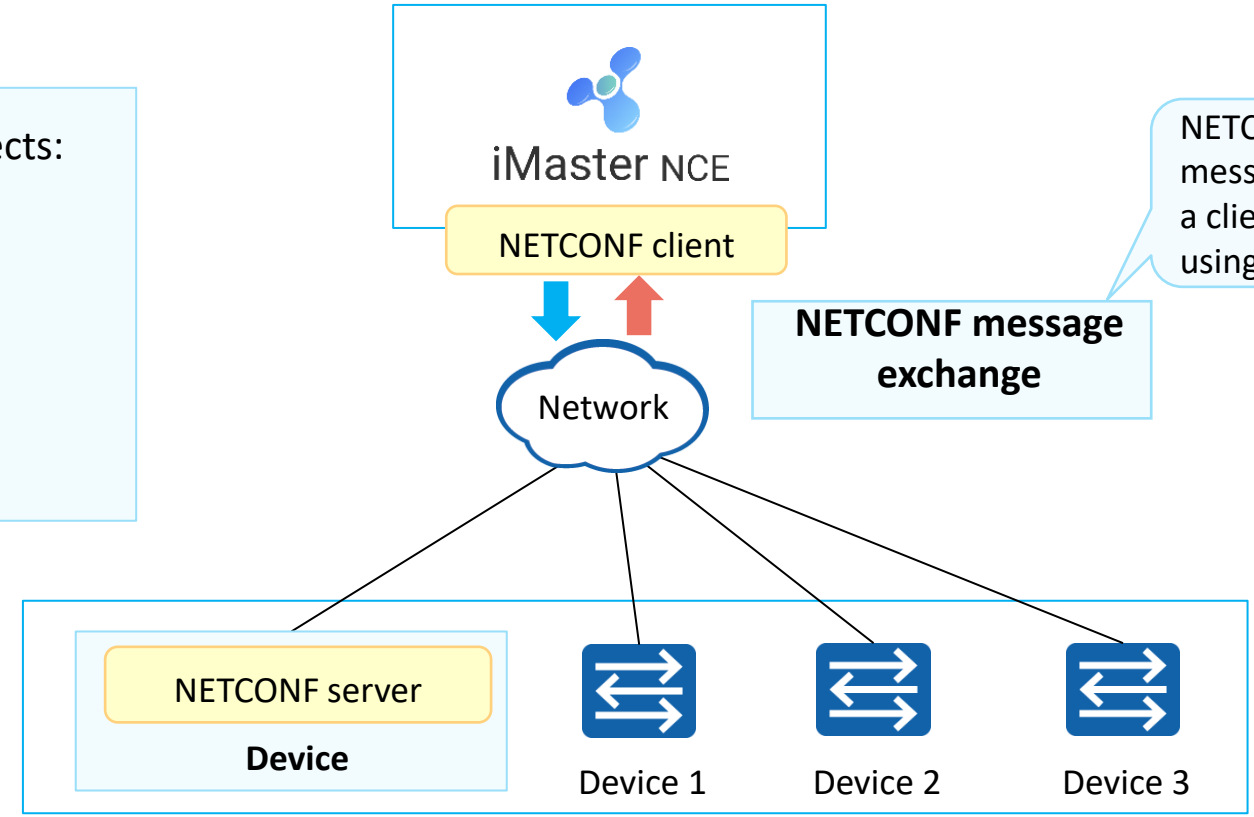
- In terms of management and control, iMaster NCE allows you to:
  - **Manage and control traditional devices** through traditional technologies such as CLI and SNMP.
  - **Manage and control SDN-capable networks** through NETCONF (based on the YANG model).
- iMaster NCE collects network data through 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.

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 has three objects:

- NETCONF client
- NETCONF server
- NETCONF message



NETCONF message exchange

NETCONF requires that messages exchanged between a client and server be encoded using XML.

A client and a server establish a secure connection based on SSH or TLS

NETCONF server reports the trap or event to the client through the Notification mechanism

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

iMaster NCE

SSH connection

RPC

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id=
     "101">
 <edit-config>
  <target>
   <running/>
  </target>
  <config>
    Configuration content in XML format
  </config>
 </edit-config>
</rpc>
```

This operation is to modify configuration.

RPC-Reply

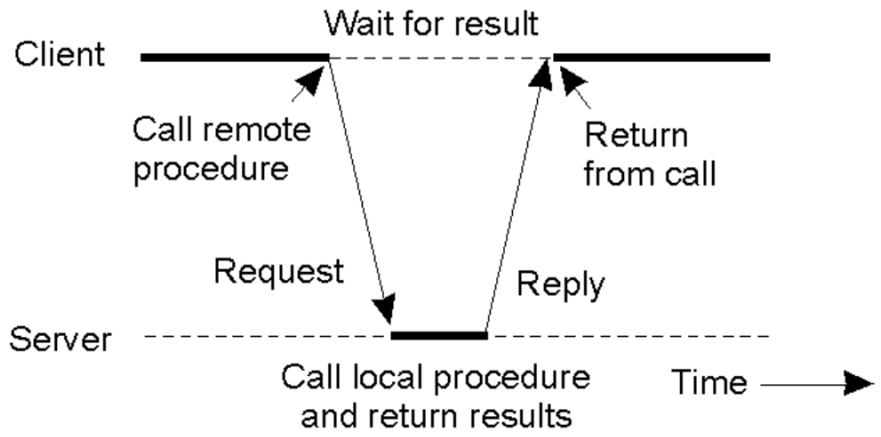
```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <ok/>
</rpc-reply>
```

Modified successfully.

Remote procedure Call

- The programming of distributed applications is difficult. In addition to the usual tasks, programmers who build clients and servers must deal with the complex issues of communication. Although many of the needed functions are supplied by a standard API such as the socket interface, the socket calls require the programmer to specify many low level details as names ,addresses,protocols and ports.

RPC model



- **Remote Procedure Call**
  a
- **Sockets**
- **TCP,UDP**
- **Internet protocol (IP)**

Hides communications details behind procedure call and helps bridge heterogeneous platforms

O.S level interface to the underlying communications protocols TCP,UDP

UDP transports data packets without guarantees, TCP verifies correct delivery of data streams

moves a packet of data from one node to another

- As in conventional procedure calls, when a client calls a remote procedure, the **client will block** until a reply is returned

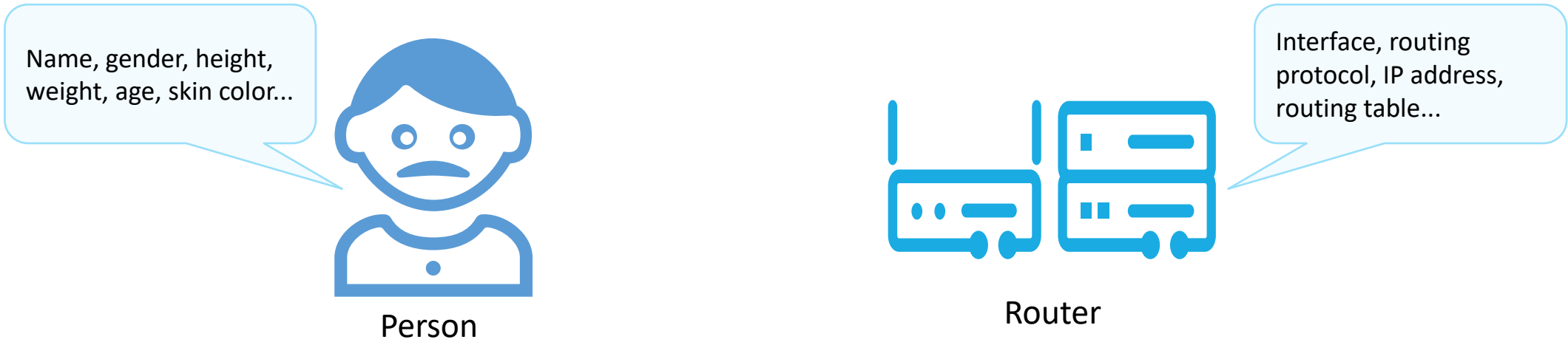
RPC as a programming abstraction that builds upon other communication layers and hides them from the programmer

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.

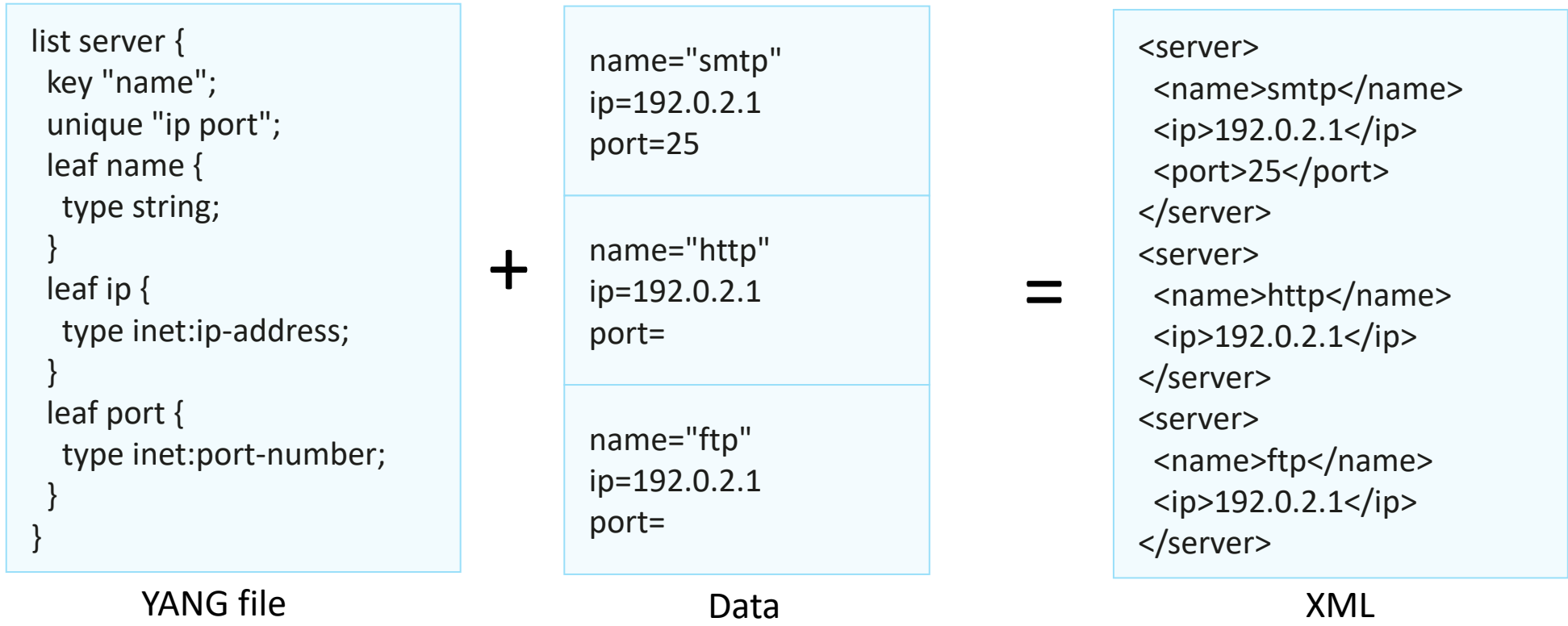
A model is an abstraction and expression of things.

A data model is an abstraction and expression of data features.



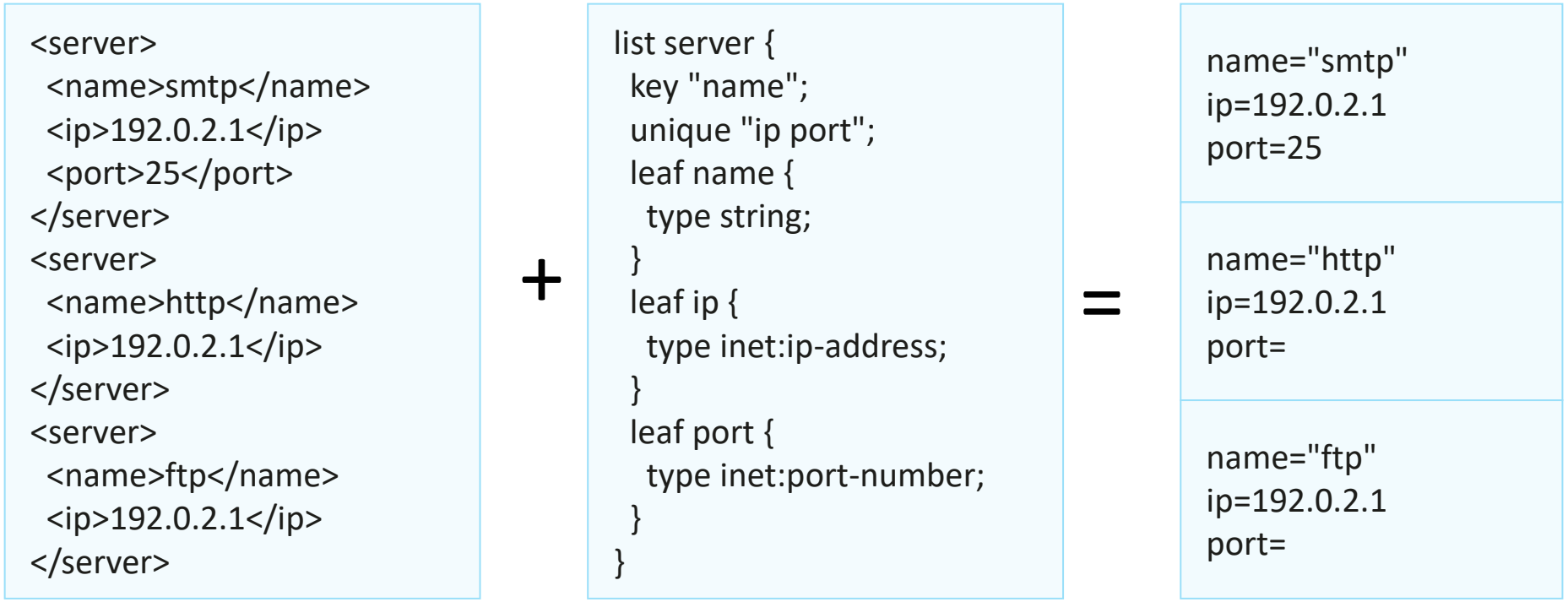
YANG and XML (1)

- 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.



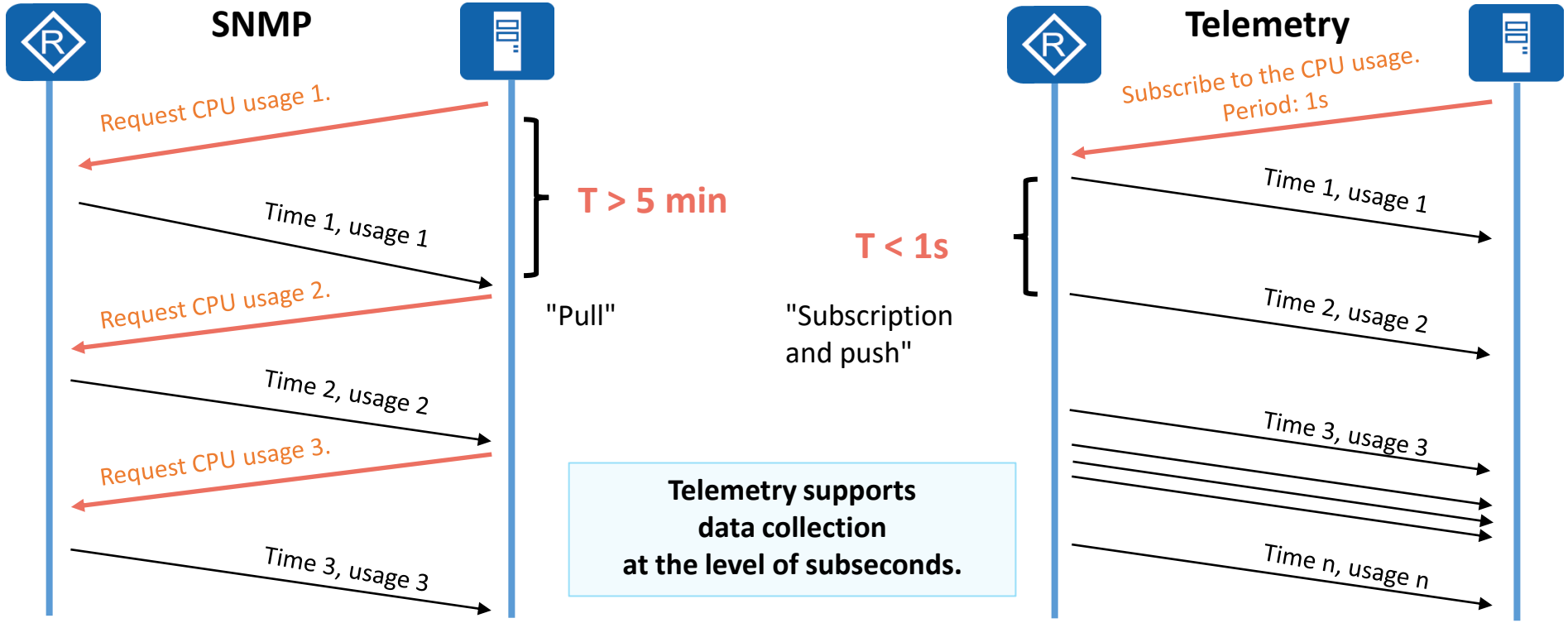
YANG and XML (2)

- 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.



Comparison between Telemetry and conventional network monitoring modes

Item	Telemetry	SNMP Get	SNMP Trap	CLI	Syslog
Working mode	Push	Pull	Push	Pull	Push
Precision	Sub-seconds	Minutes	Seconds	Minutes	Seconds
Whether structured	Structured using the YANG model	Structured using MIB	Structured using MIB	Non-structured	Non-structured

Telemetry Transport Protocol

- Support for Google Remote Procedure Call Protocol (gRPC)
  - gRPC is a high-performance general RPC open-source software framework running over HTTP2 protocols. Both communication parties perform secondary development based on the framework, so that they focus on services and do not need to pay attention to bottom-layer communication implemented by the gRPC software framework.
- Telemetry uses the gRPC protocol to report the data encoded in GPB format to the collector. This layer defines the protocol interaction format for remote procedure calls.