Network Management and O&M

1 Network Management and O&M

1.1 Basic Concepts of Network Management and O&M(Operation and Maintenance)

1.1.1 Overview

- **Purpose:** Ensure devices work properly & network runs efficiently, reliably, and securely.
- **Role:** Managed by a network administrator for stable operation.

1.1.2 Classification of Network Management

- **Software Management:**
  - Management of network applications.
  - User accounts management.
  - Permissions for file access.
- **Hardware Management:**

- Involves managing network elements (NEs) like firewalls, switches, routers.

> **Note**
>
> NEs are both hardware devices and the software running on them with at least one main control board.

1.1.3 Basic Network Management Functions (OSI Model) (FCAPS)

1.1.3.1 Configuration Management

- Monitors configurations.
- Manages hardware/software parameters and conditions.
- Configures services.

1.1.3.2 Performance Management

- Manages network performance for reliable communication with minimal resources.

1.1.3.3 Fault Management

- Maintains network availability.
- Repairs faults Quickly.

1.1.3.4 Security Management

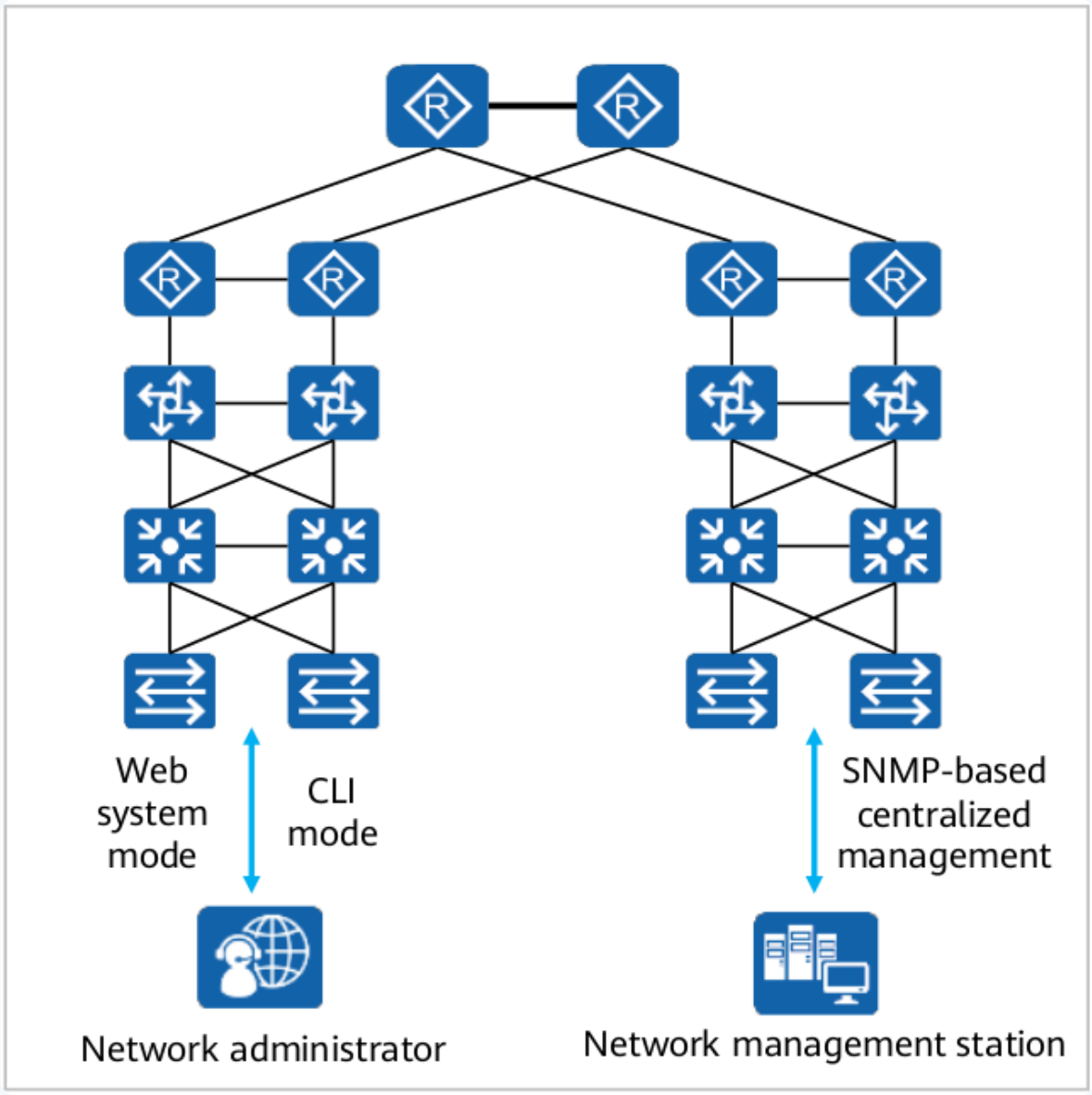
- Protects against unauthorized access and attacks.

1.1.3.5 Accounting Management

- Records user resource usage.
- Charges users based on usage.

1.1.4 Network Management Modes

1.1.4.1 Traditional Network Management



Mode	Description
Web System	GUI via built-in web server (HTTPS).
CLI Mode	Command line management via console port, Telnet, or SSH.
SNMP-based Centralized	Manages NEs using SNMP from a central management station.

CLI mode: provides Enhanced device management but requires that users be familiar with command lines.

SNMP-based centralized management: provides centralized and unified management of devices on the entire network, greatly improving

> management efficiency.

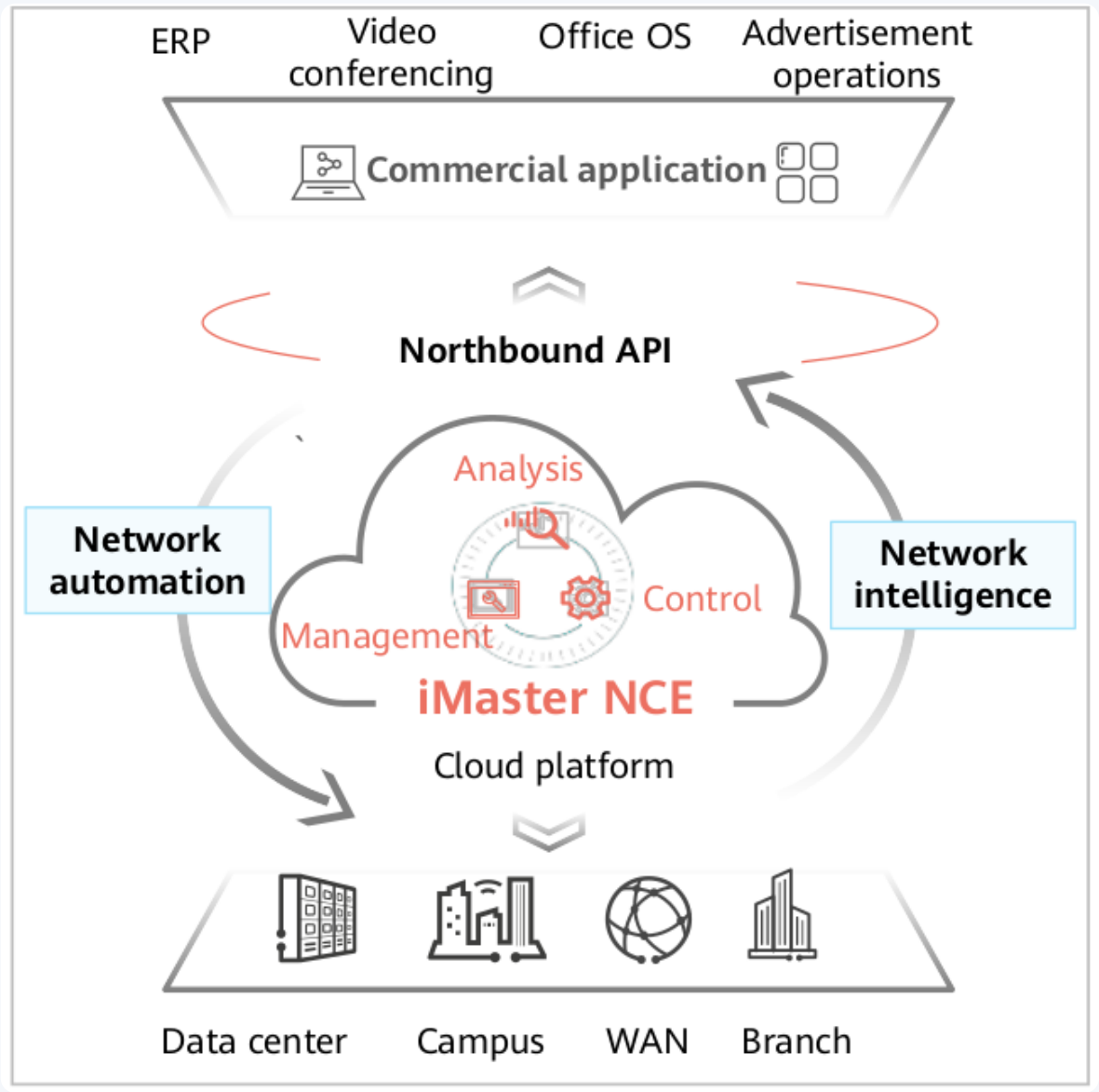
SNMP unified managment

- Without SNMP, manual login and command execution (`show ip ospf` on Cisco, `show ospf neighbor` on Juniper) are necessary for OSPF status.
- With SNMP, an SNMP manager queries OSPF data using standardized OIDs in the routers' MIBs via SNMP protocol operations without direct CLI commands.

Here's an example of what some OID requests might look like:

- To get OSPF version number: `SNMP GET 1.3.6.1.2.1.14.1.2`
- To get OSPF area ID: `SNMP GET 1.3.6.1.2.1.14.2`

1.1.4.2 iMaster NCE-based Network Management



Feature	Description
Automation & Intelligence Platform	Integrates management, control, analysis, AI.
Full-lifecycle Automation	Simplifies operations through automation.
Intelligent Closed-loop Mgmt.	Utilizes big data & AI for decision-making.
Open Programmability	Supports scenario-specific applications ecosystem.
All-cloud Platform Capacity	Manages networks on a large scale efficiently.

Protocols Used:

- NETCONF & RESTCONF for configuration delivery.
- Telemetry for traffic monitoring.

1.2 SNMP Fundamentals and Configuration

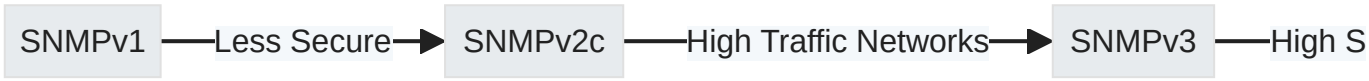
1.2.1 Key Concepts

1.2.1.1 SNMP Basic Understanding

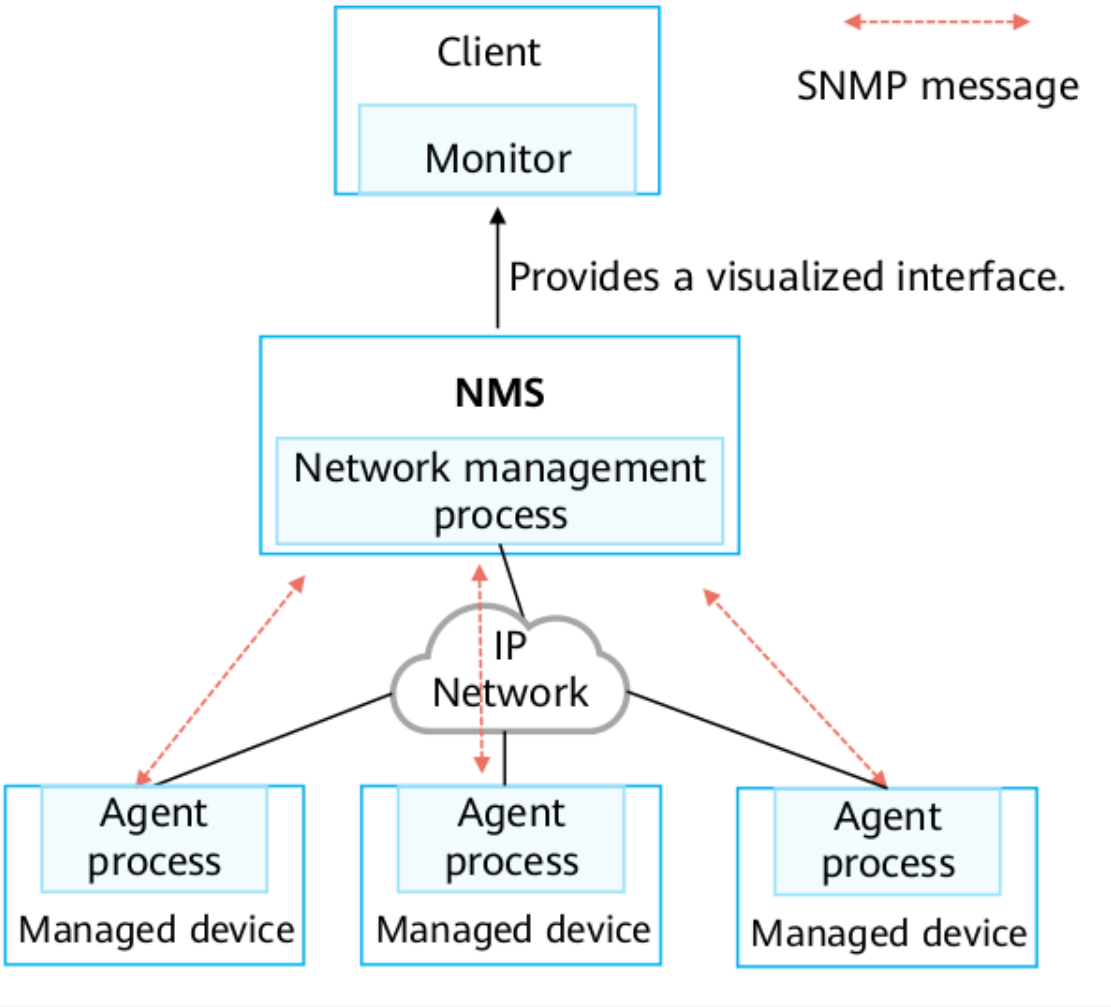
> **Note:** SNMP is crucial for network management, especially in large-scale networks with diverse device types.

- **Simplicity**: Uses UDP and polling mechanism.
- **Convenience**: Enables management across different devices.

1.2.1.2 SNMP Versions



- `SNMPv1` : Basic functionality, low security.
- `SNMPv2c` : Enhanced error codes and bulk operations.
- `SNMPv3` : Authentication and encryption support.



1.2.1.3 MIB (Management Information Base)

A MIB is a structured database of variables for network devices, containing OIDs, statuses, access permissions, and data types.

1.2.1.3.1 Public vs. Private MIBs

- **Public:** Defined by RFCs for standardization.
- **Private:** For enterprise-specific functions or protocols.

1.2.1.3.2 Common MIB Objects Access Permissions

OID	Object Name	Data Type	Access Level	Description
`1.3.6.1.2.1.2.1`	ifNumber	Integer	read-only	Number of interfaces
`1.3.6.1...`	hwIpAdEntNetMask	IpAddress	read-create	Subnet mask

1.2.1.4 SNMP Message Types

1.2.1.4.1 Operations and Traps in Different Versions

- `Get` , `Set` , `GetNext` , `Response` , `Trap` : Basic operations in SNMPv1.
  - `Get` : Asks for the value of a specific variable from an SNMP agent.
  - `Set` : Tells an SNMP agent to change the value of a specific variable.
  - `GetNext` : Requests the next variable in the MIB (Management Information Base) hierarchy from an SNMP agent.
  - `Response` : The reply from an SNMP agent delivering the requested information or confirmation of a set action.
  - `Trap` : An unasked or unrequested message from an SNMP agent to the management system indicating an event or change in status.
- **Added in SNMPv2c:** `GetBulk` (multiple GetNext), `Inform` (requires acknowledgment).
  - `GetBulk` : A request to efficiently retrieve large volumes of data by requesting multiple `GetNext` operations in a single command.
  - `Inform` : A message sent between SNMP managers to share alerts or notifications, with a confirmation required to acknowledge receipt.
- **SNMPv3:** Same as v2c but with security enhancements (authentication & encryption).

1.2.1.5 Configuration Basics

1.2.1.5.1 Enabling SNMP on a Device

```Markdown
[R1]snmp-agent
[R1]snmp-agent sys-info version <version>
```

- `<version>` : is v1,v2c,v3 for snmp.

> **Warning**
>
> Ensure that the protocol version matches between device and NMS.

1.2.1.5.2 Create or update MIB view information.

```Markdown
[Huawei] snmp-agent mib-view view-name < exclude | include > subtree-name {mask <mask>}
```

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

```Markdown
[Huawei] snmp-agent group v3 <group-name> <authentication||noauth||privacy> { read-view <view-name> | write-view <view-name> | notify-view <view-name> }
```

1.2.1.5.4 Add a user to the SNMP group.

```
[Huawei] snmp-agent usm-user v3 <user-name> group
<group-name>
```

1.2.1.5.5 Configure an authentication password for an SNMPv3 user.

```
[Huawei] snmp-agent usm-user v3 <user-name>
authentication-mode < md5 | sha | sha2-256 >
```

1.2.1.5.6 Configure the SNMPv3 user encryption password.

```
[Huawei] snmp-agent usm-user v3 <user-name> privacy-
mode < aes128 | des56 >
```

1.2.1.5.7 Set parameters for the device to send traps.

```
[Huawei] snmp-agent target-host trap-paramsname
<paramsname> v3 securityname <securityname>
<authentication | noauthnopriv | privacy >
```

1.2.1.5.8 Configure the target host of traps.

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

1.2.1.5.9 Enable all trap functions.

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

1.2.1.5.10 Configure the source interface that sends traps.

```Markdown
[Huawei] snmp-agent trap source <interface-type> <interface-number>
```

1.3 Network Management Based on Huawei iMaster NCE

1.3.1 Huawei iMaster NCE Platform

> Constructing automated and intelligent network systems centered on user experience is important to address the explosive increase in traffic and service complexity.

1.3.1.1 Overview

- Integrates management, control, analysis, AI functions.
- Manages both traditional devices and SDN-capable networks.

1.3.1.2 Key Capabilities

1.3.1.2.1 Full-lifecycle Automation

- Device plug-and-play.
- On-demand service provisioning.
- Fault self-healing.

1.3.1.2.2 Intelligent Closed-loop Management

- Intent engine and automation engine for real-time network status determination.
- AI algorithms provide automated analysis and decision-making.

1.3.1.2.3 Open Programmability

> Ecosystem for scenario-based applications:
>
> - Southbound programmability with Design Studio.
> - Northbound cloud-based AI training platforms.

> - **South side:** Manages network hardware and infrastructure

- **North side:** Interfaces with applications using network data for higher-level tasks.

1.3.1.2.4 Large-capacity Cloud Platform

- Supports on-premises and cloud-based deployment.
- Elastic scalability for numerous access users.

1.3.1.3 NETCONF Protocol

1.3.1.3.1 NETCONF Overview

> NETCONF is a network management protocol that allows for the installation, manipulation, and deletion of the configuration of network devices using XML.

- **NETCONF has three objects:**
  - NETCONF client
  - NETCONF server
  - NETCONF message

1.3.1.3.2 Advantages of NETCONF vs SNMP vs CLI

Function	NETCONF	SNMP	CLI
Interface	Machine-machi	Machine-man interface	Man-machine

Function	NETCONF	SNMP	CLI
Operation	High efficie	Medium efficiency	Low
Scalability	Extens	Weak	Moderate
Transactio Strong support like rollback like	Not supported	Partially	
Secure Trans.	Multiple pro cols	Only SNMPv3	SSH only

1.3.1.4 YANG Modeling Language

1.3.1.4.1 YANG Overview

YAML

```yaml
// YANG file example snippet:
module example-module {
namespace "http://example.com/ns/example-module";
prefix "ex";

container server {
    list server {
      key "name";
      unique "ip port";
      leaf name { type string; }
      leaf ip { type inet:ip-address; }
      leaf port { type inet:port-number; }
    }
}
}
```

> The YANG file is used to convert data into XML-format NETCONF messages before they are sent to the device.

> The YANG file is used to convert received XML-format NETCONF messages into data for subsequent processing.

1.3.1.4.2 Characteristics of YANG Models

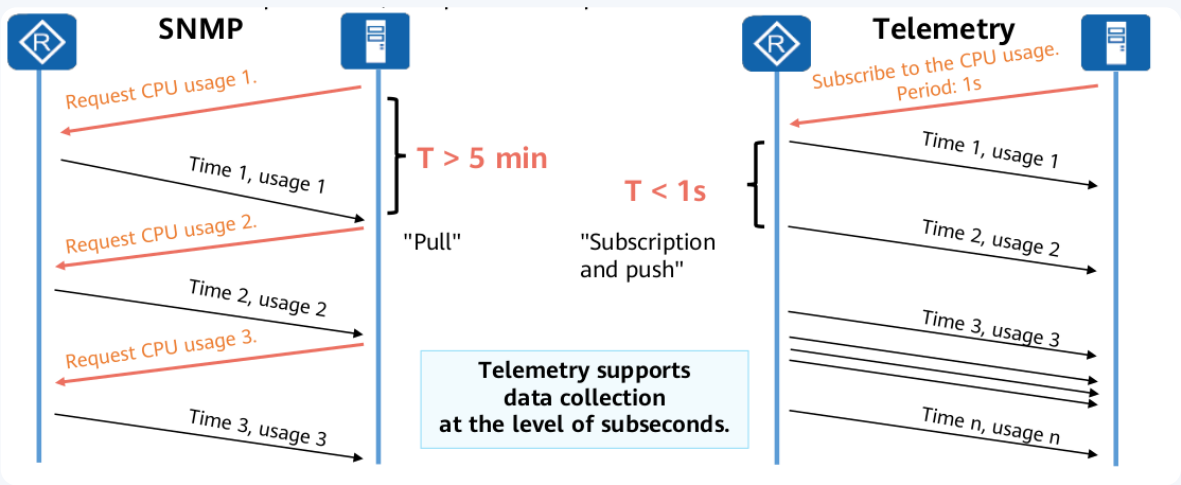
- Hierarchical tree-like structure modeling.
- Modules and sub-modules presentation.
- Conversion to XML-syntax YIN model without loss.

1.3.1.5 Telemetry Technology

1.3.1.5.1 Telemetry vs SNMP

SNMP - Pull Mode → T > 5 min

Telemetry - Push Mode → T < 1s



- **Pull mode (SNMP):** The monitoring system periodically requests information from devices.
- **Push mode (Telemetry):** Devices automatically send information to the monitoring system in real-time or at configured intervals.

1.3.1.5.2 Benefits of Telemetry

- Sub-second level data collection for real-time insights.
- Improved transmission efficiency through data packaging.