

The background features a complex network of thin, light gray lines forming a web-like structure. Scattered throughout are small circles in various colors: light blue, dark blue, purple, and white. Some of these circles are connected by solid gray lines, while others are isolated. Dashed gray lines also crisscross the background, adding to the technical, network-like aesthetic.

网络管理与运维

主讲人：鲍婷婷

目录

- 1 网络管理与运维基本概念
- 2 SNMP原理与配置
- 3 基于华为iMaster NCE的网络管理

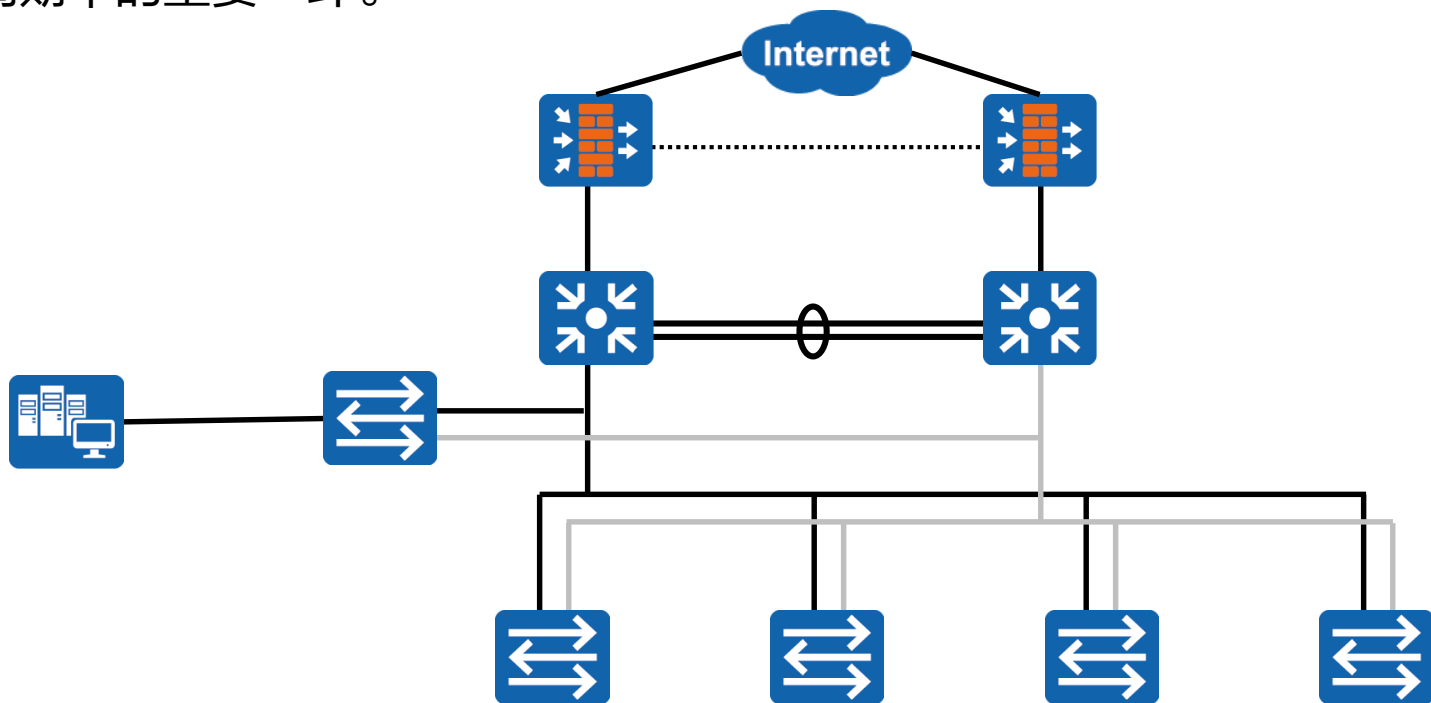
什么是网络管理?

- 网络管理是通过对网络中设备的管理，保证设备工作正常，使通信网络正常地运行，以提供高效、可靠和安全的通信服务，是通信网络生命周期中的重要一环。

网络管理员管理和维护网络，保证网络的稳定运行。



网络管理员



常见企业网络架构

网络管理基本功能

配置
管理

性能
管理

故障
管理

安全
管理

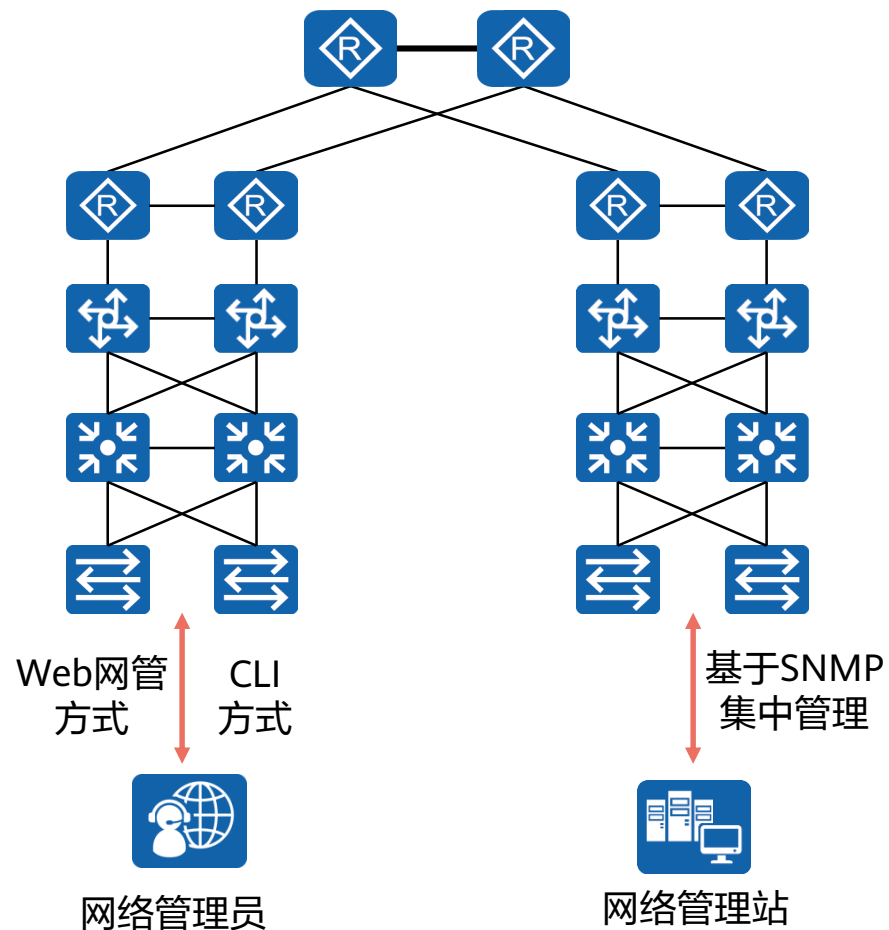
计费
管理

OSI定义了网络管理的五大功能模型：

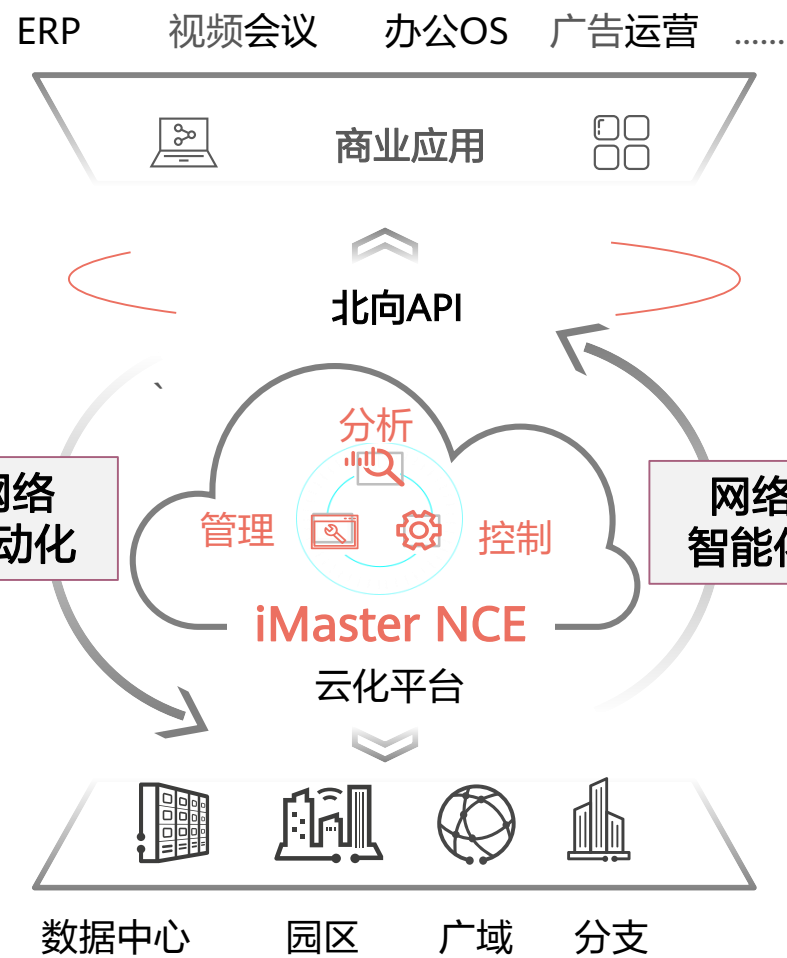
- 配置管理（ Configuration Management ）： 配置管理负责监控网络的配置信息，使网络管理人员可以生成、查询和修改硬件、软件的运行参数和条件，并可以进行相关业务的配置。
- 性能管理（ Performance Management ）： 性能管理以网络性能为准则，保证在使用较少网络资源和具有较小时延的前提下，网络能够提供可靠、连续的通信能力。
- 故障管理（ Fault Management ）： 故障管理的主要目标是确保网络始终可用，并在发生故障时尽快将其修复。
- 安全管理（ Security Management ）： 安全管理可以保护网络 and 系统免受未经授权的访问和安全攻击。
- 计费管理（ Accounting Management ）： 记录用户使用网络资源的情况并核收费用，同时也统计网络的利用率。

网络管理方式

传统网络管理



基于iMaster NCE的网络管理



目录

1

网络管理与运维基本概念

2

传统网络管理

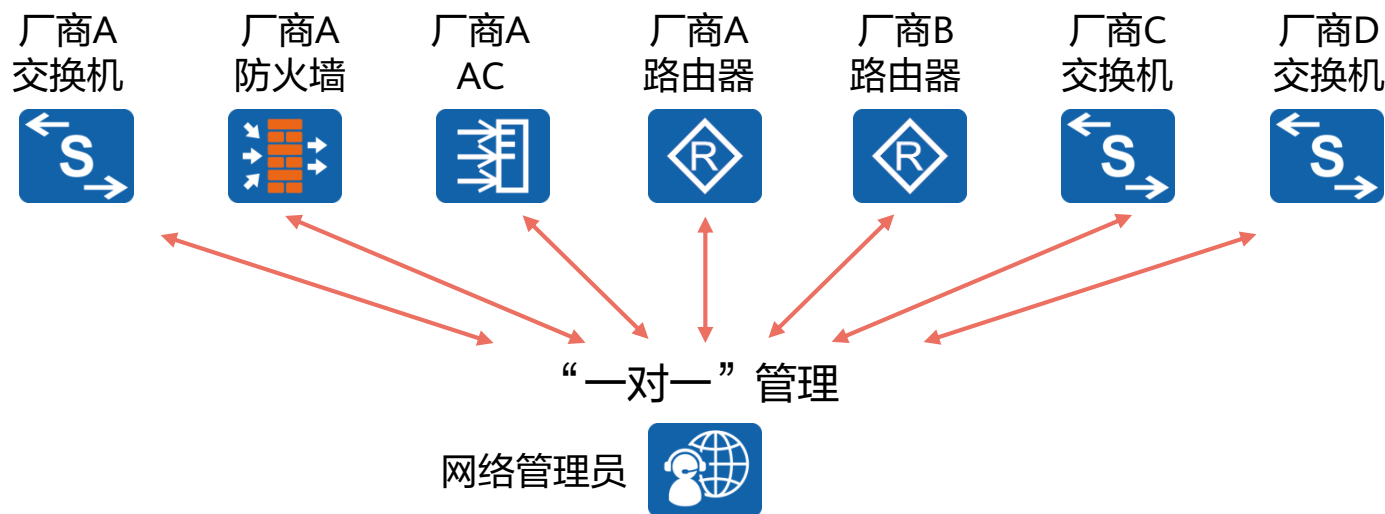
- SNMP原理
- SNMP配置

3

基于华为iMaster NCE的网络管理

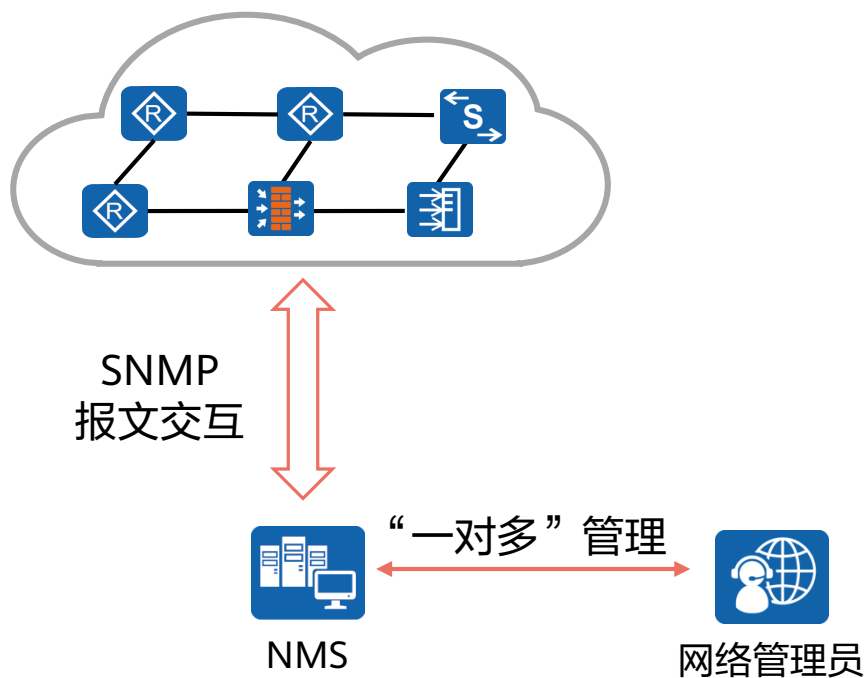
通过CLI或Web进行管理

- 当网络规模较小时，CLI和Web方式是常见的网络管理方式。
 - 网络管理员可以通过HTTPS、Telnet、Console等方式登录设备后，对设备逐一进行管理。
 - 这种管理方式不需要在网络中安装任何程序或部署服务器，成本较低。
 - 网络管理员自身需要熟练掌握网络理论知识、各设备厂商网络配置命令。
 - 当网络规模较大，网络拓扑较为复杂时，这种方式的局限性较大。



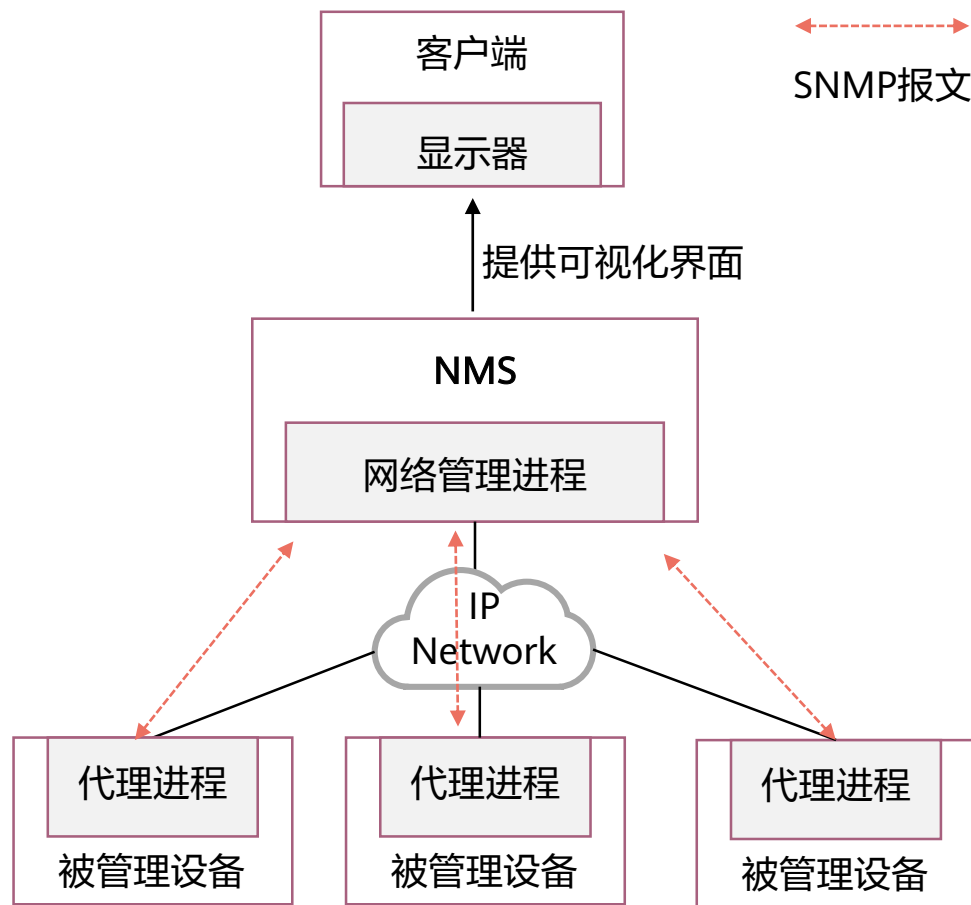
基于SNMP的集中式管理

- SNMP（Simple Network Management Protocol，简单网络管理协议）是广泛用于TCP/IP网络的网络管理标准协议，提供了一种通过运行网络管理软件的中心计算机，即NMS（Network Management Station，网络管理工作站）来管理网元的方法。



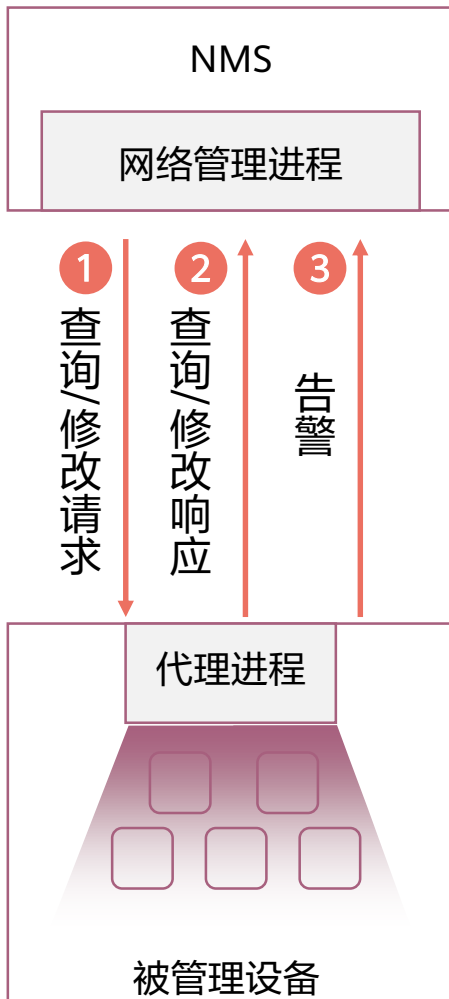
- 网络管理员可以利用NMS在网络上的任意节点完成信息查询、信息修改和故障排查等工作，提升工作效率。
- 屏蔽了不同产品之间的差异，实现了不同种类和厂商的网络设备之间的统一管理。

SNMP典型架构



- 在基于SNMP进行管理的网络中，NMS是整个网络的网管中心，在它之上运行管理进程。每个被管理设备需要运行代理（Agent）进程。管理进程和代理进程利用SNMP报文进行通信。
- NMS是一个采用SNMP协议对网络设备进行管理/监控的系统，运行在NMS服务器上。
- 被管理设备是网络中接受NMS管理的设备。
- 代理进程运行于被管理设备上，用于维护被管理设备的信息数据并响应来自NMS的请求，把管理数据汇报给发送请求的NMS。

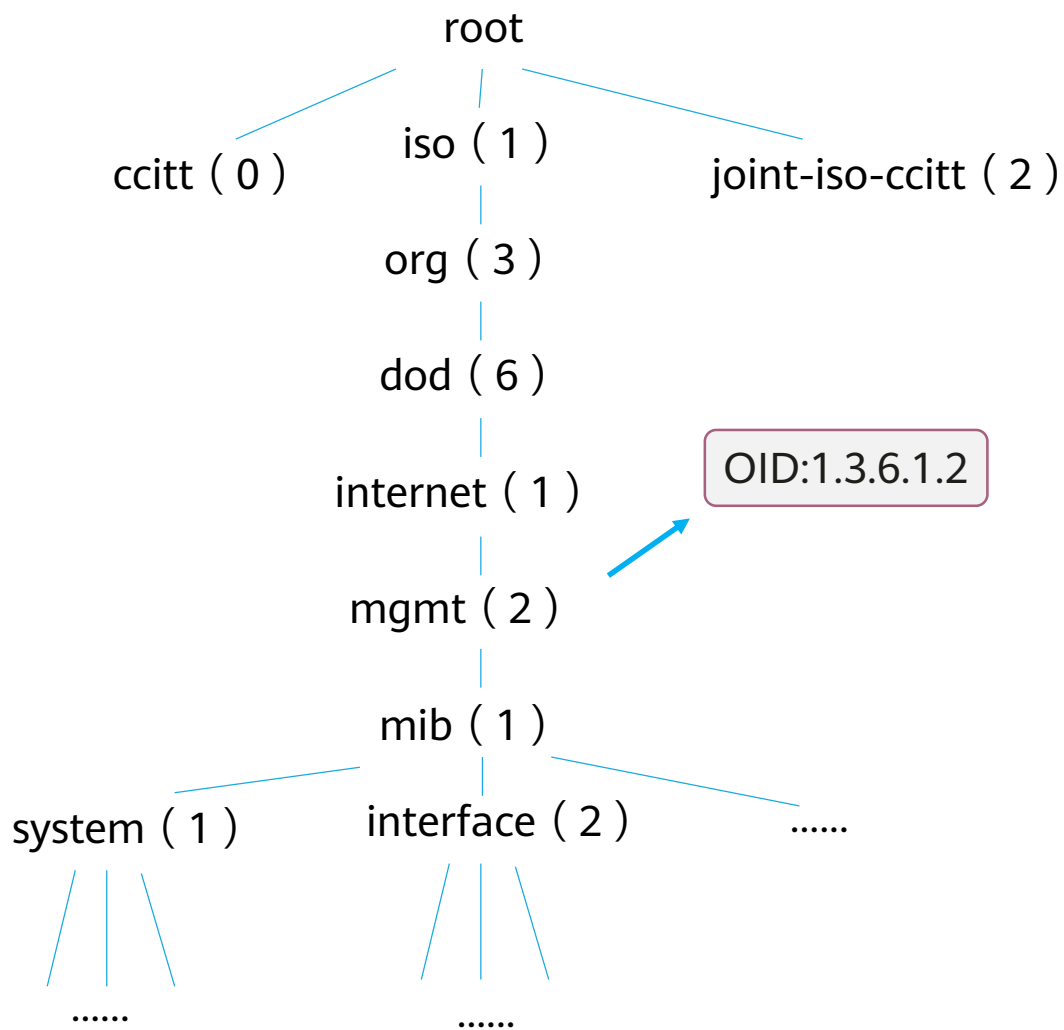
SNMP的信息交互



被管理对象

- NMS和被管理设备的信息交互分为两种：
 - NMS通过SNMP协议给被管理设备发送修改配置信息请求或查询配置信息请求。被管理设备上运行的代理进程根据NMS的请求消息做出响应。
 - 被管理设备可以主动向NMS上报告警信息（Trap）以便网络管理员及时发现故障。
- 被管理对象（Managed object）：每一个设备可能包含多个被管理对象，被管理对象可以是设备中的某个硬件，也可以是在硬件、软件（如路由选择协议）上配置的参数集合。
- SNMP规定通过MIB（Management Information Base，管理信息库）去描述可管理实体的一组对象。

MIB



- MIB是一个数据库，指明了被管理设备所维护的变量（即能够被代理进程查询和设置的信息）。MIB在数据库中定义了被管理设备的一系列属性：
 - 对象标识符（Object Identifier, OID）
 - 对象的状态
 - 对象的访问权限
 - 对象的数据类型等
- MIB给出了一个数据结构，包含了网络中所有可能的被管理对象的集合。因为数据结构与树相似，MIB又被称为对象命名树。

常见MIB节点

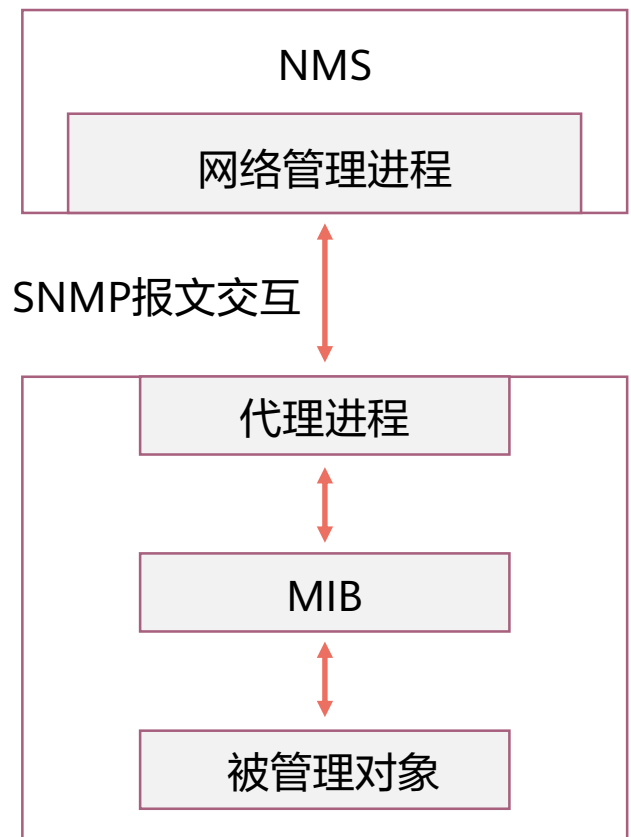
- 用于查询或修改的节点：

OID	节点名称	数据类型	最大访问权限	含义
1.3.6.1.2.1.2.1	ifNumber	Integer	read-only	系统中网络接口的数量（不关注接口当前状态）。
1.3.6.1.4.1.2011.5.25.41.1.2.1.1.3	hwIpAdEntNetMask	IpAddress	read-create	IP地址的子网掩码。

- 用于告警通知的节点：

OID	节点名称	绑定变量	含义
3.6.1.6.3.1.1.5.3	linkDown	ifIndex ifAdminStatus ifOperStatus ifDesc	经检测到由于ifOperStatus节点中的其中一条通信链路已经从其他状态（但不是notPresent状态）进入Down状态。这里的其他状态由ifOperStatus的值显示。

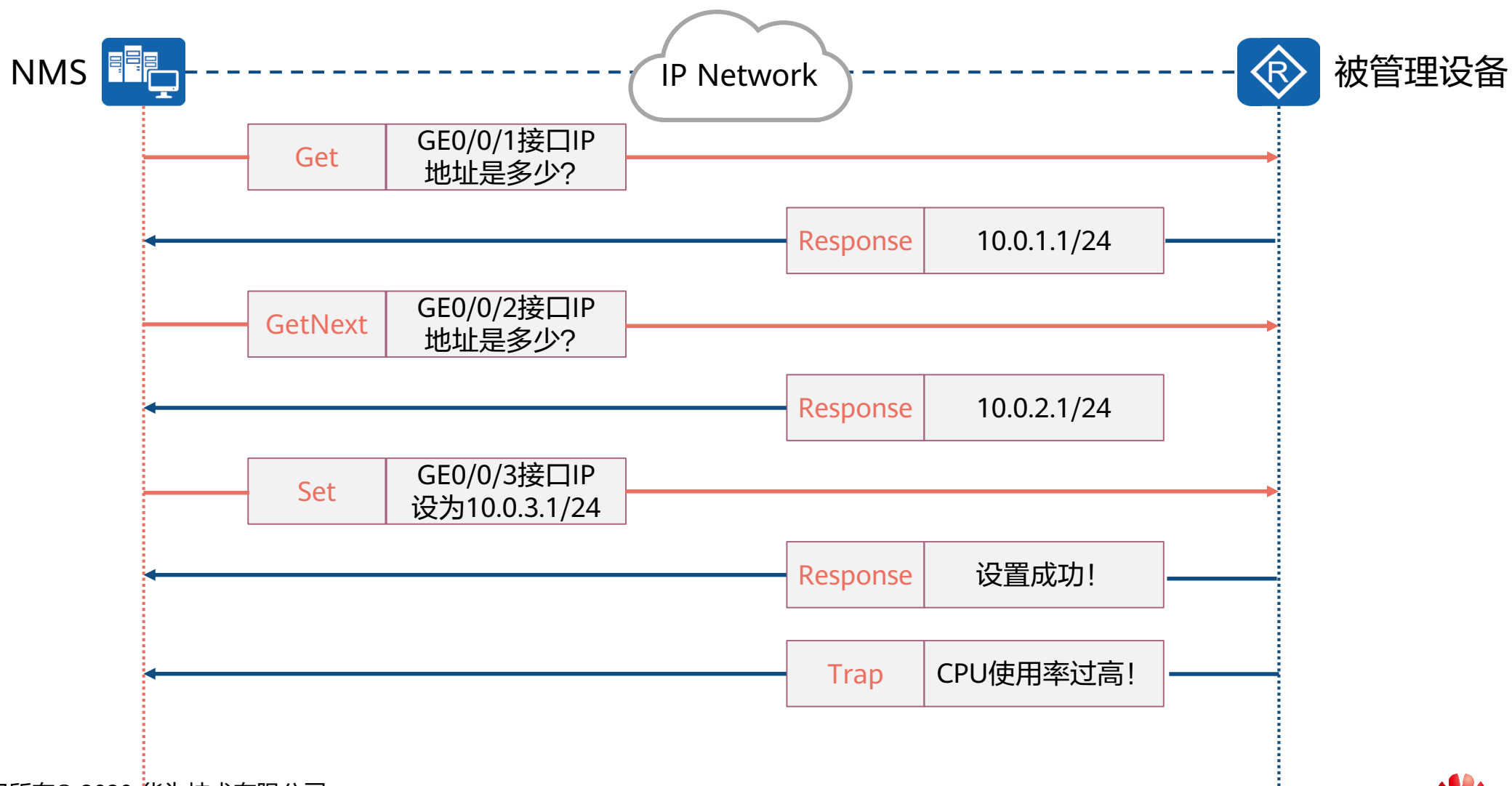
SNMP管理模型



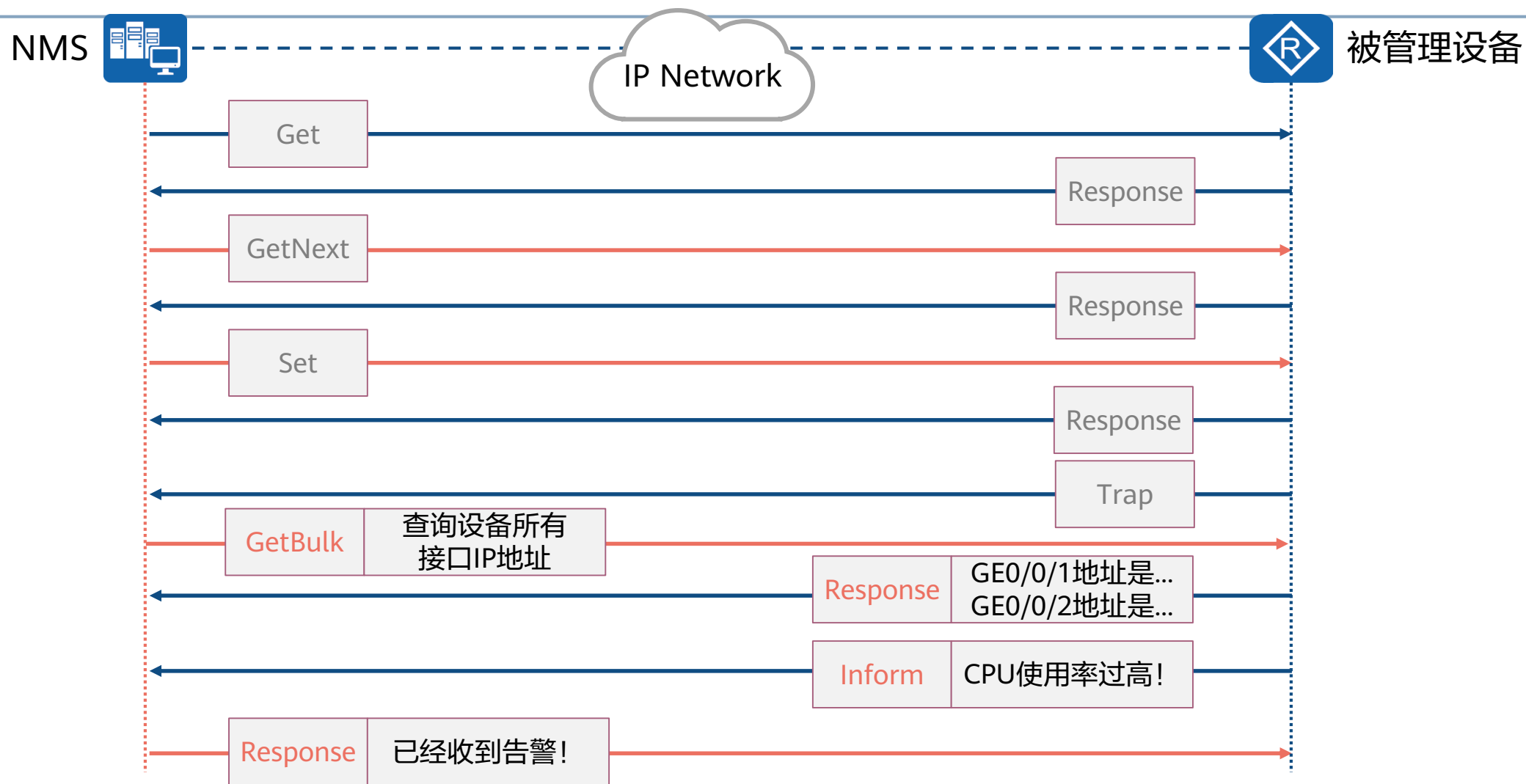
被管理设备

- 查询/修改操作：
 - NMS作为管理者，向代理进程发送SNMP请求报文。
 - 代理进程通过设备端的MIB找到所要查询或修改的信息，向NMS发送SNMP响应报文。
- 告警操作：
 - 设备端的模块由于达到模块定义的告警触发条件，通过代理进程向NMS发送消息，告知设备侧出现的情况，这样便于网络管理人员及时对网络中出现的情况进行处理。

SNMPv1

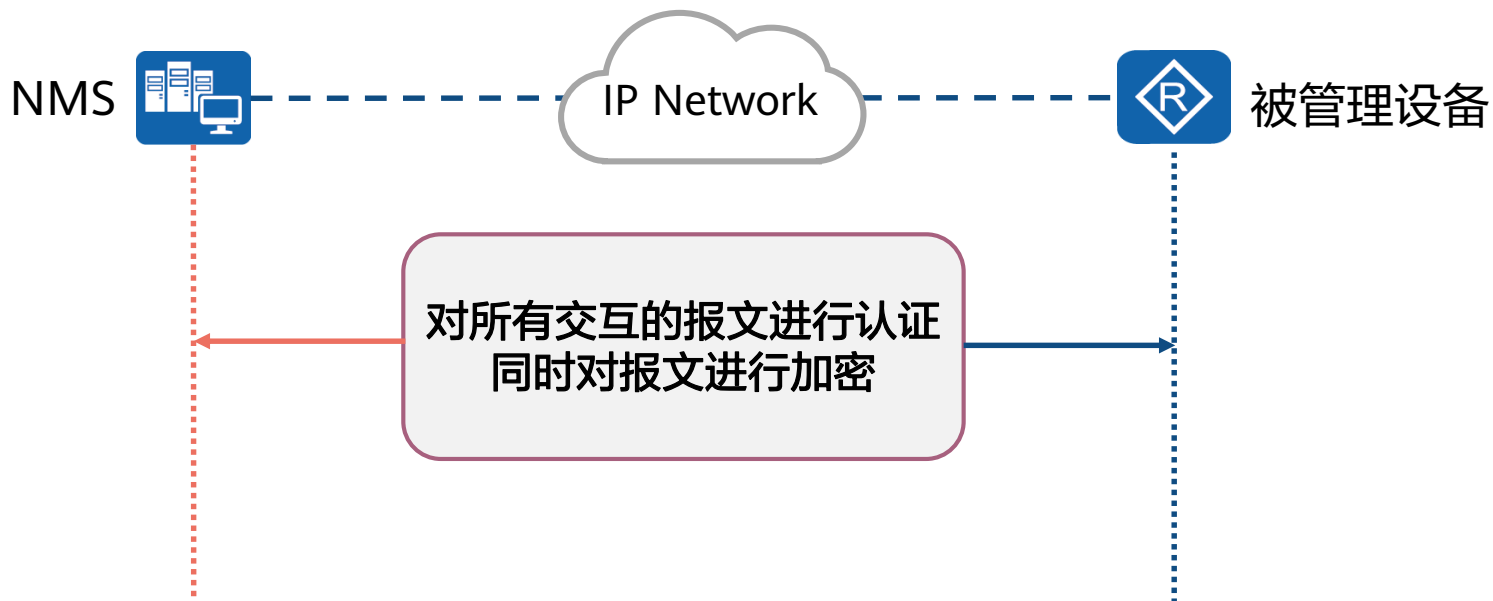


SNMPv2c



SNMPv3

- SNMPv3与SNMPv1和SNMPv2c的工作机制基本一致但添加了报头数据和安全参数。
- SNMPv3报文具有身份验证和加密处理的功能。
- SNMPv3适用于各种规模的网络，安全性极高。



SNMP小结

- SNMP的特点如下：
 - 简单：SNMP采用轮询机制，提供基本的功能集，适合快速、低价格的场景使用，而且SNMP以UDP报文为承载，因而得到绝大多数设备的支持。
 - 强大：SNMP的目标是保证管理信息在任意两点传送，便于管理员在网络上的任何节点检索信息，进行故障排查。
- SNMPv1版本适用于小型网络。组网简单、安全性要求不高或网络环境比较安全且比较稳定的网络，比如校园网，小型企业网。
- SNMPv2c版本适用于大中型网络。安全性要求不高或者网络环境比较安全，但业务比较繁忙，有可能发生流量拥塞的网络。
- SNMPv3版本作为推荐版本，适用于各种规模的网络。尤其是对安全性要求较高，只有合法的管理员才能对网络设备进行管理的网络。

目录

1

网络管理与运维基本概念

2

传统网络管理

- SNMP 原理
- **SNMP 配置**

3

基于华为iMaster NCE的网络管理

SNMP基本配置 (1)

1. 使能SNMP代理功能

```
[Huawei] snmp-agent
```

2. 配置SNMP的版本

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

用户可以根据自己的需求配置对应的SNMP版本，但设备侧使用的协议版本必须与网管侧一致。

3. 创建或者更新MIB视图的信息

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

4. 增加一个新的SNMP组，将该组用户映射到SNMP视图

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

该命令用于SNMPv3版本中创建SNMP组，指定认证加密方式、只读视图、读写视图、通知视图。是安全性需求较高的网管网络中的必需指令。

SNMP基本配置 (2)

5. 为一个SNMP组添加一个新用户

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

6. 配置SNMPv3用户认证密码

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

7. 配置SNMPv3用户加密密码

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

8. 配置设备发送Trap报文的参数信息

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

SNMP基本配置 (3)

9. 配置Trap报文的目的主机

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

10. 打开设备的所有告警开关

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

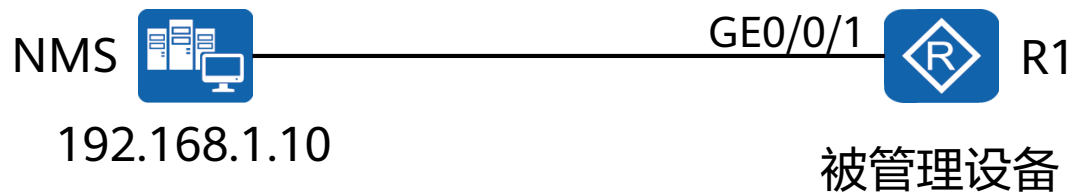
注意该命令只是打开设备发送Trap告警的功能，要与snmp-agent target-host协同使用，由snmp-agent target-host指定Trap告警发送给哪台设备。

11. 配置发送告警的源接口。

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

注意Trap告警无论从哪个接口发出都必须有一个发送的源地址，因此源接口必须是已经配置了IP地址的接口。

SNMP配置举例（网络设备侧）



- 上述路由器R1上使能SNMP功能，配置版本为v3。
- 配置SNMPv3组名为test，加密认证方式为privacy。
- 创建SNMPv3用户，名为R1同时配置认证和加密密码为HCIA-Datacom123。
- 创建名为param的Trap参数信息，securityname为sec
- 设置SNMP告警主机地址为192.168.1.10。
- 打开告警开关，设置发送告警的源接口为GE0/0/1。

R1配置如下：

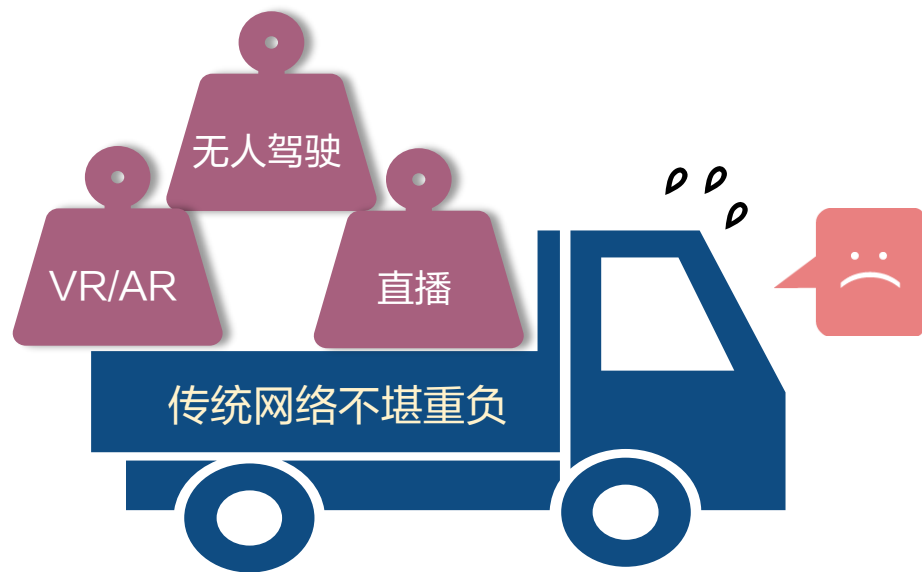
```
[R1]snmp-agent
[R1]snmp-agent sys-info version v3
[R1]snmp-agent group v3 test privacy
[R1]snmp-agent usm-user v3 R1 test authentication-mode
md5 HCIA@Datacom123 privacy-mode aes128 HCIA-
Datacom123
[R1]snmp-agent target-host trap-paramsname param v3
securityname sec privacy
[R1]snmp-agent target-host 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
```

目录

- 1 网络管理与运维基本概念
- 2 传统网络管理
- 3 基于华为iMaster NCE的网络管理
 - 基于华为iMasterNCE的网络管理

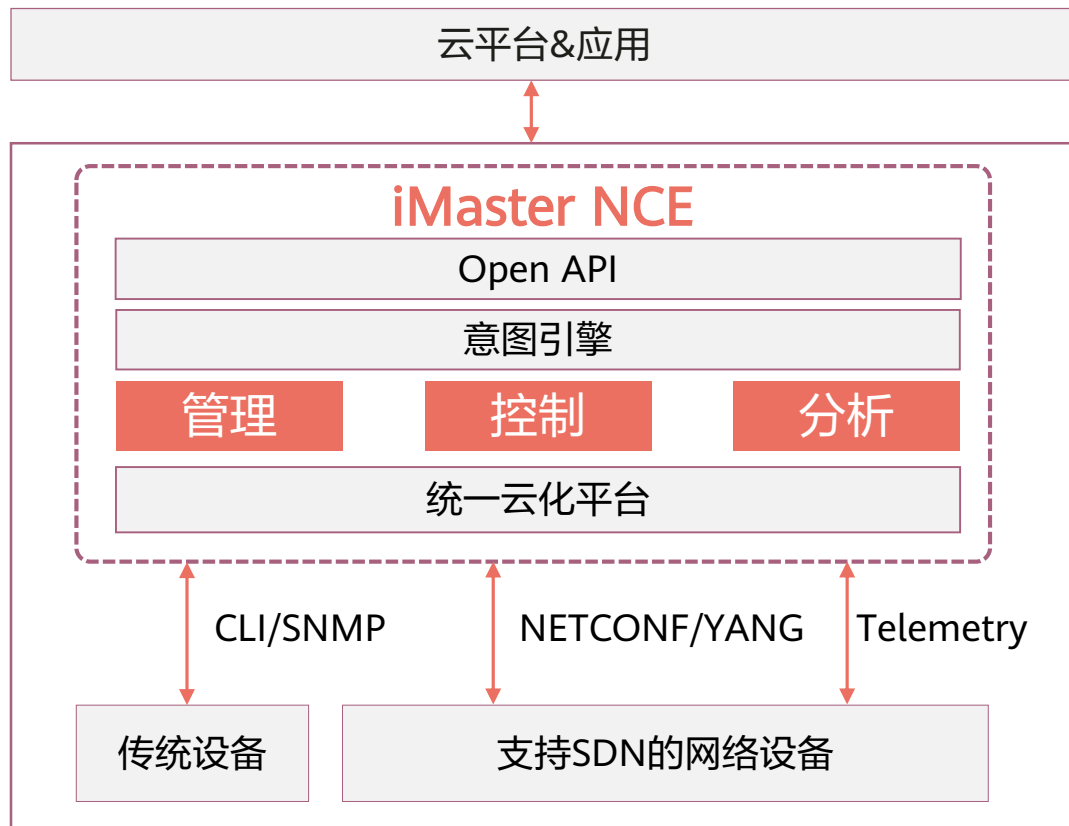
网络产业的变革与挑战

- 伴随5G和云时代的到来，VR/AR、直播、无人驾驶等各类创新性业务大量涌现，整个ICT产业迸发出蓬勃生机。与此同时，整个网络的流量也呈现出爆炸式增长，华为GIV（Global Industry Vision，全球产业展望）预计，2025年新增的数据量将达到180 ZB。业务的动态复杂性也使得整个网络复杂度不断攀升。
- 整体来看，这些问题的源头都指向了现有的网络系统，只有通过构建自动化、智能化的以用户体验为中心的网络系统才能有效应对。



华为iMaster NCE

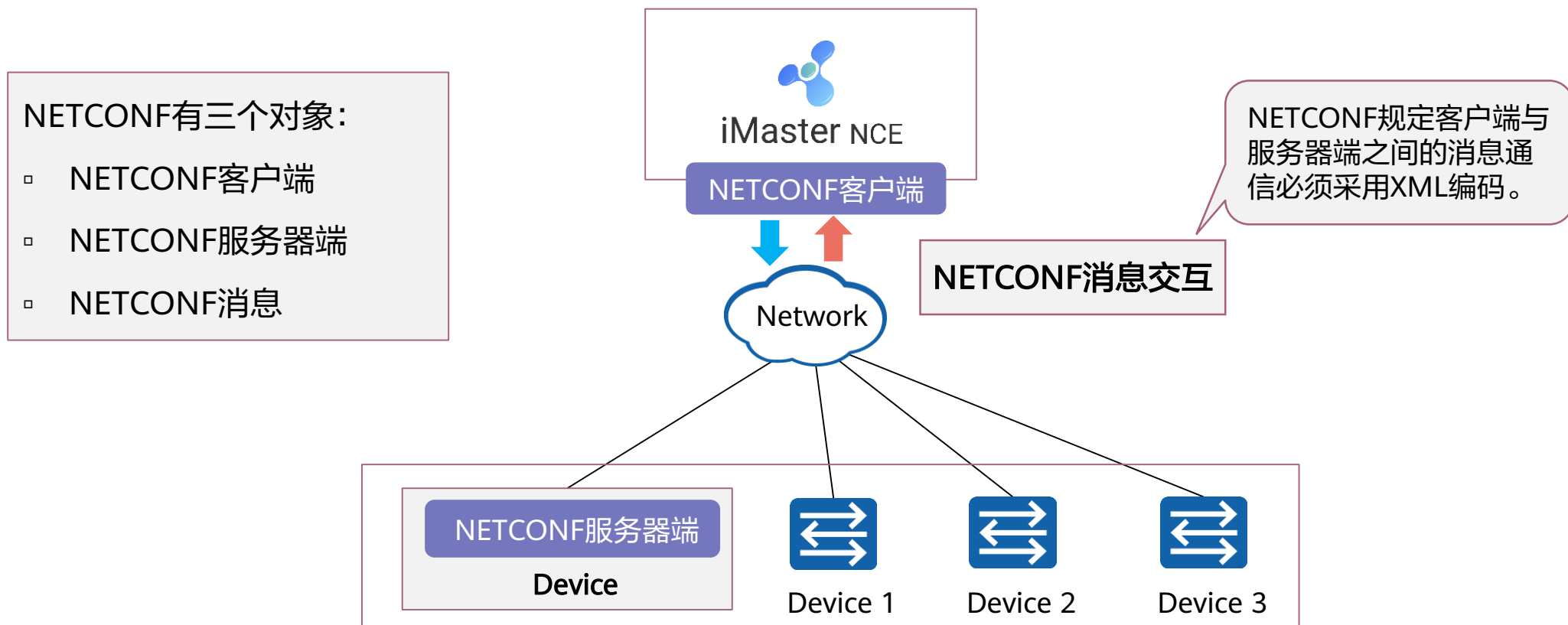
- 华为iMaster NCE是一款集管理、控制、分析和AI智能功能于一体的网络自动化与智能化平台。



- 在管理与控制方面，iMaster NCE支持：
 - CLI和SNMP等传统技术实现传统设备的管理和控制。
 - NETCONF（基于YANG模型）协议实现对支持SDN的网络的管理和控制。
- iMaster NCE通过SNMP、Telemetry等协议采集网络数据，结合AI算法进行大数据智能分析，通过Dashboard、报表等方式多维度呈现设备及网络状态、帮助运维人员快速发现设备及网络异常情况并处理，保障设备和网络的正常运作。

NETCONF简介

- NETCONF（Network Configuration Protocol，网络配置协议），提供一套管理网络设备的机制。用户可以使用这套机制增加、修改、删除网络设备的配置，获取网络设备的配置和状态信息。



NETCONF的优势

功能	NETCONF	SNMP	CLI
接口类型	机机接口：接口定义完善、规范、标准，便于接口控制和使用。	机机接口	人机接口
操作效率	高：基于对象建模，对象操作一次交互即可，支持过滤、批量等操作。	中	低
扩展能力	可以扩展协议私有能力。	弱	一般
事务处理	支持：试运行、出错回滚、配置回退等事务处理机制。	不支持	部分支持
安全传输	多种安全协议：SSH，TLS，BEEP/TLS，SOAP/HTTP/TLS	仅SNMPv3支持	支持SSH

一次典型NETCONF交互



iMaster NCE

SSH连接



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>
      XML格式的配置内容
    </config>
  </edit-config>
</rpc>
```

本操作为修改配置

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>
```

修改成功

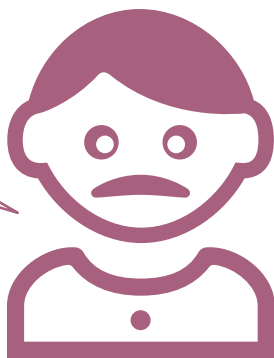
YANG语言概述

- YANG（Yet Another Next Generation）是一种数据建模语言，实现了NETCONF数据内容的标准化。
- YANG模型定义了数据的层次化结构，可用于基于NETCONF的操作。建模对象包括配置、状态数据、远程过程调用和通知。它可以对NETCONF客户端和服务端之间发送的所有数据进行一个完整的描述。

模型（Model）是对“事物”的一种抽象和表达。

数据模型（Data Model）是对数据特征的抽象和表达。

姓名、性别、身高、
体重、年龄、肤色.....



人

接口、路由协议、IP
地址、路由表.....



路由器

YANG与XML (1)

- 在NETCONF客户端（例如网管平台/SDN控制器）加载YANG文件。
- 通过YANG文件将数据转换为XML格式的NETCONF消息发送到设备。

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

YANG文件

+

```
name="smtp"  
ip=192.0.2.1  
port=25
```

```
name="http"  
ip=192.0.2.1  
port=
```

```
name="ftp"  
ip=192.0.2.1  
port=
```

数据

=

```
<server>  
  <name>smtp</name>  
  <ip>192.0.2.1</ip>  
  <port>25</port>  
</server>  
<server>  
  <name>http</name>  
  <ip>192.0.2.1</ip>  
</server>  
<server>  
  <name>ftp</name>  
  <ip>192.0.2.1</ip>  
</server>
```

XML

YANG与XML (2)

- 在NETCONF服务器（例如路由器/交换机等）加载YANG文件。
- 通过YANG文件将接收到的XML格式的NETCONF消息转换为数据并做后续处理。

```
<server>
  <name>smtp</name>
  <ip>192.0.2.1</ip>
  <port>25</port>
</server>
<server>
  <name>http</name>
  <ip>192.0.2.1</ip>
</server>
<server>
  <name>ftp</name>
  <ip>192.0.2.1</ip>
</server>
```

XML

+

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

YANG文件

=

```
name="smtp"
ip=192.0.2.1
port=25
```

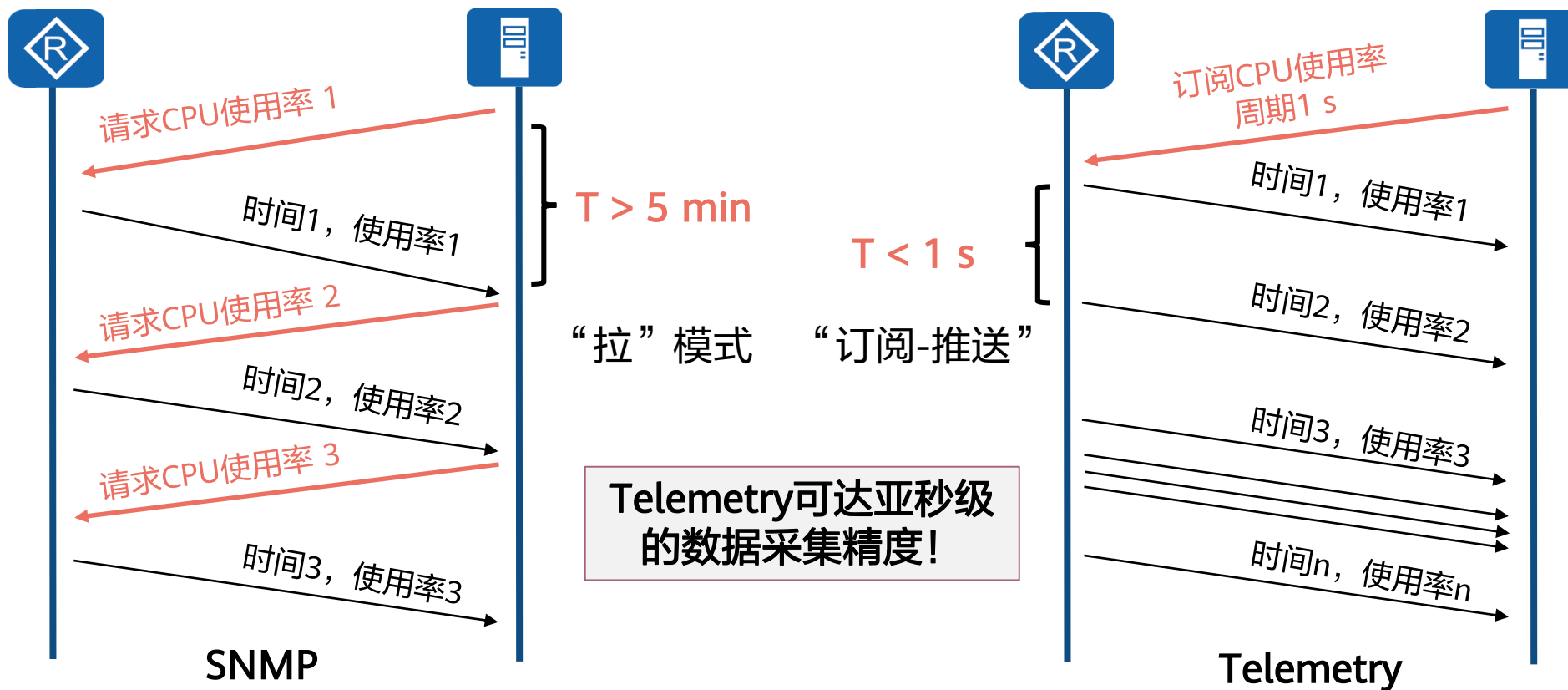
```
name="http"
ip=192.0.2.1
port=
```

```
name="ftp"
ip=192.0.2.1
port=
```

数据

Telemetry基本概述

- Telemetry也作Network Telemetry，即网络遥测技术，是一项远程地从物理设备或虚拟设备上高速采集数据的技术。
- 设备通过推模式（Push Mode）周期性地主动向采集器上送设备的接口流量统计、CPU或内存数据等信息，相对传统拉模式（Pull Mode）的一问一答式交互，提供了更实时更高速的数据采集功能。



本章总结

- 随着网络技术不断发展，网络的管理与运维手段也越来越多，常见的有：
 - CLI或Web方式
 - SNMP协议方式
 - 通过华为iMaster NCE “管-控-析” 智能化运维平台方式