第八章 网络管理和网络安全

8.1 网络管理

（1） 网管概述

目的：对组成网络的各种硬软件设施的综合管理，以达到充分利用这些资源的目标。

必要性：

单机性能问题：软件本身、系统设置和配置，系统工具+人工；

网络性能问题：影响因素众多，网络应用、网络流量、设备的运行状况等；

设备的分布性，需要相应的工具协助管理员—网络管理。

网络规模扩展，意义日益显著。

实质：对各种网络资源状态及其使用进行监测、控制和记录，并在网络出现故障时，及时报告和处理，向管理员报警，以便尽快维护。

关键：获取网络设备的工作状态；

标准：网络设备的异构性导致标准化的需求。

ISO/OSI网络管理标准—公共管理信息协议（CMIP）；

因特网网络管理标准—简单网络管理协议（SNMP）。

（2） ISO OSI网络管理的体系结构

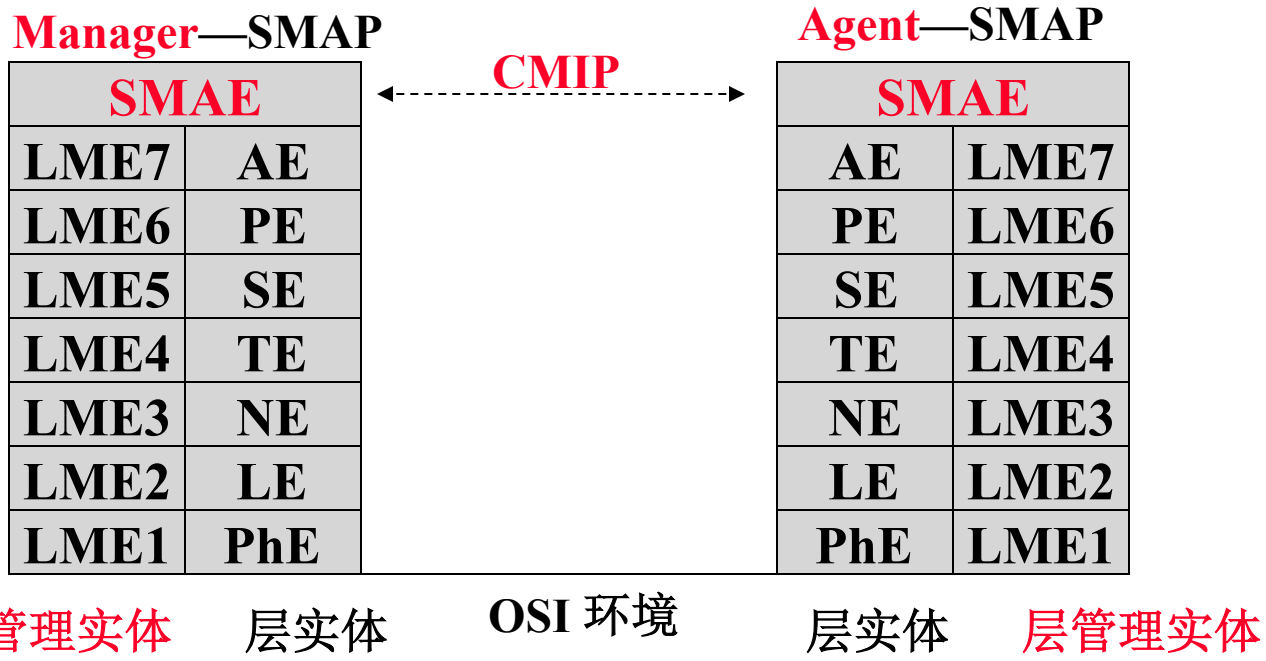
OSI的资源具有层次的概念，OSI管理也涉及这些层次。系统管理应用实体SMAE收集系统信息。

ISO/OSI的SMAE分管理员和代理两类实体：

管理员：负责对整个网络的资源进行管理；

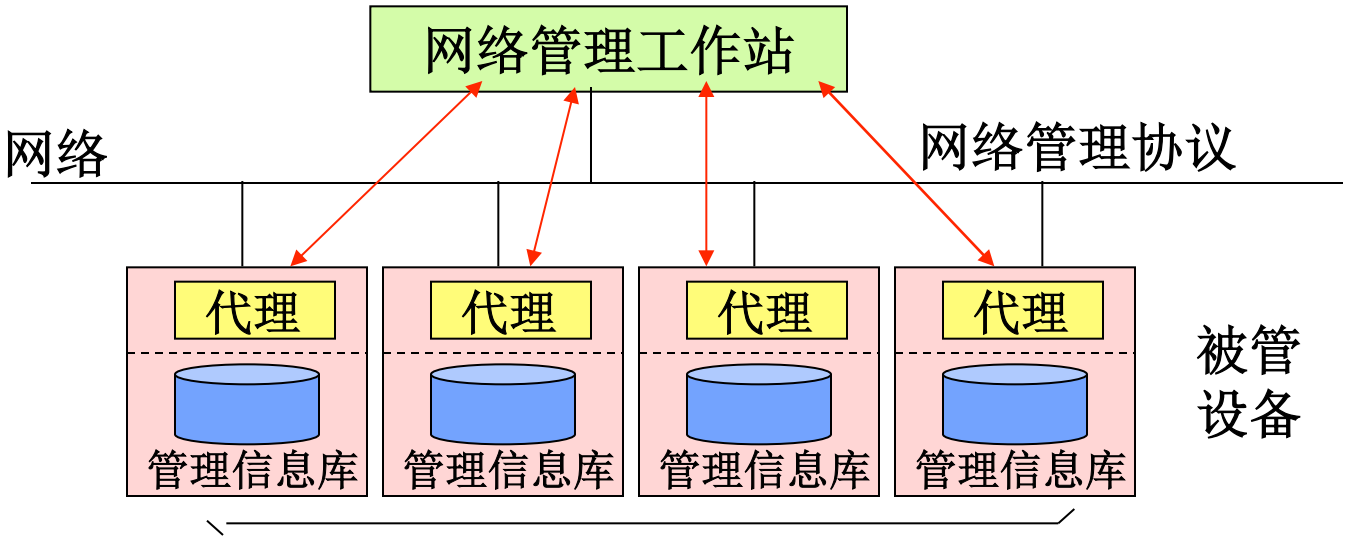
代理：驻留在被管对象上，响应管理员的指令。

管理员和代理之间遵循公共管理信息协议（CMIP）。



ISO 10164/10165定义了OSI管理的标准，目前仅在电信网中部分应用。

（3） 网络管理的基本模型



网络管理工作站：通过网络向各种被管网络设施发出各种控制命令，并对被管设备反馈的信息进行汇总分析。

被管设备：网络交换结点、集中器、线路设备、用户结点等；运行在被管设备上的相关软件（代理）负责响应网络管理工作站的命令，将被管设备的信息通过网络管理协议提供给管理工作站，包括主动监测和记录故障并报于管理工作站。

管理信息库：保存为OSI管理目的而收集的信息。

（4） 网络管理的功能— ISO OSI定义

性能管理：收集和统计网络系统的数据（如网络的吞吐量、用户响应时间和网络资源的利用率等)，以便根据统计信息来评价网络资源的使用等系统性能，分析系统资源的使用趋势，或者平衡系统资源的负载。

故障管理：对网络设备进行监控，包括故障检测、隔离和恢复；必要时通知系统管理员，进行人工干预。

配置管理：定义、监测和管理系统的配置参数，使得网络资源可用、性能较优。

安全管理：资源的授权管理、访问控制管理、安全检查跟踪和事件处理、密钥管理（密钥分配）等。

计费管理：记录网络资源的使用情况，统计已被使用的网络资源和估算用户应付的费用；

性能管理

- 性能管理是优化服务质量的需要。它定义了网络的动态评估方法，以便于检验网络所保持的服务水平，确定实际的和潜在的网络性能瓶颈。根据网络的各项运行指标的趋势，为制定和规划管理决策产生报告。性能管理还包括了为操作控制建立和维护性能数据库和自动操作程序，随机或定时收集由统计数据产生的性能日志。

- 这些日志除了性能管理本身使用外，其它管理功能亦可充分加以利用：
  - 故障管理应用性能日志检测故障；
  - 配置管理根据性能日志决定何时需要改变配置；
  - 计费管理应用性能日志调整计费策略。

IPPM and ITU-T Relevant Recommendations

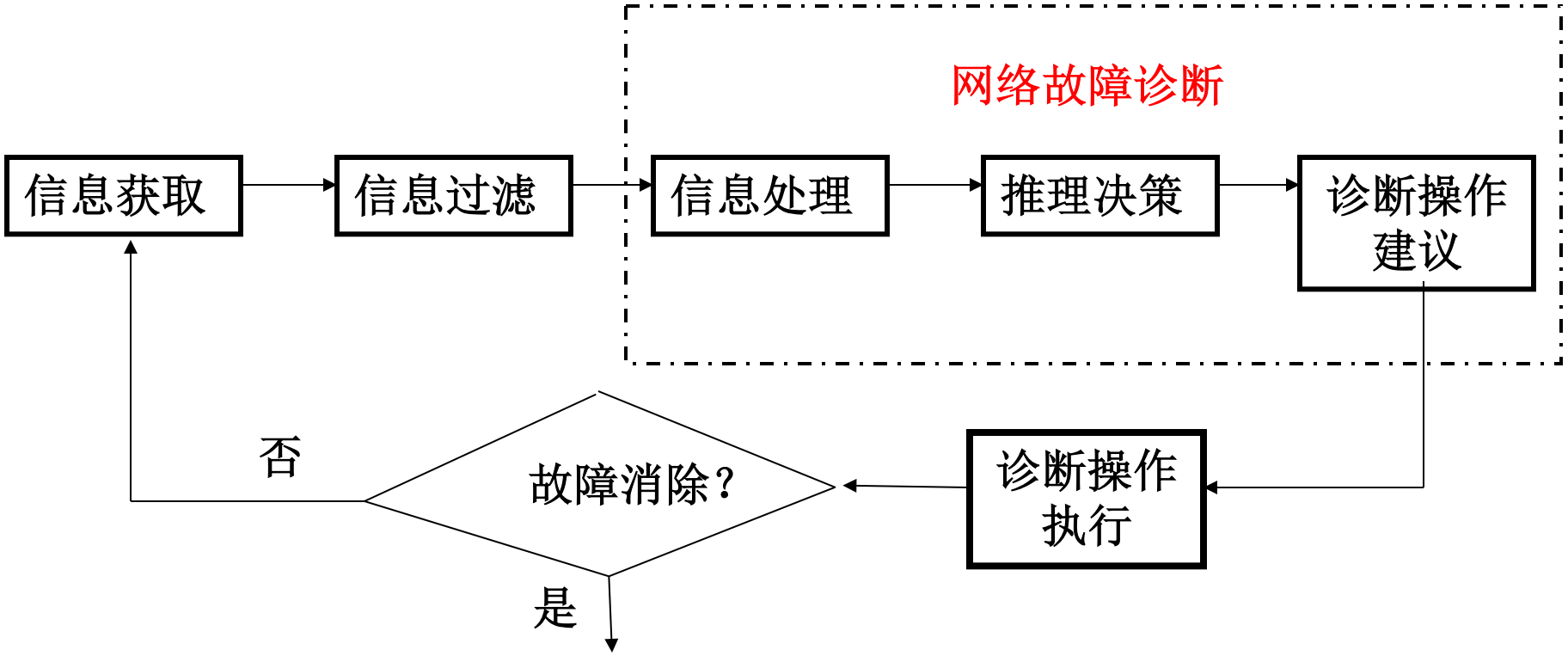
- Series Y: Global information infrastructure and Internet protocol aspects.
  - Quality of service and network performance is given in Y.1500–Y.1599 especially in Y.1540
- IPPM(IP Performance Metrics)
  - Framework for IP Performance Metrics (RFC 2330)
  - IPPM Metrics for Measuring Connectivity (RFC 2678)
  - A One-way Delay Metric for IPPM (RFC 2679)
  - A One-way Packet Loss Metric for IPPM (RFC 2680)
  - A Round-trip Delay Metric for IPPM (RFC 2681)
  - A Framework for Defining Empirical Bulk Transfer Capacity Metrics (RFC 3148)
  - One-way Loss Pattern Sample Metrics (RFC 3357)
  - IP Packet Delay Variation Metric for IPPM (RFC 3393)
  - Network performance measurement for periodic streams
  - A One-way Active Measurement Protocol Requirements (RFC 3763)

故障管理

- 故障管理是对系统非正常操作的操作管理。所谓故障就是那些引起系统以非正常方式操作的事件，可分为
  - 由损坏的部件或软件故障（bug）引起的（内部）故障，常常是可重复的;
  - 由环境影响引起的外部故障，通常是突发的，不可重复。

- 故障管理的主要内容有
  - 故障检测：维护和检查故障日志，检查事件的发生率看是否已（或将）成为故障；接收故障报告。
  - 故障诊断：寻找故障发生的原因，可执行诊断测试，以寻找故障发生的准确位置。
  - 故障纠正：将故障点从正常系统中隔离出去，并根据故障原因进行修复。
- 故障管理为操作决策提供依据，以确保网络的可用性。

网络故障管理过程



配置管理

- 配置管理的目的是通过定义、收集、管理、和使用配置信息，以及网络资源配置的控制来最佳地维持网络环境所提供的服务质量。
  - 被管对象（组）的标识管理
  - 被管对象的初始化/关闭
  - 系统当前状态信息的采集
  - 系统参数的更新
- 配置管理的基本任务
  - 拓扑发现
  - 资产清单管理
  - 资源和业务管理

拓扑发现的基本概念

- **网络元素**：指主机、路由器、交换机、网关、网桥、集线器等网络构成单元。
- **网络拓扑结构**：指网络元素及它们之间的连接关系。
- **网络物理连接关系**：指网络元素间有线或无线的物理连接方式。
- **网络逻辑连接关系**：指网络元素间依照某种网络协议进行通信时所表现出来的逻辑上的连接关系。
- **网络拓扑发现**：利用计算机软件自动识别网络元素之间的物理或逻辑连接关系，确定网络的拓扑结构。
  - 发现管理域结构
  - 发现网络层结构
  - 发现链路层结构

拓扑信息收集

- 基于ARP协议－取ARP表信息
- 基于ICMP协议－Ping
- 基于DNS－Zone Transfer
- 基于SNMP、OSPF、RIP等协议－取相应的路由表信息

安全管理

- 安全管理用于保证降低运行网络及其网络管理系统的风险。它是一些功能组合，通过分析网络安全漏洞将网络危险最小化。
- 实施网络安全规划，可动态地确保网络安全。
- 主要包括维护防火墙和安全日志、安全指示器的监测、分区隔离、口令管理和提供各种级别的警告或报警。

计费管理

- Metering
  - the way to collect accounting data
- Pricing
  - flat-rate: the customer pays a fixed price regardless of how much data is sent
  - usage-based
  - combination of both
- Charging
  - based on some business models
- Billing
  - process of paying

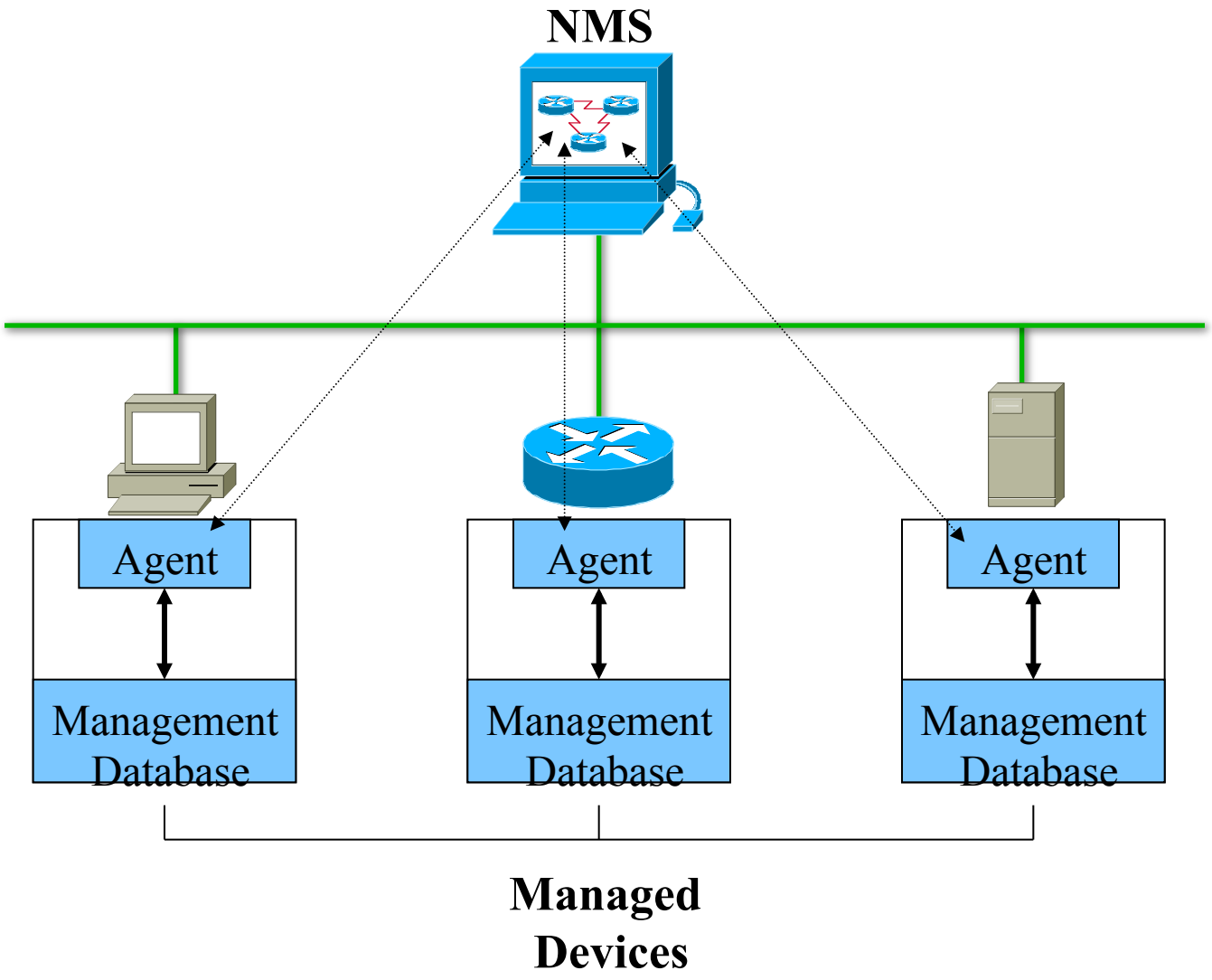
Internet Accounting

- Flat-rate
  - 测量和管理都简单，易于实现
  - 可能导致小部分的用户消耗掉大部分资源
- Usage-based
  - 测量和管理都复杂，很难实现
  - 鼓励使用者更有效地利用资源
  - 将使Internet从提供尽力而为服务转变成提供不同等级的服务
- 微支付 Micro-Charge
  - 支付单位小，响应快
  - 例如收费网页

Network Management Components

- A **managed device** is a network node that collects and stores management information
- An **agent** is network-management software that resides in a managed device
- A **network-management system (NMS)** runs applications to display management data, monitor and control managed devices, and communicate with agents

Network Management Architecture



Architecture Concerns

- In-band versus out-of-band monitoring
  - In-band is easier to develop, but results in management data being impacted by network problems
- Centralized versus distributed monitoring
  - Centralized management is simpler to develop and maintain, but may require huge amounts of information to travel back to a centralized network operations center (NOC)

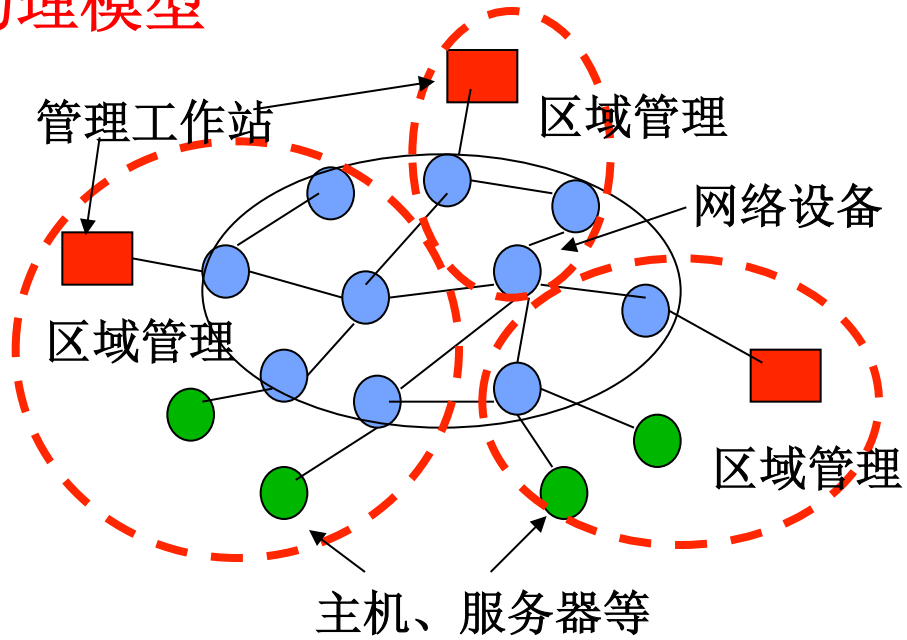
（5） 网络管理实例—因特网网络管理

★ 网络管理模型

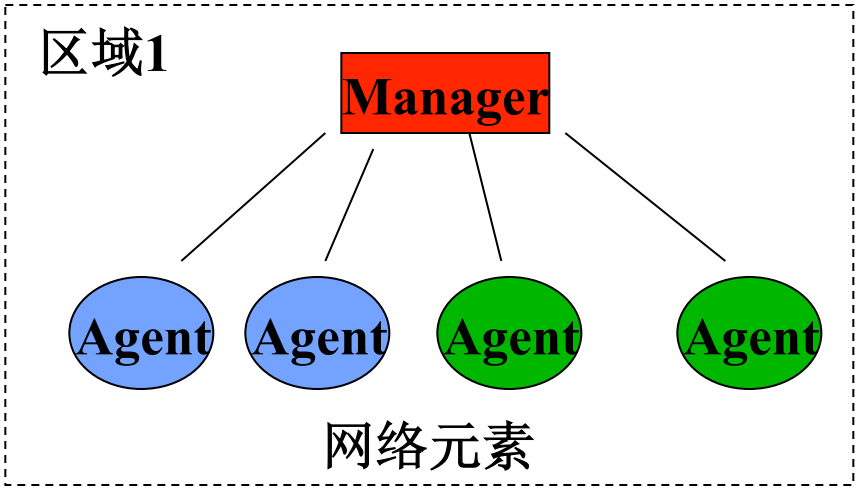
网络管理体系模型由一系列网络管理站点和网络元素（被管对象包括主机、网络部件等）构成；前者监控网络元素的状态，后者借助管理代理（Agent）执行网络管理的指令；

为提高管理效率，引进分区域管理（分布式管理）概念。

物理模型



逻辑模型



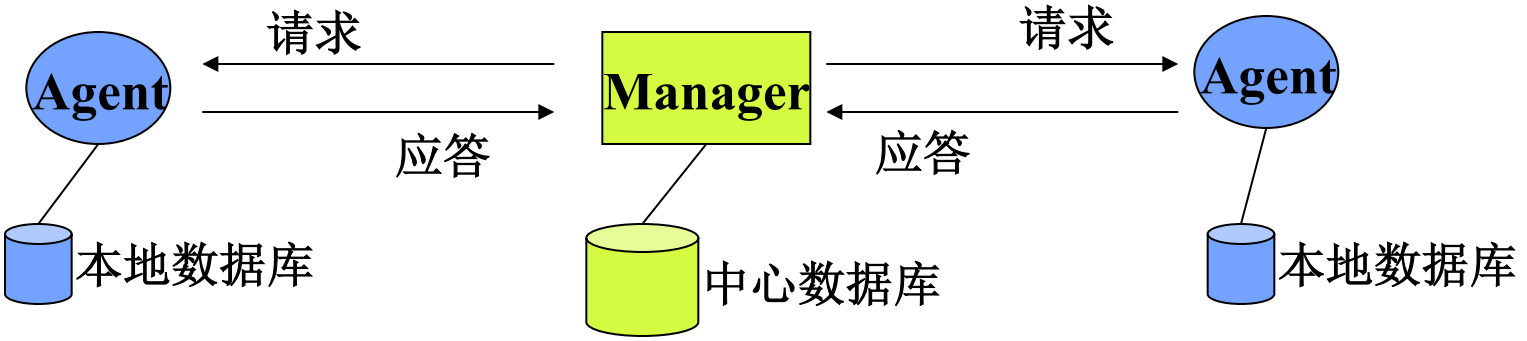
★ 因特网网络管理的工作方式

管理员和代理之间主要以请求/应答方式工作；
管理员向代理发出“请求”指令，获取或者设置网络元素的参数；
代理向管理员返回“应答”响应，报告“请求”的执行结果；

为了使一个管理员可以管理多个代理，常采用“轮询”的方式；

为了使得管理工作可以延续，管理员和代理分别维护全局和本地数据库（习惯上称管理信息库—MIB）。

本地数据库保存结点的参数及运行状况；
中心数据库保存全网（或者区域）的设备参数等。



★ 因特网网络管理协议—简单网络管理协议（SNMP）

☆ 相关标准

为支持管理员和代理之间的管理信息的交换，IETF成立两个工作组，从两个方面定义因特网管理的标准。

管理信息库（MIB）工作组负责定义MIB的元素及结构（交换的对象）；

网络管理协议（SNMP）工作组定义不同厂商的设备之间交换的协议（交换的方式和格式）；

1990年，SNMPv1（RFC1157）和MIBv1（RFC1156）；

1996年，SNMPv2（RFC1905）和MIBv2（RFC1904）

—目前大部分网络设备均支持该版本；

1998年，SNMPv3（RFC2273）和MIBv3（RFC2272）。

☆ 简单网络管理协议（SNMPv1—RFC1157）

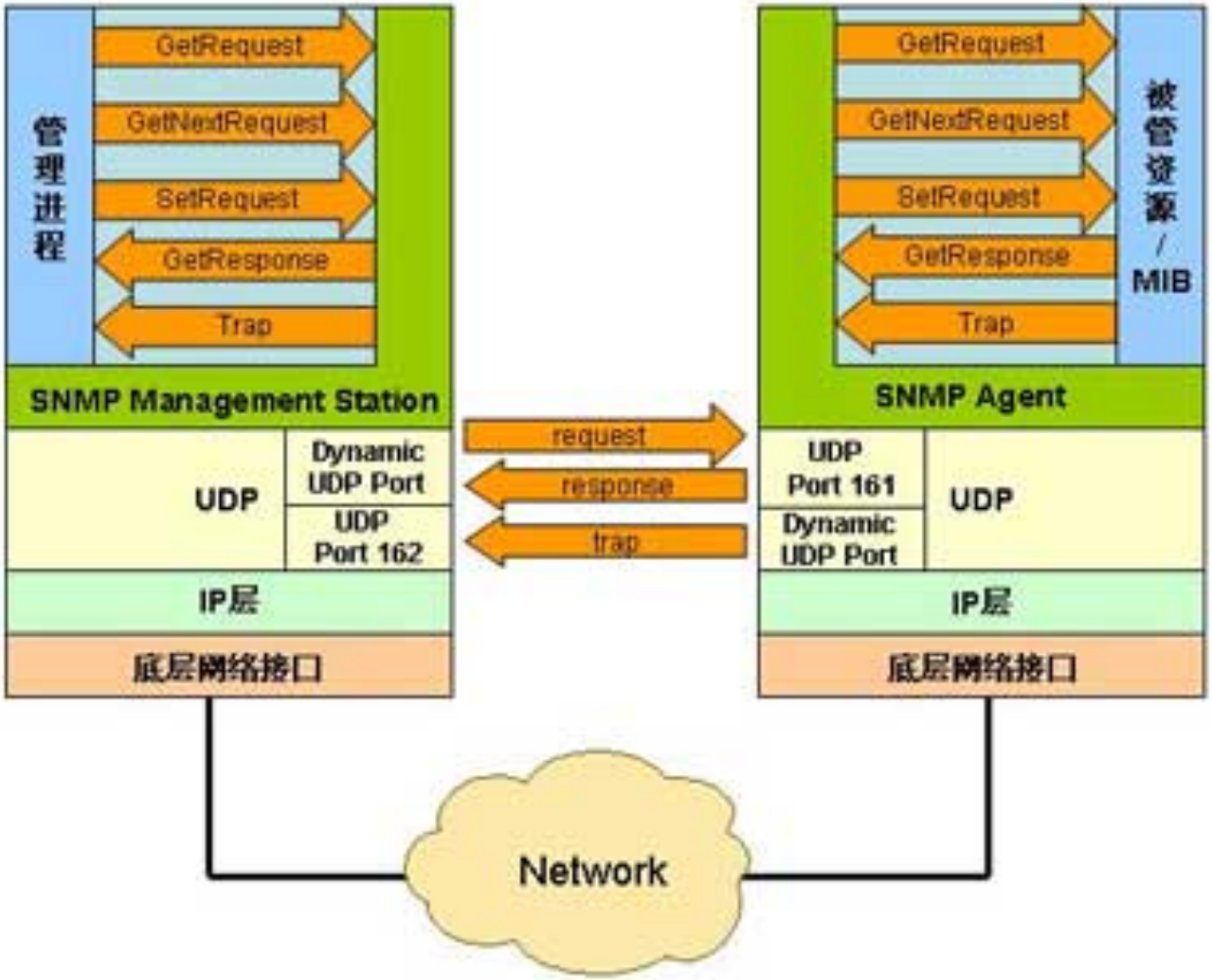
SNMP作用于应用层，利用UDP的两个端口（161和162）实现管理员和代理之间的管理信息交换。

UDP端口161用于数据收发，UDP端口162用于代理报警；

SNMPv1（RFC1157）采用集中管理模式，一个管理员轮询管理多个代理；

管理员/代理之间交换五种类型的PDU：

名称	编码	功能说明
GetRequest	0	管理员至代理，查询指定变量的值；
GetNextRequest	1	管理员至代理，查询下一变量的值；
GetResponse	2	代理至管理员，回送执行结果（正确/差错）；
SetRequest	3	管理员至代理，设置代理维护的某个变量的值；
Trap	4	代理至管理员，主动传递报警信息。



SNMPv1模型示意图

- SNMP的作用范围称为域（Community），只有域内的 NMS和管理代理之间才能进行SNMP协议交互，从而控制网络管理信息的流动范围。
- 为了使用 SNMP具有通用性，除了要求使用标准的网管协议进行信息交互外，还要求交换的信息具有标准的语义，因此 SNMP对 MIB的定义有一个公共集合，即对被管对象定义标准的状态变量集，同时也允许实现者定义附加的状态变量。从这个意义上说， SNMP既有一致性测试问题，也有互操作性测试问题。

1．命令类型

- 如果NMS要控制某个被管设备，可以发送一个命令要求被管设备改变其某个或多个变量的数值。NMS与被管设备之间的交互命令有以下五种：
  - Get-Request/Response－NMS通过读取由被管设备维护的各种变量来监视被管设备
  - Set-Request－NMS通过写存贮在被管设备中的各种变量来控制被管设备
  - Get-Next-Request－与Get-Request一起使用可使NMS在被管设备的变量表中（如IP路由表）收集信息
  - Trap－被管设备利用Trap异步地向NMS报告各种确定的事件

SNMP的报文格式

Version	Community	PDU type	Request ID	0	0	Name X	Value X	……

(a) Get-Request, Get-Next-Request, Set-Request

Version	Community	PDU type	Request ID	Error status	Error index	Name X	Value X	……

(b) Get-Response

Version	Community	PDU type	Enterprise	Agent addr	Generic trap	Specific trap	Time	Name X	Value X

(c) Trap

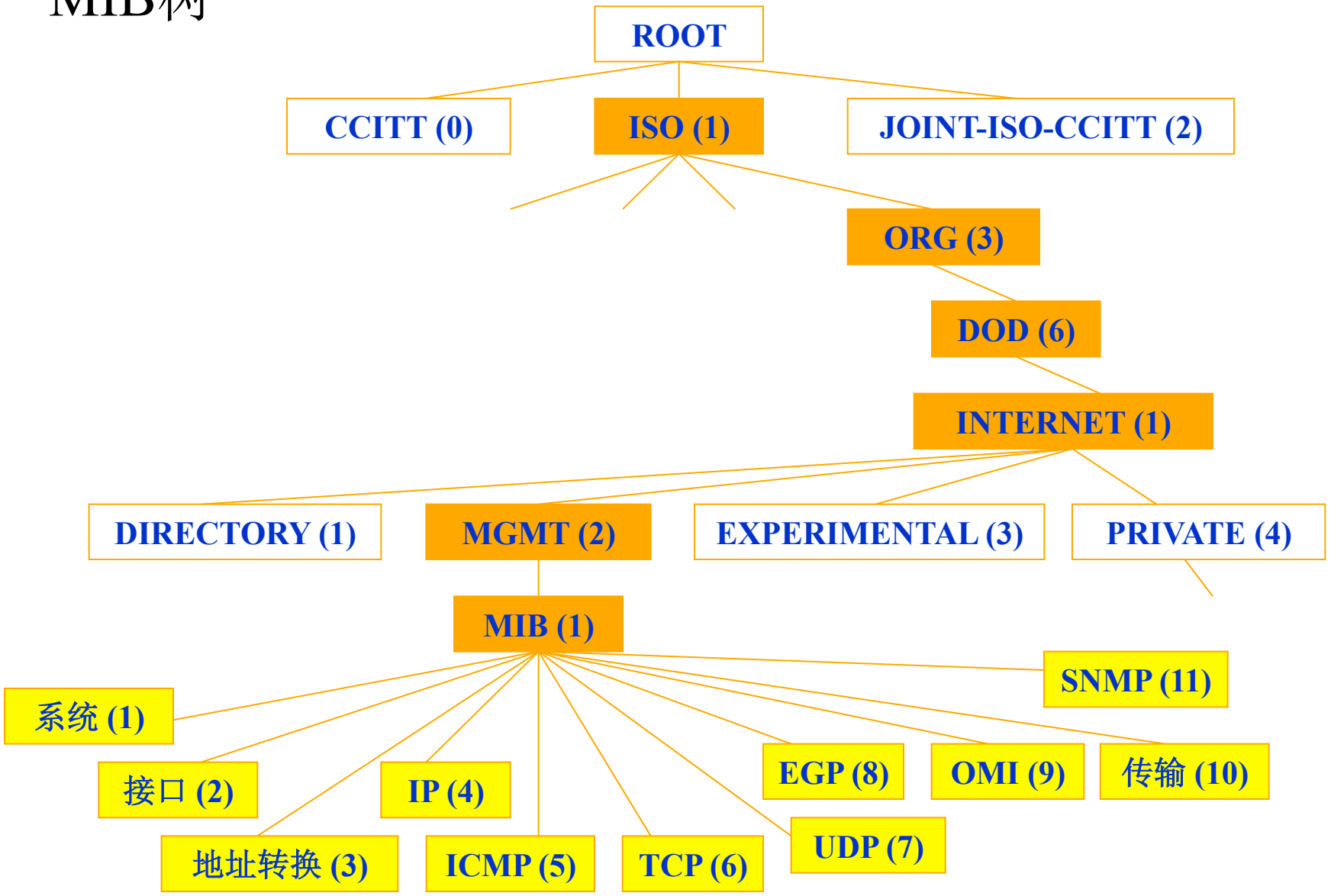
SNMP Trap types

- Coldstart of a system - *可能有配置改变*
- Warmstart of a system - *无配置改变*
- Link down
- Link up
- Failure of authentication
- EGP neighbor loss
- Enterprise specific

2. MIB与对象标识符

- 管理信息库（MIB）可以描述为一棵抽象树，树的根没有名字，各个数据项组成了树的叶节点。对象标识符（OID）唯一地标识或命名了树中的各种MIB对象。对象标识符类似于电话号码系统结构，不同的组织和机构有层次地分配了特定的数字组成了这些对象标识符。

MIB树


ROOT
CCITT (0)
ISO (1)
JOINT-ISO-CCITT (2)
ORG (3)
DOD (6)
INTERNET (1)
DIRECTORY (1)
MGMT (2)
EXPERIMENTAL (3)
PRIVATE (4)
MIB (1)
SNMP (11)
系统 (1)
接口 (2)
IP (4)
EGP (8)
OMI (9)
传输 (10)
地址转换 (3)
ICMP (5)
TCP (6)
UDP (7)

- SNMP MIB的对象标识符结构定义了三个主要分枝：CCITT负责分枝0，ISO管理分枝1，CCITT和ISO联合管理分枝2。
- 目前多数MIB的活动发生在ISO分枝部分，ISO将它的分枝分给了几个组织，其中将子树1给了美国国防部（DOD），DOD用它作为Internet对象表示。这样在Internet子树中，对象标识符以1.3.6.1开头,意思是它们属于ISO，ORG，DOD，Internet子树，专门用于Internet范围。
- Internet子树有四个分枝：Directory（1）、Mgmt（2）、Experimental（3）和Private（4）。Directory计划用于OSI目录；Mgmt用于IAB承认的被管对象的定义；Experimental用于Internet网络实验；Private用于专用MIB的定义。

- 目前在RFC1213中定义的Internet标准MIB和MIB－II包含了171个对象。这些对象按照协议（包括TCP，IP，UDP，SNMP和其它）和其它类项（包括“系统”和“接口”）进行分组。
- MIB树可以扩展为实验和专用分枝。没有标准化的那些MIB往往被放置在实验分枝。厂商可以定义自己的专用分枝来包括其产品的各种实例。例如，Cisco的专用MIB的对象标识符是1.3.6.1.4.1.9，该标识符包括了许多对象，如用OID 1.3.6.1.4.1.9.2.2.1.51来标识对象“HostConfigAddr”。它说明了为一台具体的Cisco设备提供主机配置文件的主机的地址。
- IP信息类变量标识为1.3.6.1.2.1.4;

  GetRequest（1.3.6.1.2.1.4）表示取IP相关的信息；

  GetNextRequest（1.3.6.1.2.1.5）表示取ICMP相关的信息；

3．不同的数据表示法

- 被管网络中的信息交换会因为被管设备所采用的数据表示技术的不同而产生麻烦，因此要设法在这些异构设备通信时消除这些不兼容性，统一使用一种语法表示法可以使不同种类的计算机共享管理信息。
- SNMPv1应用了ISO的开放系统互连抽象语法表示法1（ASN.1）的一个子集，它以与机器无关的形式对MIB的变量进行描述。
- 被管对象之间可存在多种关联关系，例如分级或表格，而变量是被管对象在MIB中的对应表示。例如，主机中当前活动的TCP连接就是一个被管对象，对于MIB而言每个特定的连接是这个变量的一个值。
- 变量及其值构成了MIB的内容。

☆ SNMP信息分类

编码	类（组）别	内 容 描 述
1	系统类	元素名称、厂商、硬件类型、软件版本、启停时间等
2	接口类	网络元素的接口数目、带宽、流量等
3	地址迁移类	物理地址和网络地址（如IP地址）对应关系等
4	IP信息类	进、出、丢弃IP数据报统计，IP地址及掩码、路由信息等
5	ICMP统计类	ICMP报文的统计信息，含出错分类统计
6	TCP信息类	TCP连接数、收发TCP报文统计，重发算法及次数统计等
7	UDP信息类	收发的UDP报文统计
8	EGP信息类	支持外部网关协议（EGP）的路由器的流量统计信息
9		待扩充
10		待扩充
11	SNMP信息类	SNMP报文统计信息

SNMPv2

1. 概述

- 与 SNMPv1相比，SNMPv2在管理信息结构(SMI)、协议操作、管理体系结构、以及安全性等方面均有较大的改进。
- SNMPv2支持多域的分布式管理结构。一些系统既可以用管理员的身份操作，也可以用代理的身份操作。当以代理身份操作时，它执行上一级管理系统的命令，这些命令可能是要求访问存储在本地的 MIB，或者是要求该系统以中间管理者的身份提供有关下一级代理的概要信息。另外，中间管理者还可向上一级管理者发送报警信息。

- SNMPv2引入了一种信息模型的概念，它描述了一组相关的定义。主要有三种信息模型：
  - MIB模型—包含了相互关联的被管对象的各种定义。
  - MIB模型的一致性描述—提供了一个系统性方法描述必须实现的被管对象组。
  - 代理实现的性能描述—定义了代理要求的相关MIB分枝所提供信息的精确程度。这些描述表明了有些对象具有语法约束或扩充以及访问控制级别。对代理性能作规范性描述有助于改善和优化各设备之间的互操作性，如果管理系统能够描述与每个代理之间相互关系，则该系统就能够调整其动作来优化自身资源，并且能合理使用代理和网络的资源。

2. 协议操作

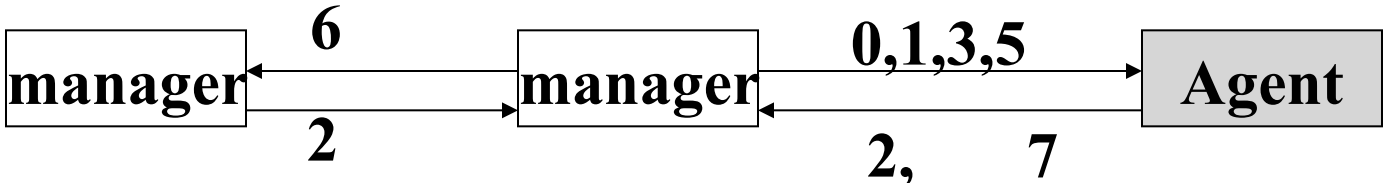
- SNMPv2定义了两种新的操作：
  - Inform－允许一管理者向另一管理者发送trap类信息并要求其返回一个响应。
  - Get-bulk－允许管理者有效地获取大块数据，例如一次可读取一张表的多行数据项，而不是将表分成多个小块数据再进行传输。

- SNMPv2除了响应get之外，get-next、set和 trap操作与SNMPv1相同。在v1中，如果发出响应的代理不能提供表中变量的值，那么它就提供不了任何其它值。在SNMPv2中，即使不能为所有变量提供所需数值，也预备了一张变量赋值表。如果变量与一个意外条件相关联，则该变量包括了该意外条件的名称。

☆ 简单网络管理协议（SNMPv2—RFC1905）

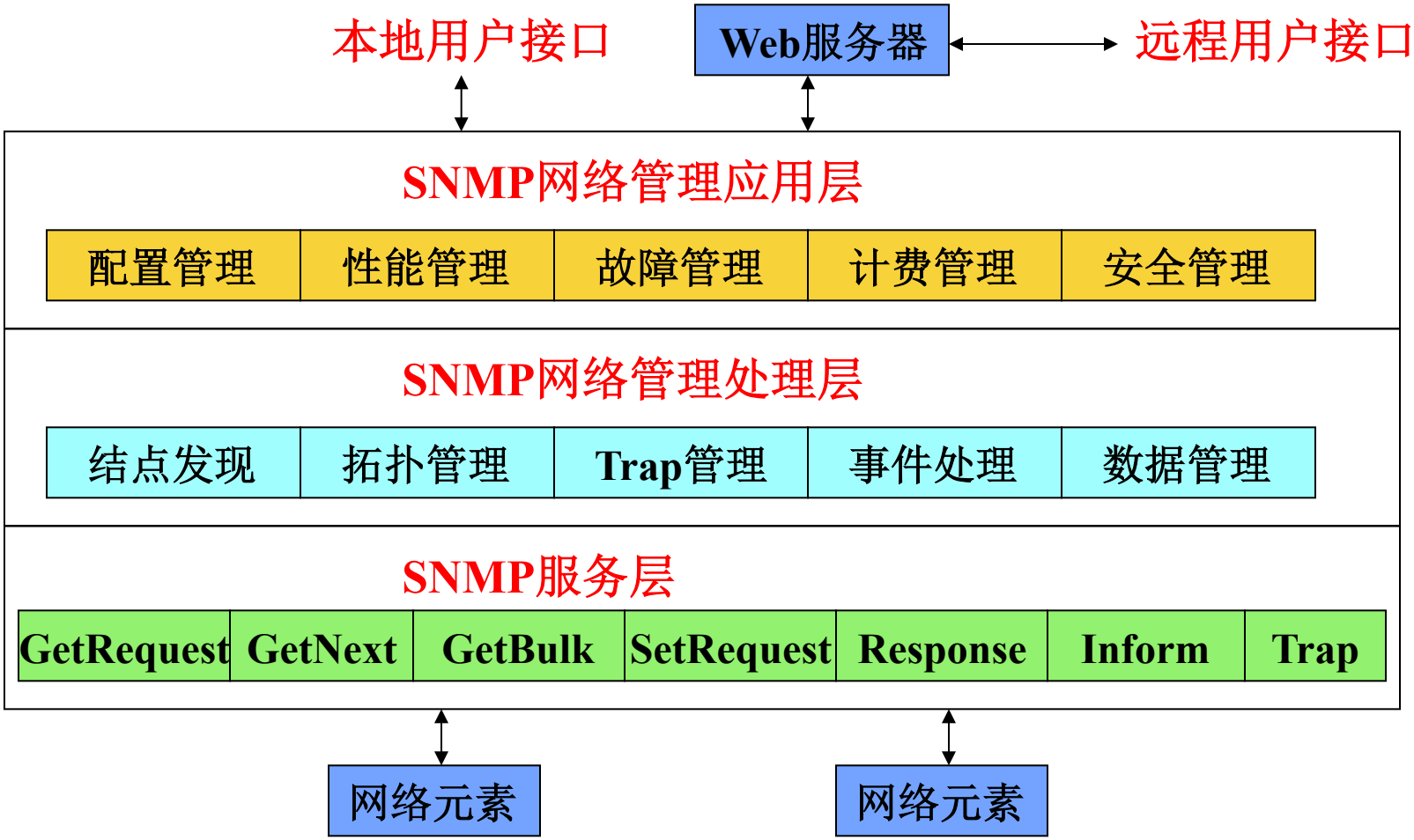
SNMPv2引进区域管理（分布式管理）的思想，扩充了管理员之间的操作。并用Snmpv2-Trap取代了原Trap报警PDU。

名称	编码	功能说明
GetRequest	0	管理员至代理，查询指定变量的值；
GetNextRequest	1	管理员至代理，查询下一变量的值；
Response	2	至管理员，回送执行结果（正确/差错）；
SetRequest	3	管理员至代理，设置代理维护的某个变量的值；
GetBulkRequest	5	管理员至代理，传递批量信息；
InformRequest	6	管理员至管理员，传递参数处理请求；
SNMPV2-Trap	7	代理至管理员，传递报警信息；（取代原4）
Report	8	待定义



☆ SNMP产品的一般结构

SNMP仅定义了网络元素的参数传递，如何利用这些参数为人类管理员服务是产品追求的目标。



3. 安全性

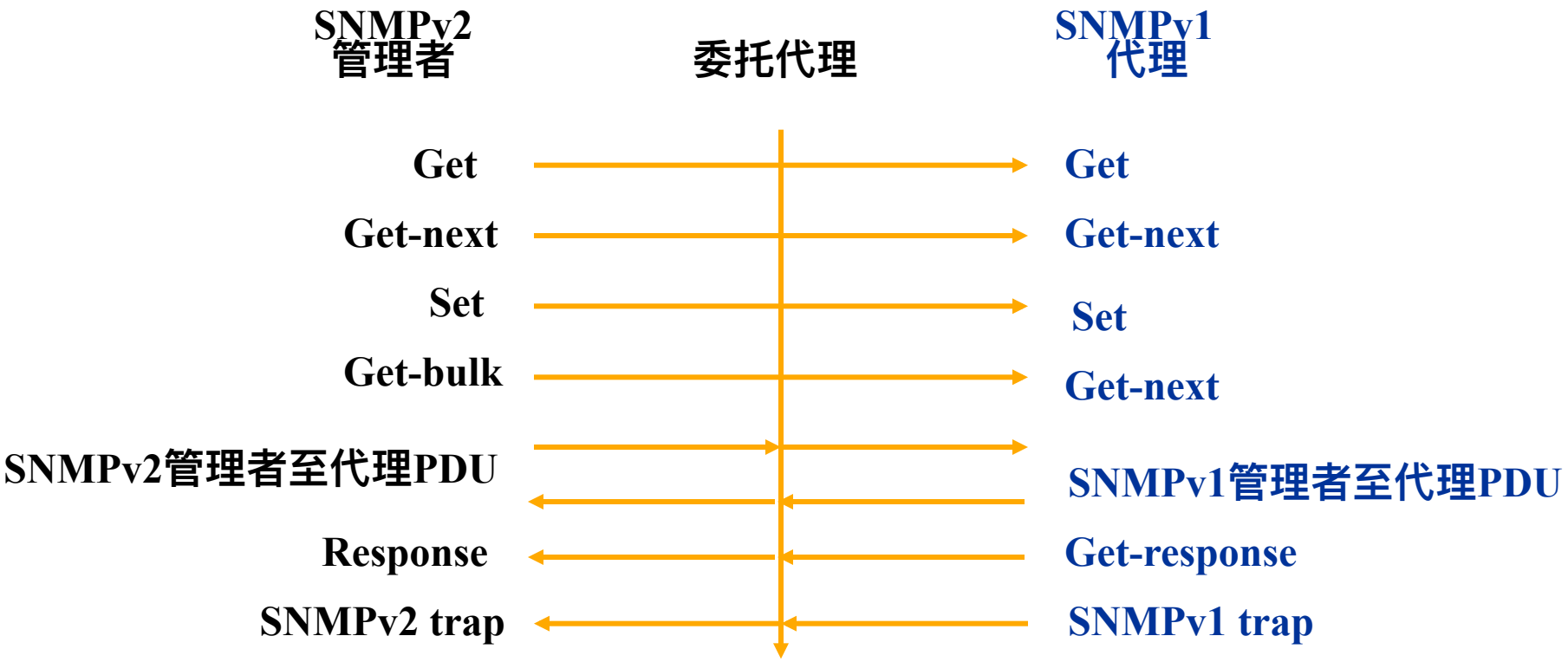
- SNMPv2提供了防止下列破坏行为的安全设施：
  - 假冒－ 一个未经授权的实体假冒授权实体来执行管理操作；
  - 信息的改变－ 一个实体可能改变由授权实体所产生的信息，该信息可导致某些未授权的管理操作，如改变配置或计费信息等；
  - 信息顺序和时间的改变－ 由于 SNMPv1是在无连接传输上进行操作的，因此实体可以重排序、延时或拷贝，然后重新执行某个报文，如导致重启某台设备；
  - 泄密－ 实体可以通过窃听被管对象和管理员中间的信息交换来学习被管对象的值和通知事件的发生。

- 为实现这些安全性，SNMPv2提供了三种报文：
  - 非安全的— 未采用任何 SNMPv2提供的安全功能；
  - 鉴别但未加密— 采用某种密钥体制计算报文的信息摘录，以此实现对报文的鉴别，但密钥体制的确定，以及密钥的分配和管理不在本协议中；
  - 鉴别且加密— 采用某种密钥体制对报文进行鉴别和加密。
- 时标是管理员和代理之间时钟松散同步（loosely synchronized）的维护机制，使信息的接收方可发现被回放的报文，并能够对收到的报文进行定序。

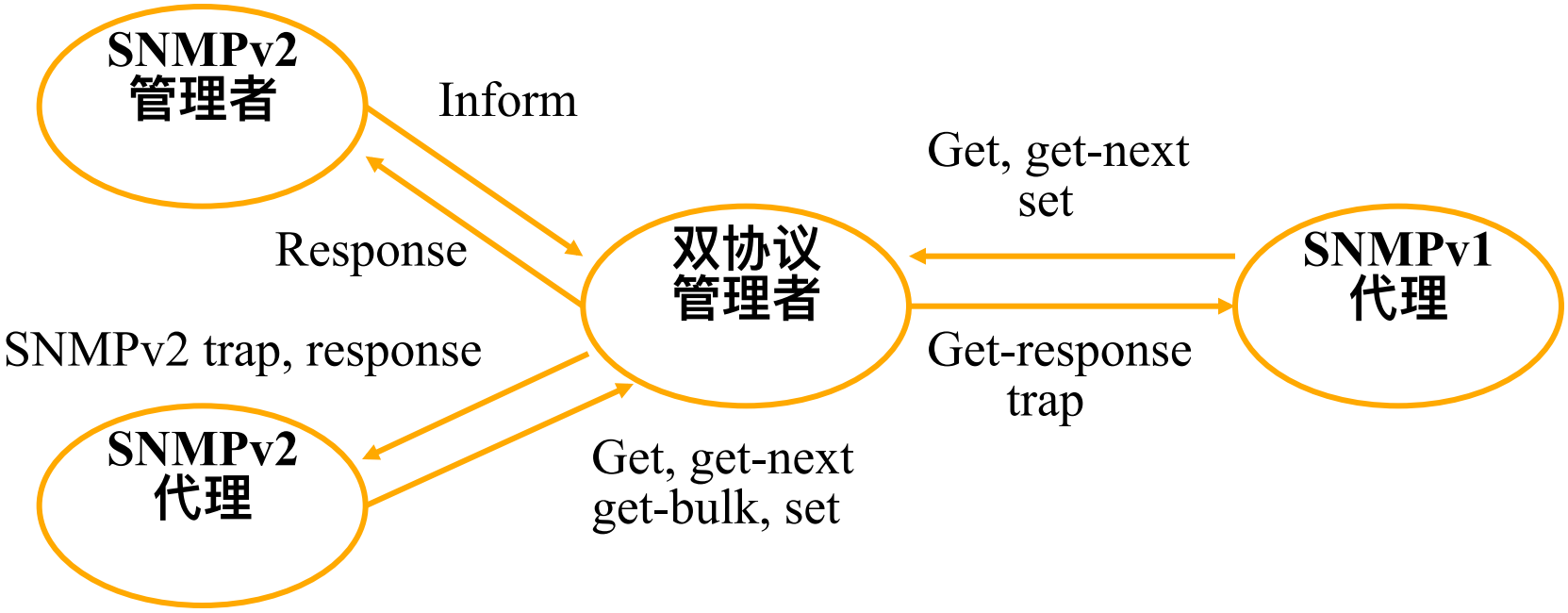
4. 互操作性

- 新的信息格式、协议操作和安全特性使 SNMPv2 与 SNMPv1不一致，但由于 SNMPv1已被大量使用，因此必须需求这两个协议版本（主要是 SNMPv2的管理员、SNMPv2的代理、和 SNMPv1代理）之间的共存和过渡方法。互操作性问题主要涉及以下两个方面：
  - 管理信息— SNMPv2的 SMI可看作是 SNMPv1的 SMI的一个超集，因此对一个代理而言，它可将 SNMPv1的 MIB保持不变，并共存于 SNMPv2的环境。
  - 协议操作— 两个协议的 PDU大部分兼容，但 SNMPv2扩展了新操作。

- 协议共存的方法有两种。
- 一种是通过委托代理来实现两个协议版本不同操作之间的转换；



- 另一种是通过一个能同时支持这两个协议版本的双语管理员来与不同版本的代理交互。



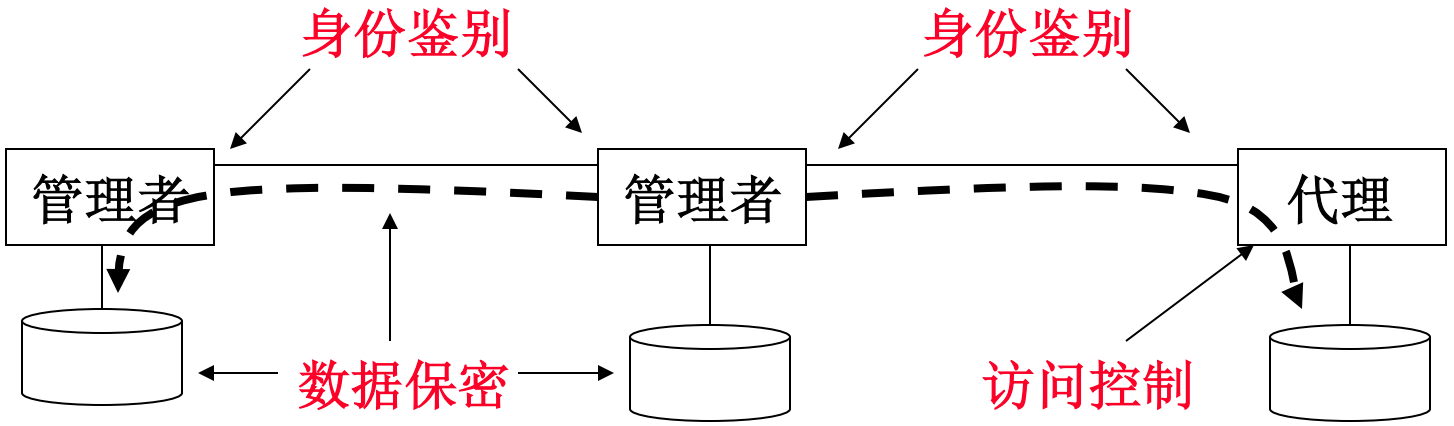
☆ 简单网络管理协议（SNMPv3—RFC2273）

在SNMPv2的基础上，扩充相关安全功能；

身份鉴别：实体鉴别，确保收到的指令或者数据来自于真实的实体；

数据保密：MIB信息存储保密和PDU传输保密，确保指令或者数据不被截取、伪造、篡改和重放；

访问控制：实体授权和访问控制，禁止越权或者非授权操作。

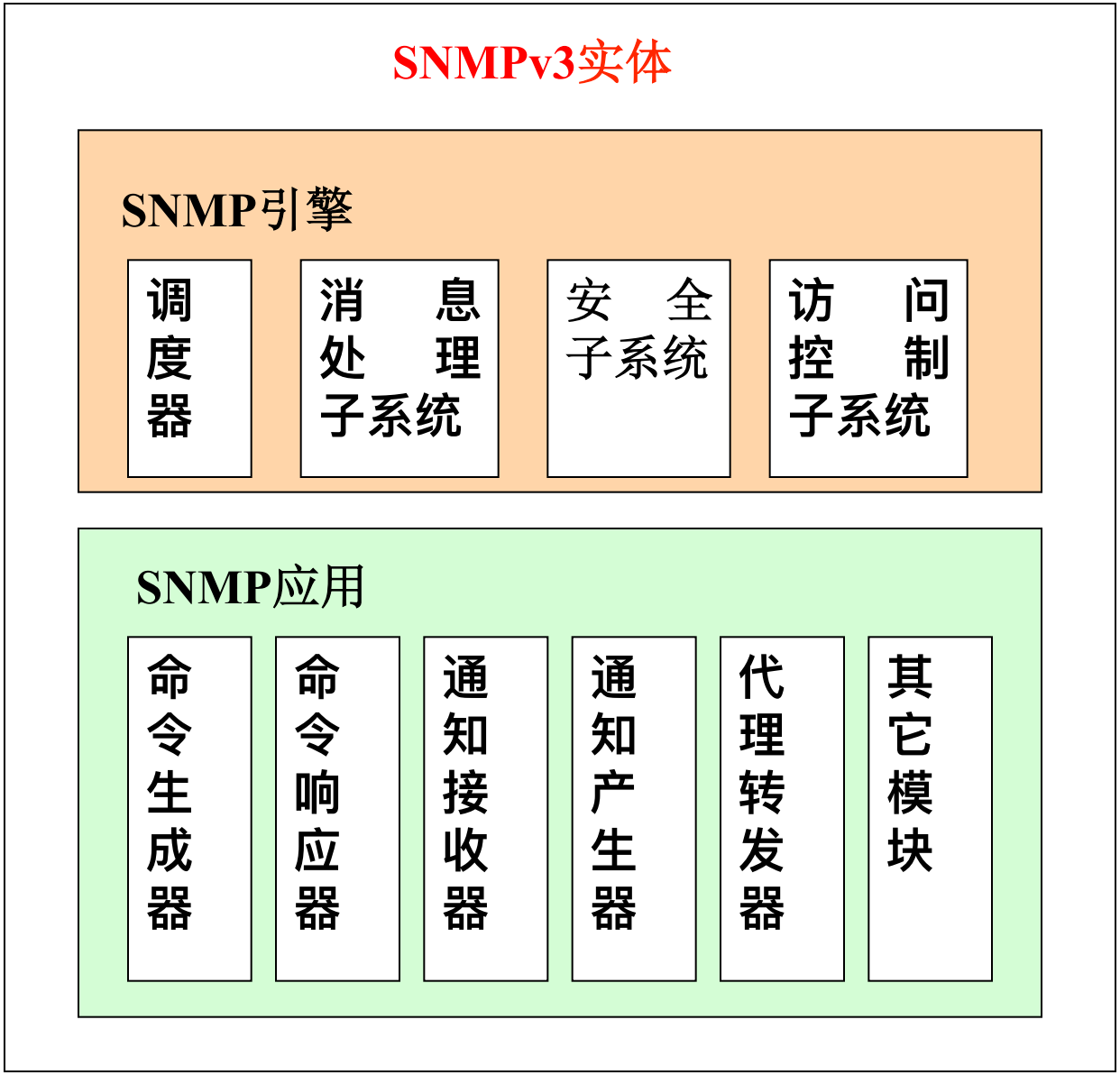


热点：智能化网络管理系统（引入人工智能的思想）。

SNMPv3

- RFC2570 Introduction to Version 3 of the Internet-standard Network Management Framework. April 1999.
- RFC2571 An Architecture for Describing SNMP Management Frameworks. April 1999.
- RFC2572 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). April 1999. (Obsoletes RFC2272)
- RFC2573 SNMP Applications. April 1999.(Obsoletes RFC2273)
- RFC2574 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). April 1999. (Obsoletes RFC2274)
- RFC2575 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). April 1999.(Obsoletes RFC2275)
- RFC2576 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework. March 2000. (Obsoletes RFC1908, RFC2089)

- 重点突出了模块化的概念
- 以尽量小的代价定义了一个适用于所有*SNMP*版本的较为完善的体系结构
- 可以针对不同环境的需要提供不同的安全方案


SNMPv3实体
SNMP引擎
调度器
消息处理子系统
安全子系统
访问控制子系统
SNMP应用
命令生成器
命令响应器
通知接收器
通知产生器
代理转发器
其它模块

SNMP引擎

- SNMP引擎为发送和接收消息、鉴别和加密消息、控制对被管对象的访问等活动提供服务，具体包括
  - 调度器：为多个版本的消息处理系统分派任务，并为不同的应用提供发送和接收PDU的服务；并进行有关SNMP消息以及被管对象处的SNMP引擎的统计数据收集工作。
  - 消息处理子系统：负责准备要发送的消息以及从收到的消息中抽取数据；它可以包含多个模块，分别处理不同版本的SNMP消息。
  - 安全子系统：提供消息的鉴别与保密等服务。
  - 访问控制子系统：通过一个或多个访问控制模型来约束对被管对象的访问活动。

SNMP引擎ID

- 在一个管理域中，每个引擎都有一个唯一和明确的标识符，称为SNMP引擎ID。由于SNMP引擎与实体之间一一对应，因此SNMP引擎ID也可以用来标识SNMP实体。

0	厂商ID *1~4字节*	厂商定义的方法 *第5字节*	该方法的功能 *6~12字节*

SNMPv1和SNMPv2的引擎ID

1	厂商ID *1~4字节*	格式指示符 *第5字节*	格式 *长度可变*

SNMPv3的引擎ID

标识指示符	格式	标识指示符	格式
0	保留	3	MAC地址，6 bytes
1	IP地址，4 octets	4	文本，<= 127 bytes
2	IPv6地址，16 octets	5	字节串，<= 27 bytes

SNMP应用

- 监测和操纵管理数据的命令产生器
- 对管理数据提供访问的命令接收器
- 发出异步消息的通知产生器
- 处理异步消息的通知接收器
- 在实体之间转发消息的代理转发器
- 定制的管理功能模块

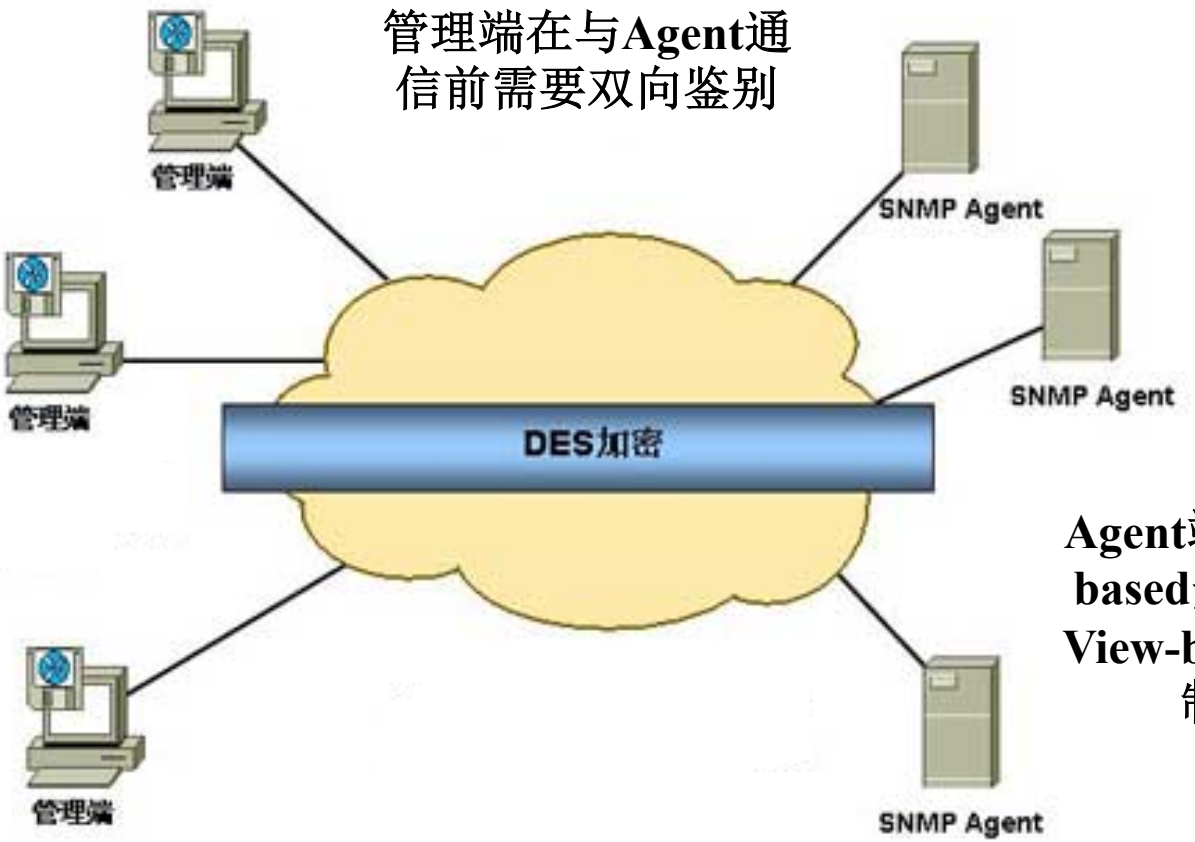
SNMPv3实体

- 网络中所有的管理者和被管节点都必须包含一个SNMP实体，其中包括一个SNMP引擎和一个或多个SNMP应用；管理者和被管对象通过实体之间的交互来实现对网络资源的监控和管理。
- 根据所拥有的SNMP应用的不同，SNMP实体可分为
  - SNMP代理实体（最小化实体）：包含一个或多个命令接收器和/或通知产生器；
  - SNMP中级管理者（dual-role实体）：包含命令产生器和/或通知接收器，命令响应器和/或通知产生器，或代理转发器；
  - SNMP管理服务器：包含命令产生器和/或通知接收器。

SNMPv3的安全性

管理端在与Agent通信前需要双向鉴别

报文使用DES加密传输



Agent端实现User-based安全模型和View-based访问控制模型

基于用户的安全模式USM

- 安全目标
  - 对收到的每个SNMP消息进行鉴别检查，确认其数据完整性；
  - 对提供对发送消息的用户的身份认证功能，防止冒充；
  - 提供适时性检查，防止消息的重定向、延迟和回放；
  - 提供消息内容的保密功能。

基于用户的安全模式USM

- 安全功能
  - 鉴别：包括数据完整性和数据源鉴别功能，所使用的协议可以是(散列消息鉴别码)HMAC-MD5-96，或者HMAC-SHA-96(安全散列算法)，其中前者是必备的。如果系统具有鉴别模块，则一定要进行完整性检查。
  - 加密：对消息的净负荷进行加解密操作，首选的算法是DES-CBC。USM规定如果使用了这个功能，则一定要使用鉴别功能。
  - 适时检查：通过在SNMP消息中放置一个适时值来对消息的回放和延迟进行保护。如果消息在以该值为中心的某个窗口（缺省是150s）内到达，则认为是适时的。该功能与鉴别功能同时使用。

CBC密文分组链接，加密算法的输入是上一个密文组和下一个明文组的异或。

基于视图的访问控制模型VACM

- 与SNMPv1和SNMPv2所使用的Community概念不同，SNMPv3使用组的概念来进行访问控制；
- 组是一个由零到多个<安全模式，安全名>对构成的有名集合，通过各个安全模式定义了属于该组的所有安全名的访问权限；要求每个<安全模式，安全名>对只能属于一个组。
- 一个组的成员可以定义不同的安全级别，包括无认证无保密性检查，认证但无保密性检查，和认证并作保密性检查等。
- 通过MIB视图的概念来定义一个组可访问的网管数据，并根据对应的管理功能确定特定的可标识的上下文。
- VACM的访问控制策略就是对于一个特定的组的特定上下文使用特定的安全模式和安全级别，而具体的管理活动是根据上下文的约束对指定的MIB视图进行的。

SNMP分析

- SNMP提供了标准的网管数据采集功能，使得网管系统与被管网络可以分离。
- SNMP的设计思想是尽量减少关联信息库、信息访问协议以及代理的实现等方面的复杂性，因为在资源受限的设备环境内处理实时管理任务时，简单性是非常重要的。
- SNMP的简单数据结构和众多的MIB变量限制了网管系统的处理效率，缺乏数据粒度控制能力。
- SNMP的主从控制结构限制了可扩展性，因此移动代理和主动网管技术受到关注。

Remote Monitoring (RMON)

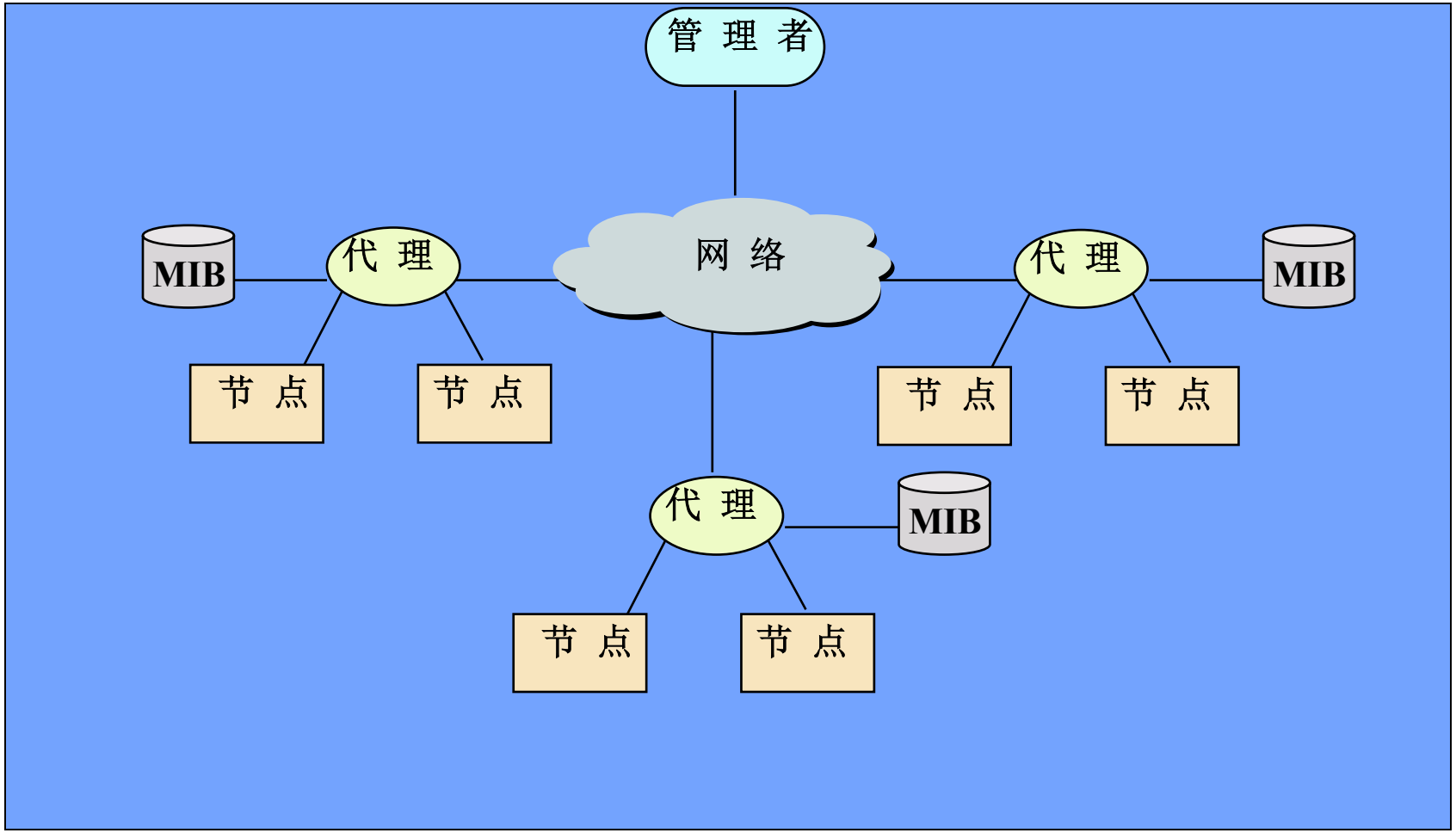
- Developed by the IETF in the early 1990s to address shortcomings in standard MIBs
  - Provides information on data link and physical layer parameters
  - Nine groups of data for Ethernet
  - The statistics group tracks packets, octets, packet-size distribution, broadcasts, collisions, dropped packets, fragments, CRC and alignment errors, jabbers, and undersized and oversized packets

RMON组	功能	元素
统计量	包括探测器为该设备每个监控的接口测量的统计值。	数据包丢弃、数据包发送、广播数据包、CRC错误、大小块、冲突以及计数器的数据包。范围从64~128、128~256、256~512、512~1024以及1024~1518字节。
历史	定期地收集统计网络值的记录并为日后处理把统计存储起来。	例子的周期、数目和项。提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。
告警	定期从探测器的变量选取统计例子。并与前面配的阈值相比较。	告警类型、间隔、阈值上限、阈值下限
主机	包括网络上发现的与每个主机相关的统计值。	主机地址、数据包、接收字节、传输字节、广播传送等。
HostTopN	准备描述主机的表，根据一个统计值排序列表。	统计值、主机、周期的开始和结束、速率基值、持续时间。
真值表	记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储起来。	源地址和目的地址对、数据包、字节和每一对的错误。
过滤器	允许监视器观测与一过滤器相匹配的数据包。	字节过滤器类型、过滤器表达式等。
捕获包	数据包在流过一个信道之后被捕获。	捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。
事件	提供关于RMON代理所产生的所有事件的表。	事件类型、描述、事件最后一个发送的时间

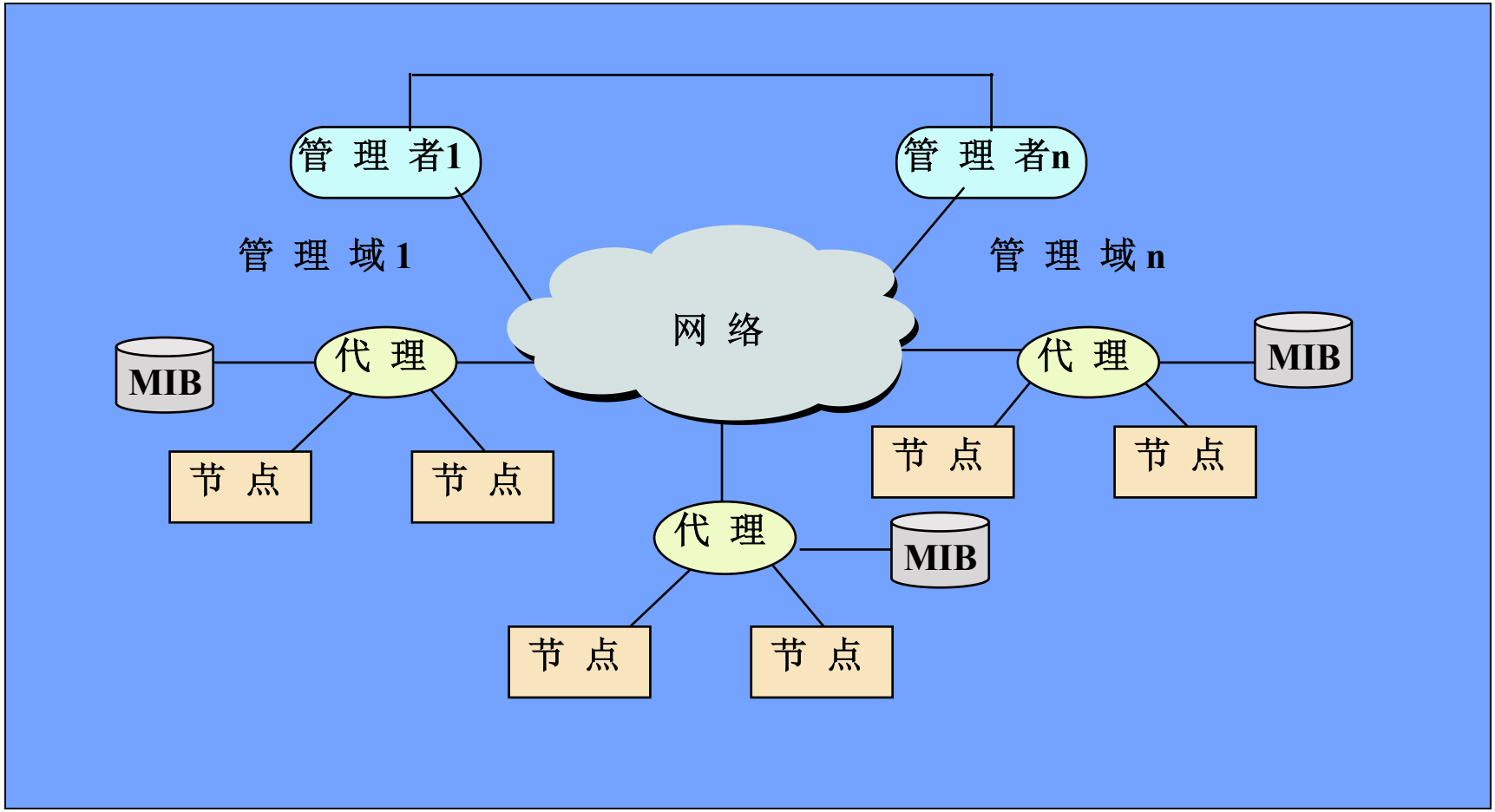
网络管理系统的各种实现结构

- 随着技术的不断进步，出现了许多使用不同实现方案和结构的网络管理系统，流行的有四种方式：
  - 集中式
  - 分布式（peer system）
  - 分层结构式
  - 基于Web技术
- 这些系统的不同点主要在于它们所设置的管理者（manager）的数量、相互交互深度以及各自的独立程度。

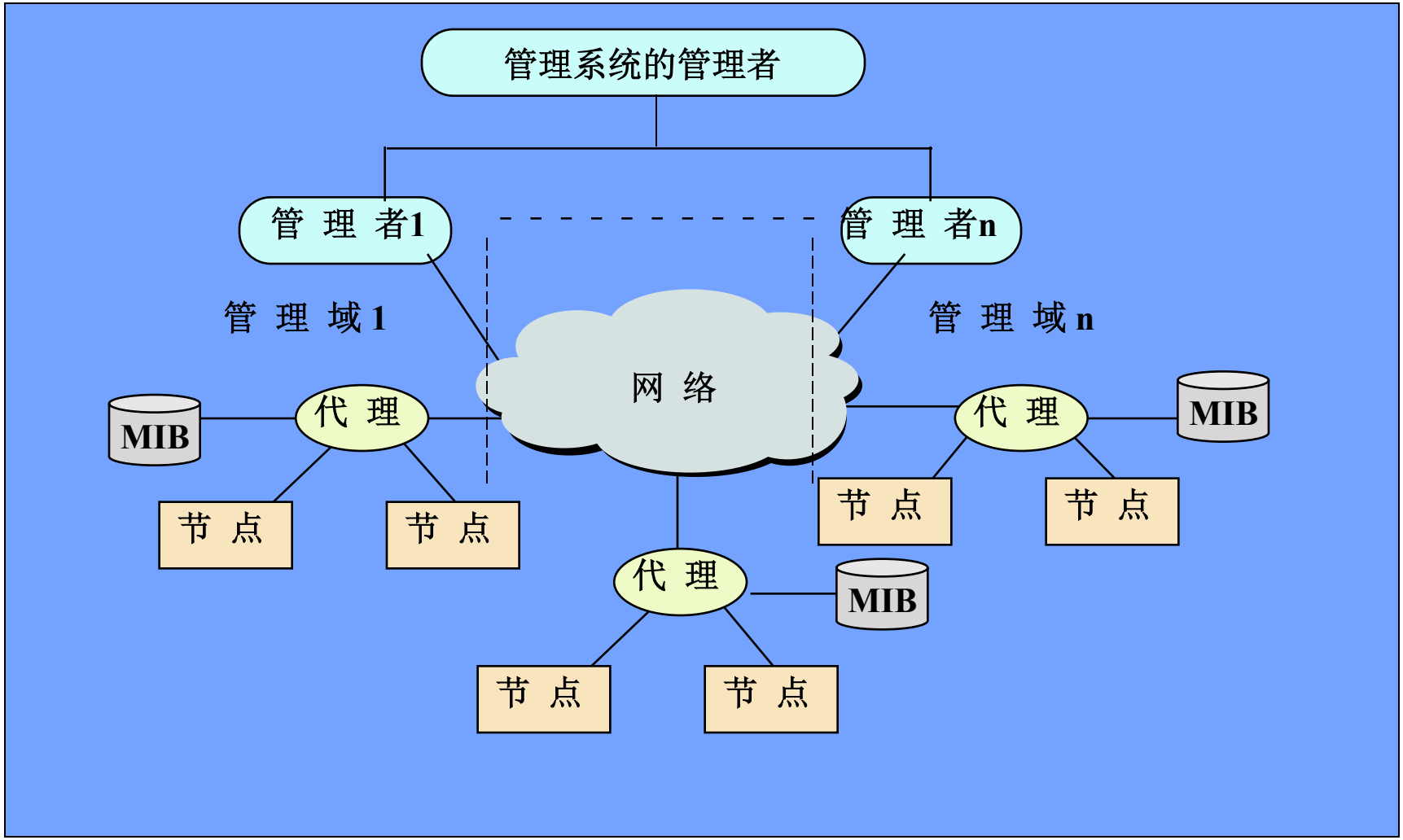
- 集中式结构



- 分布式结构



- 分层结构式


管理系统的管理者
管 理 者1
管 理 者n
管 理 域 1
管 理 域 n
网 络
代 理
代 理
代 理
MIB
MIB
MIB
节 点
节 点
节 点
节 点
节 点
节 点

网络管理系统的实现

- 商用系统
  - 网管平台: IBM, HP, Sun, …
  - 设备厂家自备系统: CiscoWork, D-View, …
- 常用网管工具
  - ping, traceroute, nslookup
- Public domain software
  - MRTG, …
- 新型试验系统

MRTG 图例

- Multi Router Traffic Grapher,
  - by Tobias Oetiker and Dave Rand
  - http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html