

网络管理

学习内容

- 网络管理的概念
- 网络管理的体系结构
- 网络管理的功能

网络管理的概念

- 网络管理是指对网络的运行状态进行监测和控制,并能提供有效、可靠、安全、经济的服务。网络管理完成两个任务,一是对网络的运行状态进行监视,二是对网络的运行进行控制。通过监测了解网络当前状态是否正常;通过控制对网络资源进行合理分配,优化网络性能,保证网络服务质量。因此,网络管理就是对网络的检测和控制。
- 网络管理的目标是使网络的性能达到最优化。最大限度地满足网络管理者 和网络用户队计算机网络的有效性、可靠性、开放性、综合性、安全性和经济性的要求。

●网络管理的对象

被管对象是对网络资源的抽象表示。主要分为两类，即硬件资源和软件资源。

➤ 硬件资源是指物理介质、计算机设备和网络互连设备。物理介质通常是物理层和数据链路层设备，如网卡、双绞线、同轴电缆、光纤等。计算机设备包括处理机、打印机、存储设备和其他计算机外围设备。网络互连设备包括中继器、网桥、交换机、路由器和网关等。

➤ 软件资源主要包括操作系统、应用软件和通信软件。通信软件指实现通信协议的软件，如FDDI、ATM这些网络就大量采用了通信软件保证其正常运行。另外，软件资源还包括路由器软件、网桥软件和交换机软件等。

●网络管理的标准

主要标准:

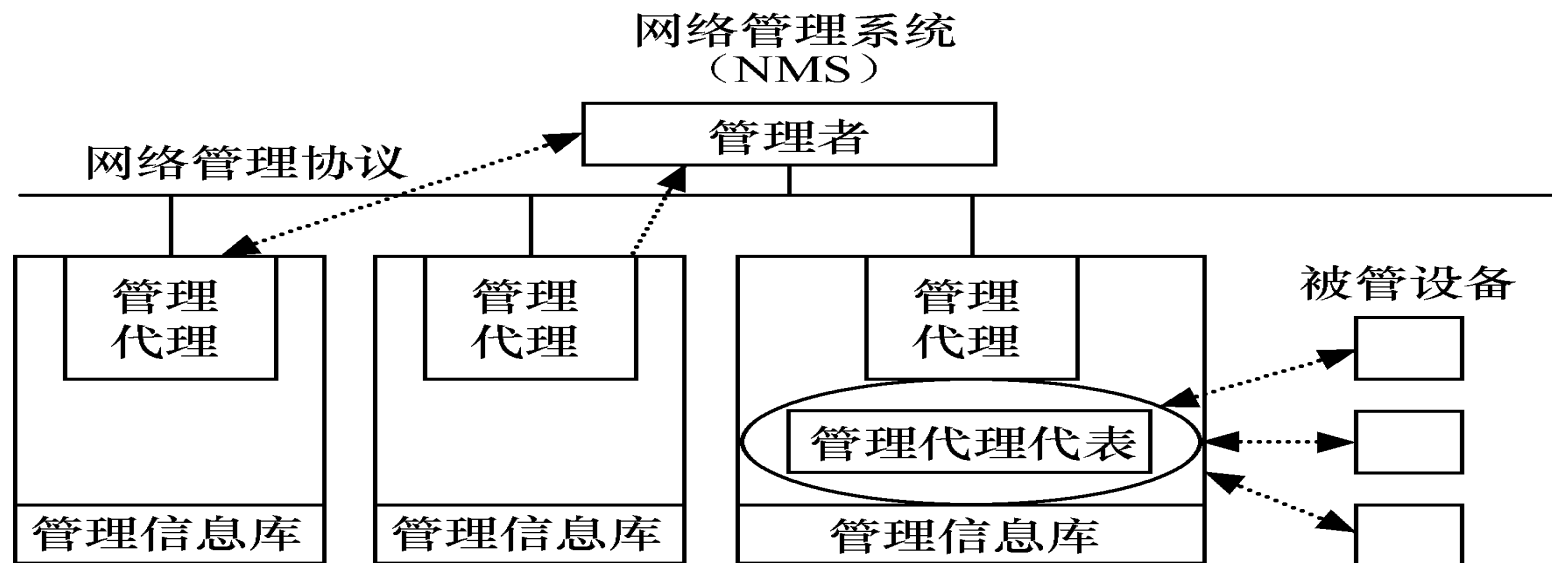
OSI参考模型、TCP/IP参考模型、TMN参考模型、
IEEE LAN/WAN以及基于Web的管理。

网络管理的体系结构

- ◆两种主要的网络管理体系结构，即基于OSI参考模型的公共管理信息协议（CMIP）体系结构与基于TCP/IP参考模型的简单网络管理协议（SNMP）体系结构。
- ◆CMIP体系结构和SNMP体系结构各有优点。CMIP的优点是它的通用性和完备性，而SNMP体系结构的优点是它的简单性和实用性。CMIP在电信网管理标准（TMN）中得到了应用，而SNMP在计算机网络管理，尤其是Internet的管理中得到了应用。随着Internet的广泛应用，SNMP的影响日益扩大，其自身也得到了较快的改善和发展。

管理者-管理代理的模型

网络管理模型的核心是一对相互通信的系统管理实体. 在这种体系结构中，一个系统中的管理进程担当管理者角色，而另一个系统中的对等实体担当代理者角色，代理者负责提供对被管对象的访问。前者称为网络管理者，后者被称为管理代理。网络管理者将管理要求通过管理操作指令传送给位于被管理系统中的管理代理，对网络内的各种设备、设施和资源实施监视和控制，管理代理则负责管理指令的执行，并且以通知的形式向网络管理者报告被管对象发生的一些重要事件。



现代网络管理系统是由以下4个要素组成：

网络管理者（Network Manager）（也称网络管理站，管理进程）、管理代理（Managed Agent）、网络管理协议（Network Management Protocol, NMP）、管理信息库（Management Information Base, MIB）。

1) 网络管理者(network manager)

位于网络系统的主干或接近主干位置的工作站、微机等

(2) 管理代理(managed agent)

位于被管理的设备内部 转换代理

(3) 网络管理协议NMP(Network Management Protocol)

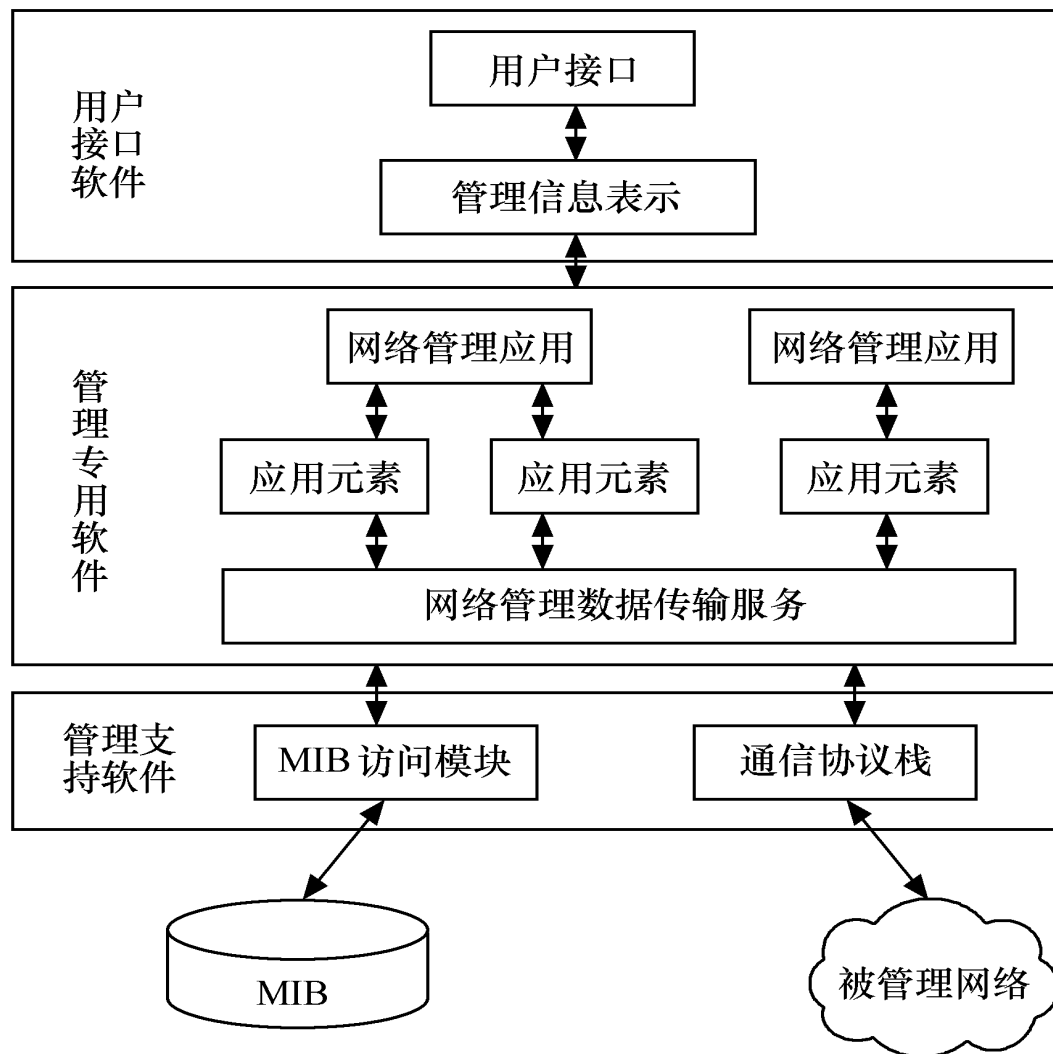
用于网络管理者和管理代理之间传递信息，并完成信息交换安全控制的通信规约

(4) 管理信息库MIB(Management Information Base)

对于通过网络管理协议可以访问信息的精确定义

网络管理软件结构

网络管理软件包括用户接口软件、管理专用软件和管理支持软件3个部分。



网络管理的功能

ISO 7498 – 4文档中定义了网络管理的5大功能：

- 故障管理
- 配置管理
- 性能管理
- 计费管理
- 安全管理

故障管理

故障管理是为了尽快发现故障，找出故障的原因，以便及时采取补救措施，即对计算机网络中的问题或故障进行定位的过程，它包含故障检测和报警功能、故障预测功能、故障诊断和定位功能3个模块。

1．故障检测和报警功能

故障监视代理要随时记录网络系统出错的情况和可能引起故障的事件，并把这些信息存储在运行日志数据库中。

2．故障预测功能

对各种可能引起故障的参数建立门限值并随时监视参数值变化，一旦超过门限值，就发送警报。

3．故障诊断和定位功能

对设备和通信线路进行测试，找出故障原因和地点。

配置管理

配置管理是指设备初始化、维护和关闭网络设备或子系统等操作。被管理的网络资源包括物理设备（如服务器、工作站、路由器）和底层的逻辑对象。

1. 网络配置信息

网络配置信息主要包括以下几种。

- (1) 网络设备的拓扑关系，即存在性和连接关系。
- (2) 网络设备的域名、IP地址，即寻址信息。
- (3) 网络设备的运行特性，即运行参数。
- (4) 网络设备的备份操作参数，即是否备份、备份启用条件。
- (5) 网络设备的配置更改条件。

2．配置管理的主要功能

- (1) 定义配置信息。配置信息描述网络资源的特征和属性。
- (2) 设置和修改设备属性。配置管理允许管理站远程设置和修改代理中的管理信息值，但修改操作要受到两种限制：一是只有授权的管理站才可以施行修改操作；二是有些属性值反映了硬件配置的实际情况，不可更改，如路由器的端口数。
- (3) 定义和修改网络元素间的互连关系。
- (4) 启动和终止网络运行。
- (5) 发行软件。即给系统装载指定的软件、更新软件版本和配置软件参数等功能，除了装载可执行的软件之外，这个功能还包括下载驱动设备工作的数据表。
- (6) 检查参数值、互连关系和报告配置现状。管理站通过轮询随时访问代理保存的配置信息，或者代理通过事件报告及时向管理站通知配置参数改变的情况。

安全管理

- 安全管理的目的是确保网络资源不被非法使用，防止网络资源由于入侵者攻击而遭受破坏。安全基础主要内容包括，与安全措施有关的信息分发（如密钥的分发和访问权设置等），与安全有关的通知（如网络有非法侵入、无权用户对特定信息的访问企图等），安全服务措施的创建、控制和删除，与安全有关的网络操作事件的记录、维护和查询日志管理工作等等
- 安全管理的目的是确保网络资源不被非法使用，防止网络资源由于入侵者攻击而遭受破坏。

1. 安全信息维护

网络管理中的安全管理是指保护管理站和代理之间信息交换的安全。

对安全信息的维护主要包括以下功能。

- (1) 记录系统中出现的各类事件（如用户登录、退出系统、文件复制等）。
- (2) 追踪安全设计试验，自动记录有关安全的重要事件，例如，非法用户持续试验不同口令文字企图登录等。
- (3) 报告和接收侵犯安全的警示信号，在怀疑出现威胁安全的活动时采取防范措施，例如，封锁被入侵的用户账号或强行停止恶意程序的执行等。
- (4) 经常维护和检查安全记录，进行安全风险分析，编制安全评价报告。
- (5) 备份和保护敏感的文件。
- (6) 研究每个正常用户的活动形象，预先设定敏感资源的使用形象，以便检测授权用户的异常活动和对敏感资源的滥用行为。

2 . 资源访问控制

资源访问控制包括认证服务和授权服务，以及对敏感资源访问授权的决策过程。访问控制服务的目的是保护各种网络资源，这些资源中与网络管理有关的主要内容包括：安全编码、源路由和路由记录信息、路由表、目录表、报警门限、计费信息。

3 . 网络安全技术

目前，网络安全管理使用的网络安全技术主要包括以下5种。

- (1) 数据加密技术
- (2) 防火墙技术
- (3) 网络安全扫描技术
- (4) 网络入侵监测技术
- (5) 黑客诱骗技术

性能管理

网络性能管理活动是持续地测评网络运行中的主要性能指标，以检验网络服务是否达到了预定的水平，找出已经发生或潜在的网络瓶颈，报告网络性能的变化趋势，为网络管理决策提供依据。

典型的网络性能管理可以分为两部分：性能监测与网络控制。性能监测指网络工作状态信息的收集和整理；而网络控制则是为改善网络设备的性能而采取的动作和措施

1. 性能管理的基本功能

- (1) 实时采集与网络性能相关的数据。跟踪系统、网络或业务情况，收集合适的的数据，及时发现网络拥塞或性能不断恶化的状况。提供一系列的数据采集工具，以便对网络设备和线路的流量、负载、丢包、温度、内存、延迟等性能进行实时监测并可随意设置数据的采集间隔。
- (2) 分析和统计数据。对实时数据进行分析，判断是否处于正常水平，从而对当前的网络状况作出评估，并自动形成管理报表，以图形方式直观地显示出网络的性能状况。分析和统计历史数据，绘出历史数据的图形。
- (3) 维护并检查系统的运行日志。
- (4) 性能的预警。决定是否为每个重要的指标设定一个适当的阈值，当性能指标超过该阈值时，就表明出现了值得怀疑的网络故障。
- (5) 生成性能分析报告。性能分析报告包括性能趋势曲线和性能统计分析报表。

2. 常用的网络性能测评指标

- (1) 吞吐量。它是指单位时间内通过网络设备的平均比特数，单位是bit/s（比特/秒）。
- (2) 包（帧）延迟。它是指数据分组（帧）的最后一位到达输入端口或输出数据分组的最后一位出现在端口的时间间隔，即LIFO（Last In First Out）延迟。对于交换机来说，延迟是衡量交换机性能的主要指标，延迟越大说明交换机处理帧的速度越慢。
- (3) 丢包（帧）率。它是指在正常稳定的网络状态下，本来应该转发而没有转发的数据包（帧）所占的百分比。丢包率的大小表示网络的稳定性及可靠性。丢包（帧）率可以用来描述过载状态下交换机的性能，也是衡量防火墙性能的一个重要参数。
- (4) 可用性。表征通信网作为一个整体的性能，它意味着一个用户在总的时间内，可以取得对网络访问将成为可用服务时间的百分数。
- (5) 响应时间。对用户来讲，响应时间包括思考时间和输入时间，各部分的时间长短依赖于要完成的任务。对于网络来说，响应时间包括内部、外部和处理时间。
- (6) 利用率。它是网络资源使用频度的动态参数，提供的是现实运行环境下吞吐量的实际限制。网络管理系统通常给出各种网络部件的利用率，如线路、节点、节点处理机的利用率。

3 . 网络性能的测评方法

- (1) 直接测量法。对网络的信道利用率、碰撞分布和吞吐率等参数进行动态数据统计，以得到测评结果。
- (2) 模拟法。给网络建立数学模型，运用仿真程序通过数学计算得出网络相关参数指标。同时也可以与实测结果进行比较，经过多次校正得到真实的测评结果。
- (3) 分析法。通过采用概率论、过程论和排队论等对各种网络进行模拟，其分析结果可用于对未来的网络进行优化设计。

计费管理

1. 计费管理功能

- (1) 计算网络建设及运营成本，包括设备、网络服务、人工费用等成本。
- (2) 统计网络及其所包含的资源的利用率，确定计费标准。
- (3) 将应该缴纳的费用通知用户。
- (4) 支持用户费用上限的设置。
- (5) 在必需用多个通信实体才能完成通信时，能够把使用多个管理对象的费用结合起来。
- (6) 保存收费账单及必要的原始数据，以备用户查询和质疑。

2 . 计费管理的类型

根据网络资源的种类可以将目前的计费管理分为3类。

- (1) 基于网络流量计费。网络流量计费是根据用户的网络或者用户的主机在一段时间内使用的网络流量收取用户费用的一种计费方式，主要用于专线（如DDN、E1、X.25线路等）接入用户。
- (2) 基于使用时间计费。使用时间计费是根据用户使用网络的时间长短来收取用户费用的一种计费方式。该方法主要用于用电话线或ISDN、ADSL接入网络的用户。
- (3) 基于网络服务计费。