21世纪高等教育网络工程规划教材

21st Century University Planned Textbooks of Network Engineering

计算机网络管理

（第2版）

Network Management (2nd Edition)

雷震甲◎编著

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等教育网络工程规划教材
21st Century University Planned Textbooks of Network Engineering

计算机网络管理

（第2版）

Network Management (2nd Edition)

雷震甲◎编著

人民邮电出版社
北京

图书在版编目（CIP）数据

计算机网络管理 / 雷震甲编著. -- 2版. -- 北京 : 人民邮电出版社, 2016.9
21世纪高等教育网络工程规划教材
ISBN 978-7-115-41696-4

Ⅰ. ①计… Ⅱ. ①雷… Ⅲ. ①计算机网络管理－高等学校－教材 Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2016)第036374号

内 容 提 要

本书根据网络管理课程教学大纲的要求，以 SNMP 为基础讨论了网络管理系统的体系结构、管理功能域、协议操作规范、管理信息库组成、远程网络监视，以及网络管理系统的安全机制。本书还介绍了网络管理的实用技术，包括 Windows 中的网络管理工具以及广泛使用的网络分析软件。最后本书讨论了网络测试和网络性能评价的标准、方法和工具。

本书适用于高等学校计算机和通信专业本科生学习，也可供相关专业人员参考。

◆ 编　　著　雷震甲
责任编辑　刘　博
责任印制　沈　蓉　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：14.5　　2016 年 9 月第 2 版
字数：378 千字　　2016 年 9 月北京第 1 次印刷

定价：39.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

第 2 版前言

本书自 2009 年出版以来得到了读者的青睐，经多次重印，一直在许多高校作为网络管理课程的教材。

这次再版主要做了如下三项修订：一是删去了原书的第 7 章和第 8 章，这些内容可以在其他课程或进一步的研究工作中学习。二是把原来第 5 章中介绍 SNMPc 软件的内容改换成了当前更常用的科来网络分析系统。最主要的是第三项改进，就是根据有关网络管理课程教学大纲的要求，新编了第 7 章网络测试和性能评价，其中对网络测试的基本概念，网络测试的标准、方法和工具都进行了详细论述，也比较完整地讨论了网络设备和网络系统的性能评价指标和评价方法。

通过这些修改，本书的内容更加切合当前网络管理工作的实际要求，为学生进一步学习和考研提供更多的帮助。

本书第 1～2 章由雷震甲编写，第 3 章由严体华编写，第 4 章由雷英编写，第 5 章由王斌宁编写，第 6 章由高振江编写，第 7 章由景为编写。

编　者

2015 年 11 月

第 1 版前言

在人们的日常生活和商业活动日益依赖互联网的情况下，对计算机网络的性能、安全和效率提出了更高的要求。研究网络管理技术和开发适用的网络管理工具无疑是计算机专业技术人员的重要职责，使用统一的网络管理标准和适用的网络管理工具，就可以对计算机网络实施有效的管理，减少停机时间，改进响应时间，提高设备的利用率，还可以减少运行的费用。本书就是围绕这些方面展开讨论的。

第 1 章讲述网络管理系统的体系结构和管理功能域，并简要介绍了网络管理标准制定和使用情况；第 2 章介绍网络管理信息库的结构和组成，以此为线索回顾了计算机网络方面的基础知识；第 3 章介绍简单网络管理协议 SNMP 的基本理论和操作技术，对 SNMP 的三个版本都有详细的论述；第 4 章讲述 RMON 管理信息库，以及在局域网管理方面的应用；第 5 章在前述内容的基础上，以 SNMPc 软件为例，综合讲述实际的网络管理技术；第 6 章介绍了一些常用的网络管理工具，适用于各种流行的网络操作系统；第 7 章介绍 Windows 环境下的网络配置和服务器管理技术；最后一章介绍网络管理技术的发展和研究方向，供读者进一步研究时参考。

本书是作为计算机相关专业的专业课教材编写的，也可以供通信类专业的本科生参考。由于作者的水平有限，书中难免出现错误之处，敬请读者不吝指正。

编　者

2009 年 2 月

目 录

第 1 章 网络管理概论

计算机网络的组成越来越复杂，一方面是网络互连的规模越来越大，另一方面是连网设备越来越多样。异构型网络设备、多协议栈互连、性能需求不同的各种网络业务都增加了网络管理的难度和管理费用，单靠管理员手工管理已经无能为力。研究网络管理的理论，开发先进的网络管理技术，采用自动化的网络管理工具是一项迫切的任务。

1.1 网络管理的基本概念

对于不同的网络，管理的要求和难度也不同。局域网的管理相对简单，因为局域网运行统一的操作系统，只要熟悉网络操作系统的管理功能和操作命令，就可以管好一个局域网。对于由异构型设备组成的、运行多种操作系统的 Internet 的管理就不是那么简单了，这需要跨平台的网络管理技术。

TCP/IP 由于其开放性，20 世纪 90 年代以来逐渐得到网络制造商的支持，获得了广泛的应用，已经成为事实上的 Internet 标准。在 TCP/IP 网络中有一个简单的管理工具——ping 程序。用 ping 发送探测报文可以确定通信目标的连通性及传输时延。如果网络规模不是很大，互连的设备不是很多，这种方法还是可行的，但是当网络互连规模很大时，这种方法就不适用了。这是因为，一方面 ping 返回的信息很少，无法获取被管理设备的详细情况；另一方面用 ping 程序对很多设备逐个测试检查，工作效率很低。在这种情况下出现了用于 TCP/IP 网络管理的标准——简单网络管理协议（SNMP）。这个标准适用于任何支持 TCP/IP 的网络，无论是哪个厂商生产的设备，或是运行哪种操作系统的网络。

与此同时，国际标准化组织也推出了 OSI 系统管理标准 CMIS/CMIP。从长远看，OSI 系统管理更适合结构复杂、规模庞大的异构型网络，但由于其技术开发缓慢，所以尚未进入实用阶段，也许它代表了未来网络管理发展的方向。

网络管理标准的成熟刺激了制造商的开发活动，市场上已经出现了符合国际标准的商用网络管理系统。有主机厂家开发的网络管理应用系统开发软件（如 IBM NetView、HP OpenView），有网络产品制造商推出的与硬件相结合的网管工具（如 Cisco Works 2000、Cabletron Spectrum）。这些产品都可以称为网络管理平台，只有在此基础上开发适合于用户网络环境的网络管理应用软件，才能实施有效的网络管理。

有了统一的网络管理标准和适用的网络管理工具，对网络实施有效的管理，就可以减少停机时间，改进响应时间，提高设备的利用率，还可以减少运行费用。管理工具可以很快地发现并消

灭网络通信瓶颈，提高运行效率。要及时采用新技术，就需要有方便适用的网络配置工具，以便及时修改和优化网络配置，使网络更容易使用，并可以提供多种多样的网络业务。在商业活动日益依赖于 Internet 的情况下，人们要求网络工作得更安全，所以要对网上传输的信息保密，对网络资源的访问要严格地控制，以及防止计算机病毒和非法入侵者的破坏等。这些需求必将进一步促进网络管理工具的研究和开发。

1.2 网络管理系统的体系结构

1.2.1 网络管理系统的层次结构

网络管理系统的层次结构如图 1-1 所示。在网络管理站中，最下层是操作系统和硬件。操作系统之上是支持网络管理的协议簇，如 OSI、TCP/IP 等通信协议，以及专用于网络管理的 SNMP、CMIP 等协议。协议栈上面是网络管理框架（network management framework），这是各种网络管理应用工作的基础结构。各种网络管理框架的共同特点如下。

- 管理功能分为管理站（manager）和代理（agent）两部分。
- 为存储管理信息提供数据库支持，如关系数据库或面向对象的数据库。
- 提供用户接口和用户视图（view）功能，如管理信息浏览器。
- 提供基本的管理操作，如获取管理信息，配置设备参数等操作功能。

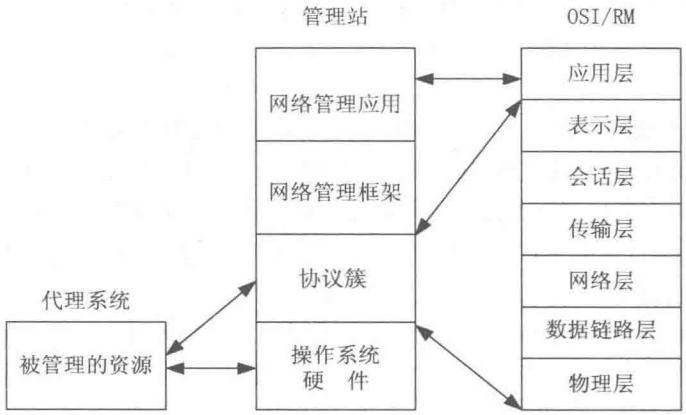


图 1-1　网络管理系统的层次结构

网络管理应用是用户根据需要开发的软件，这种软件运行在网络上，实现特定的管理目标，如故障诊断、性能优化、业务管理和安全控制等。网络管理应用的开发是目前最活跃的领域。

图 1-1 把被管理资源画在单独的框中，表明被管理资源可能与管理站处于不同的系统（或设备）中。网络管理涉及监视和控制网络中的各种硬件、固件和软件资源，如网卡、集线器、中继器、主机、外围设备、通信软件、应用软件和实现网络互连的软件等。有关资源的管理信息由代理进程/代理系统控制，代理进程通过网络管理协议与管理站对话。

1.2.2 网络管理系统的配置

网络管理系统的配置如图 1-2 所示。每一个网络节点都包含一组与管理有关的软件，叫作网

络管理实体（network management entity，NME）。网络管理实体完成以下任务。

- 收集有关网络通信的统计信息。
- 对本地设备进行测试，记录设备状态信息。
- 在本地存储有关信息。
- 响应网络控制中心的请求，发送管理信息。
- 根据网络控制中心的指令，设置或改变设备参数。

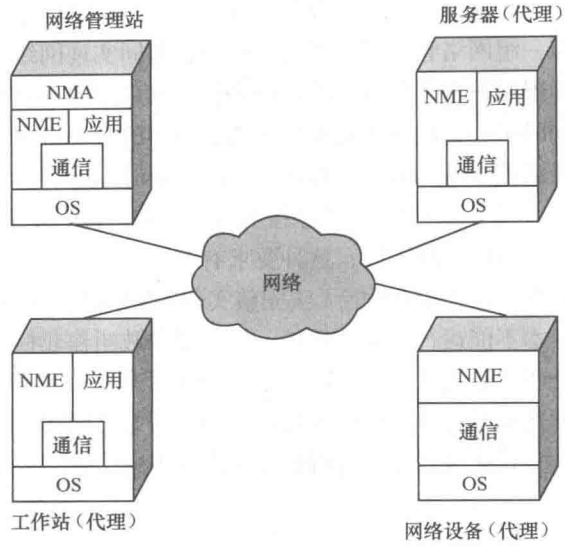


图 1-2　网络管理系统配置

网络中至少有一个节点（主机或路由器）担当管理站（manager）角色。除 NME 之外，管理站中还有一组软件，叫作网络管理应用（network management application，NMA）。NMA 提供用户接口，根据用户命令显示管理信息，通过网络向 NME 发出请求或指令，以便获取有关设备的管理信息，或者改变设备的配置状态。

网络中的其他节点在 NME 的控制下与管理站通信、交换管理信息。这些节点中的 NME 模块叫作代理模块，网络中任何被管理的设备（主机、交换机、路由器或集线器等）都必须实现代理模块。所有代理在管理站监视和控制下协同工作，实现集成的网络管理。这种集中式网络管理策略的好处是管理人员可以有效地控制整个网络资源，根据需要平衡网络负载，优化网络性能。

然而对于大型网络，集中式管理往往显得力不从心，正在让位于分布式管理策略。这种向分布式管理演化的趋势与集中式计算模型向分布式计算模型演化的总趋势是一致的。图 1-3 提出一种可能的分布式网络管理配置方案。

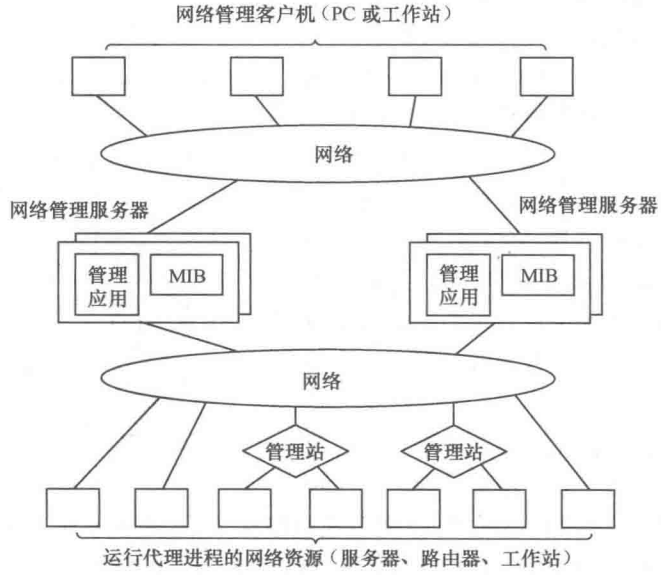


图 1-3　分布式网络管理系统

在这种配置中，分布式管理系统代替了单独的网络控制主机。地理上分布的网络管理客户机与一组网络管理服务器交互作用，共同实现网络管理功能。这种管理策略可以实现分部门管理，即限制每个客户机只能访问和管理本部门的部分网络资源，而由一个中心管理站实施全局管理。同时中心管理站还能对管理功能较弱的客户机发出指令，实现更高级的管理。分布式网络管理的灵活性（flexibility）和可伸缩性（scalability）日益为网络管理工作者所青睐。

图 1-2 和图 1-3 的系统要求每个被管理的设备都能运行代理程序，并且所有管理站和代理都支持相同的管理协议，这种要求有时是无法实现的。例如，有的老设备可能不支持当前的网络管理标准；小的系统可能无法完整实现 NME 的全部功能；甚至还有一些设备（如 Modem 和多路器等）根本不能运行附加的软件，这些设备被叫作非标准设备。在这种情况下，通常的处理方法是用一个叫作委托代理（proxy）的设备来管理一个或多个非标准设备。委托代理和非标准设备之间运行制造商专用协议，而委托代理和管理站之间运行标准的网络管理协议。这样，管理站就可以用标准方式通过委托代理得到非标准设备的信息。委托代理起到了协议转换的作用，如图 1-4 所示。

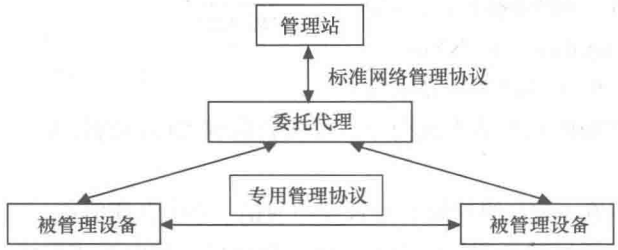


图 1-4　委托代理

1.2.3　网络管理软件的结构

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，如图 1-5 所示，大约相当于图 1-1 中管理站的上三层。

用户通过网络管理接口与管理专用软件交互作用，监视和控制网络资源。接口软件不但存在于管理站上，而且可能出现在代理系统中，以便对网络资源实施本地配置、测试和排错。有效的网络管理系统需要统一的用户接口，而不论主机和设备出自哪个厂家、运行什么操作系统，这样就可以方便地对异构型网络进行监控。接口软件还要有一定的信息处理能力，对大量的管理信息要进行过滤、统计、化简和汇总，以免传递的信息量太大而造成网络拥堵。最后，理想的用户接口应该是图形用户接口，而非命令行或表格式接口。

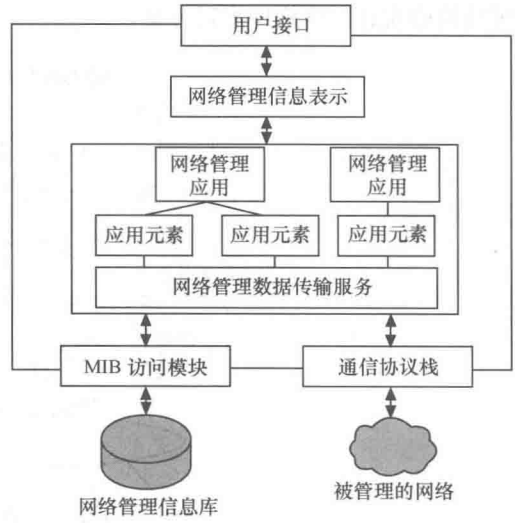


图 1-5　网络管理软件的结构

足够复杂的网管软件可以支持多种网络管理应用，如配置管理、性能管理、故障管理等。这些应用能适用于各种网络设备和网络配置，虽然在实现细节上可能有所不同。图 1-5 表现了用大量的应用元素支持少量管理应用的设计思想。应用元素实现通用的基本管理功能（如产生报警、对数据进行分析等），可以被多个应用程序调用。传统的模块化设计方法可提高软件的重用性，提高实

现的效率。网络管理软件的最底层提供网络管理数据传输服务，用于在管理站和代理之间交换管理信息。管理站利用这种服务接口可以检索设备信息，配置设备参数，代理则通过服务接口向管理站报告设备事件。

管理支持软件包括管理信息库（Management Information Base，MIB）访问模块和通信协议栈。代理中的 MIB 包含反映设备配置和设备行为的信息，以及控制设备操作的参数。管理站的 MIB 中除了保留本地节点专用管理信息外，还保存着管理站控制的所有代理的相关信息。MIB 访问模块具有基本的文件管理功能，这使得管理站或代理可以方便地访问 MIB，同时该模块还能把本地的 MIB 格式转换为适于网络管理系统传送的标准格式。通信协议栈支持节点之间的通信。由于网络管理协议位于应用层，原则上任何通信体系结构都能胜任，但具体的实现可能有特殊的通信要求。

1.3　网络监控系统

网络管理功能可分为网络监视和网络控制两大部分，统称网络监控（Network Monitoring）。网络监视是指收集系统和子网的状态信息，分析被管理设备的行为，以便发现网络运行中存在的问题。网络控制是指修改设备参数或重新配置网络资源，以便改善网络运行状态。具体地说，网络监控要解决的问题包括以下几个方面。

（1）管理信息的定义：监视哪些管理信息，从哪些被管理资源获得管理信息。

（2）监控机制的设计：如何从被管理资源中得到需要的信息。

（3）管理信息的应用：根据收集到的管理信息实现什么管理功能。

下面首先说明前两个问题，即管理信息的定义和监控机制的设计。

1.3.1　管理信息库

有用的网络监控管理信息可以分为以下 3 类。

（1）静态信息：包括系统和网络的配置信息，如路由器的端口数和端口编号、工作站的标识和 CPU 类型等，这些信息不经常变化。

（2）动态信息：与网络中出现的事件和设备的工作状态有关，如网络中传送的分组数、网络连接的状态等。

（3）统计信息：即从动态信息推导出的信息，如平均每分钟发送的分组数、传输失败的概率等。

这些信息组成的管理信息库如图 1-6 所示。配置数据库中存着计算机和网络的基本配置信息，传感器数据库中存储传感器的设置信息。传感器是一组软件，用于实时读取被管理设备的有关参数。配置数据库和传感器数据库共同组成静态数据库。动态数据库存储由传感器收集的各种网络元素和网络事件的实时数据。统计数据库中的管理信息是由动态信息计算出来的。这 3 种数据库的关系如图 1-6 所示。

网络监控功能一方面要确定从哪里收集管理信息，另一方面还要确定管理信息应该存储在什么地方。静态信息是由网络元素直接产生的，通常由驻留在这些网络元素（如路由器）中的代理进程收集和存储，必要时传送给监视器。如果网络元素（如 Modem）中没有代理进程，则可以由委托代理收集这些静态信息，并传送给监视器。

动态信息通常也是由产生有关事件的网络元素收集和存储的，例如，工作站建立的网络连接数就存储在该工作站中。然而对于一个局域网来说，网络中各个设备的行为和有关数据可以由连

接在网络中的一个专用主机来收集和记录，这个主机叫作远程网络监视器，它的作用是收集整个子网的通信数据，如在一段时间内一对主机之间交换的分组数、网络中出现冲突的次数等。

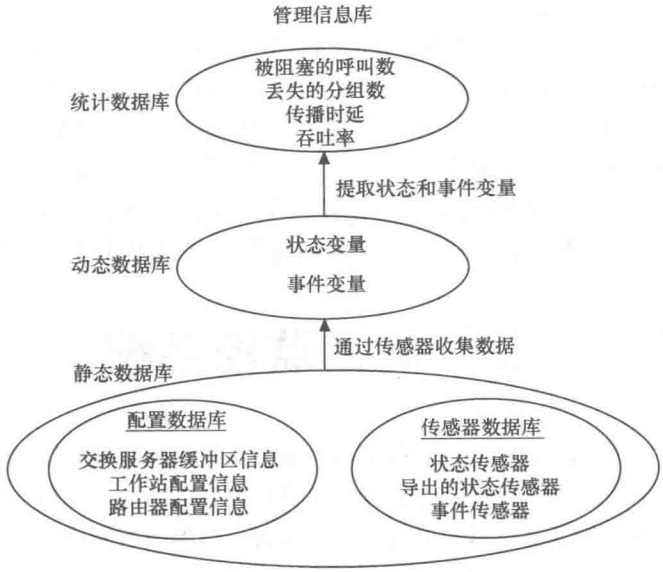


图 1-6　管理信息库的组成

统计信息可以由任何能够访问动态信息的系统产生。当然，统计信息也可以由网络监视器自己产生，这就要求把所有需要的原始数据传送给监视器，再由监视器进行分析和计算。如果原始数据量很大，则这种监控方式可能会消耗很多网络带宽。如果存储动态信息的系统进行了分析和计算，则不但节约了网络带宽，而且节省了监视器处理时间。

1.3.2　网络监控系统的配置

网络监控系统的配置如图 1-7（a）所示。监控应用程序是监控系统的用户接口，它完成性能监视、故障监视和计费监视等功能。管理功能负责与其他网络元素中的代理进程通信，把需要的监控信息提供给监控应用程序。这两个模块都处于管理站中。管理对象表示被监控的网络资源中的管理信息，所有管理对象遵从网络管理标准的规定。管理对象中的信息通过代理功能提供给管理站。图 1-7（b）中增加了监控代理功能。这个模块的作用是专门对管理信息进行计算和统计分析，并把计算的结果提供给管理站。在管理站看来，监控代理的作用和一般代理是一样的，然而它管理着多个代理系统。

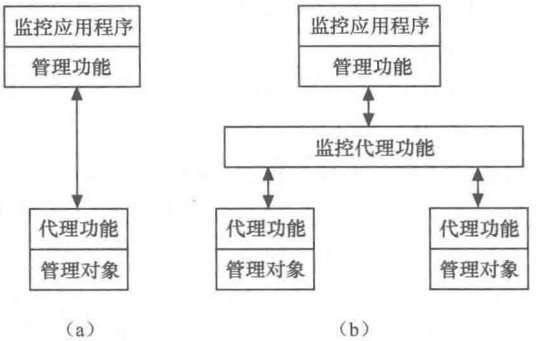


图 1-7　网络监控系统的体系结构

实际上这些功能模块可以处于不同的网络元素中，组成多种形式的监控系统。如果管理站本身就是一个被监控的网络元素，则它应该包含监控应用程序、管理功能、代理进程以及一组反映自身管理信息的对象。监视器的状态和行为对整个网络监控系统的性能起决定作用，因而监视器也应时刻监视自身的通信情况。一般情况下，监视器与代理系统处于不同的网络元素中，它们通过网络交换管理信息。另外，一个管理站/监视器

可以监控多个代理系统，也可以只监控一个代理系统；而一个代理系统可能代理一个或多个网络元素，甚至代理整个局域网；监视器可能与被监控的网络元素处于同一子网中，也可能通过远程网络互连。

1.3.3　网络监控系统的通信机制

对监视器有用的管理信息是由代理收集和存储的，那么代理怎样把这些信息传送给监视器呢？有两种技术可用于代理与监视器之间的通信，一种叫作轮询（polling），另一种叫作事件报告（event reporting）。轮询是一种请求—响应式的交互作用，即由监视器向代理发出请求，询问它所需要的信息数值，代理响应监视器的请求，从它保存的管理信息库中取得请求的信息，返回给监视器。请求可以采用不同的形式，例如，列出一些变量的名字，要求代理返回变量的值；或者给出一种匹配模式，要求代理搜索与模式匹配的所有变量的值；监视器可能要查询它所管理的系统的配置，或者周期性地询问被管理系统配置改变的情况；监视器也可能在收到一个报警后，用轮询方式详细调查某个区域的真实情况，或者根据用户的要求通过轮询生成一个配置报告。

事件报告是由代理主动发送给管理站的消息。代理可以根据管理站的要求（周期、内容等）定时发送状态报告，也可能在检测到某些特定事件（如状态改变）或非正常事件（如出现故障）时生成事件报告，发送给管理站。事件报告对于及时发现网络中的问题是很有用的，特别对于监控状态信息不经常改变的管理对象更有效。

在已有的各种网络监控系统中都设置了轮询和事件报告两种通信机制，但强调的重点有所不同。传统的通信管理网络主要依赖于事件报告，而 SNMP 强调轮询方法，OSI 系统管理则采取了与这两种方法都不同的中间道路。然而无论是 SNMP，还是 OSI，或是某些专用的管理系统，都允许用户根据具体情况决定使用何种通信方式。影响通信方式选择的主要因素如下。

- 传送监控信息需要的通信量。
- 对危急情况的处理能力。
- 对网络管理站的通信时延。
- 被管理设备的处理工作量。
- 消息传输的可靠性。
- 网络管理应用的特殊性。
- 在发送消息之前，通信设备失效的可能性。

1.4　网 络 监 视

网络管理有五大功能域，即故障管理（fault management）、配置管理（configuration management）、计费管理（accounting management）、性能管理（performance management）和安全管理（security management），简写为 FCAPS。传统上，性能、故障和计费属于网络监视功能，另外两种属于网络控制功能。这一节介绍网络监视功能。

1.4.1　性能监视

网络监视中最重要的是性能监视，然而要能够准确地测量出对网络管理有用的性能参数却是不容易的。可选择的性能指标很多，有些测量难度大，或计算量大，也不一定特别有用；有些有

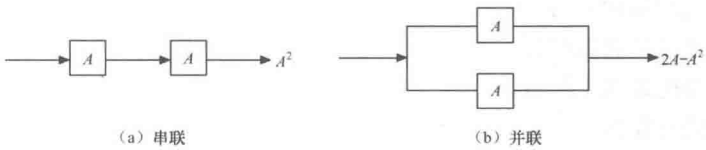
用的指标没有得到制造商的支持，无法从现有的设备上检测到。还有些性能指标互相关联，要互相参照才能说明问题。这些情况都增加了性能测量的复杂性。这一小节介绍性能监视的基本概念，给出对网络管理有用的两类性能指标，即面向服务的性能指标和面向效率的性能指标。当然，网络最主要的目标是向用户提供满意的服务，因而面向服务的性能指标应具有较高的优先级。下面要介绍的内容前三个是面向服务的性能指标，后两个是面向效率的性能指标。

1. 可用性

可用性是指网络系统、网络元素或网络应用对用户可利用的时间的百分比。有些应用对可用性很敏感，例如，飞机订票系统若宕机一小时，就可能减少数十万元的票款；而股票交易系统如果中断运行一分钟，就可能造成几千万元的损失。实际上，可用性是网络元素可靠性的表现，而可靠性是指网络元素在具体条件下完成特定功能的概率。如果用平均无故障时间（Mean Time Between Failure，MTBF）来度量网络元素的故障率，则可用性 A 可表示为 $MTBF$ 的函数

$$A=\frac{MTBF}{MTBF+MTTR}$$

其中，MTTR（Mean Time To Repair）为发生失效后的平均维修时间。由于网络系统由许多网络元素组成，所以系统的可靠性不但与各个元素的可靠性有关，而且与网络元素的组织形式有关。根据一般的可靠性理论，由元素串并联组成的系统的可用性与网络元素的可用性之间的关系如图1-8所示。由图1-8（a）可以看出，若两个元素串联，则可用性减少。例如，两个Modem串联在链路的两端，若单个Modem的可用性 A=0.98，并假定链路其他部分的可用性为1，则整个链路的可用性 A=0.98×0.98=0.9 604。由图1-8（b）可以看出，若两个元素并联，则可用性增加。如终端通过两条链路连接到主机，若一条链路失效，另外一条链路可自动备份。假定单个链路的可用性 A=0.98，则双链路的可用性 A=2×0.98-0.98×0.98=0.9 996。



（a）串联　　（b）并联

图1-8　串联和并联的可用性

【例1.1】计算双链路并联系统的处理能力。假定一个多路器通过两条链路连接到主机（见图1-8（b））。在主机业务的峰值时段，一条链路只能处理总业务量的80%，因而需要两条链路同时工作，才能处理主机的全部传送请求。非峰值时段大约占整个工作时间的40%，只需要一条链路工作就可以处理全部业务。这样，整个系统的可用性 A_f 可表示为

A_f=（一条链路的处理能力）×（一条链路工作的概率）+（两条链路的处理能力）×（两条链路工作的概率）

假定一条链路的可用性为 A=0.9，则两条链路同时工作的概率为 A^2=0.81，而恰好有一条链路工作的概率为 $A(1-A)+(1-A)A=2A-2A^2$=0.18，则有

$$A_f\text{（非峰值时段）}=1.0\times0.18+1.0\times0.81=0.99$$

$$A_f\text{（峰值时段）}=0.8\times0.18+1.0\times0.81=0.954$$

于是系统的平均可用性为

$$A_f=0.6\times A_f\text{（峰值时段）}+0.4\times A_f\text{（非峰值时段）}=0.9\ 684$$

2. 响应时间

响应时间是指从用户输入请求到系统在终端上返回计算结果的时间间隔。从用户角度看，这个时间要和人们的思考时间（等于两次输入之间的最小间隔时间）配合，越是简单的工作（如数据录入），要求响应时间越短。然而从实现角度看，响应时间越短，实现的代价越大。研究表明，系统响应时间对生产率的影响是很大的。在交互式应用中，若响应时间大于 15s，大多数人是不能容忍的。响应时间大于 4s 时，人们的短期记忆会受到影响，工作的连续性被破坏，尤其是对数据录入员来说，这种情况下击键的速度会严重受挫。在输入完一个段落后，才可以有比较大的延迟（如 4s 以上）。越是注意力高度集中的工作，要求响应时间越短。特别对于需要记住以前的响应，根据前面的响应决定下一步的输入时，延迟时间应该小于 2s。在用鼠标单击图形或进行键盘输入时，要求的响应时间更小，可能在 0.1s 以下。这样人们会感到计算机是同步工作的，几乎没有等待时间。图 1-9 表明应用 CAD 进行集成电路设计时，生产率（每小时完成的事务处理数）与响应时间的关系。可以看出，当响应时间小于 1s 时，事务处理的速率明显加快，这和人的短期记忆以及注意力集中的程度有关。

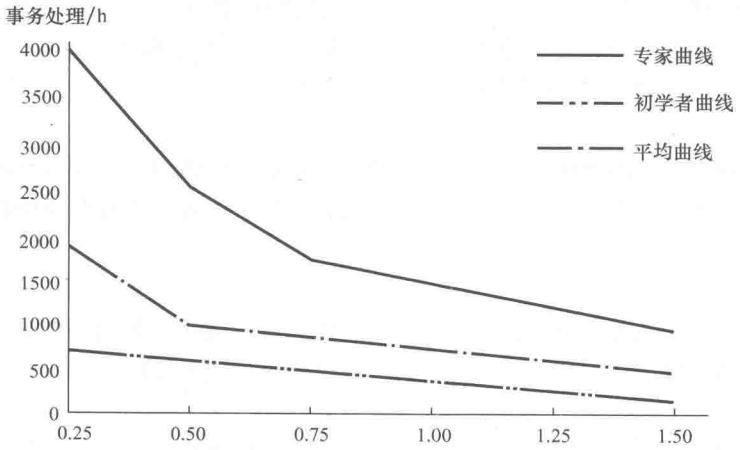
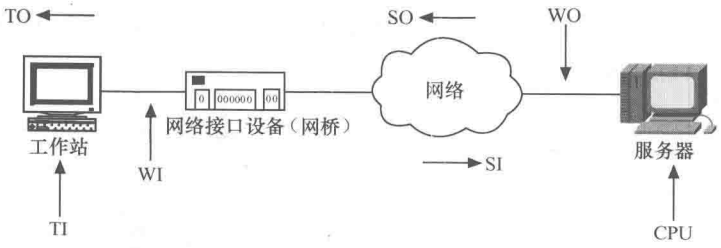


图 1-9　系统响应时间与生产率的关系

网络的响应时间由系统各个部分的处理延迟时间组成，分解系统响应时间的成分对于确定系统瓶颈有很大作用。系统响应时间 RT 由以下 7 部分组成，如图 1-10 所示。



RT=TI+WI+SI+CPU+WO+SO+TO

RT	响应时间	CPU	CPU 处理延迟
TI	入口终端延迟	WO	出口排队时间
WI	入口排队时间	SO	出口服务时间
SI	入口服务时间	TO	出口终端延迟

图 1-10　系统响应时间的组成

- 入口终端延迟（TI）：是指从终端把查询命令送到通信线路上的延迟。终端本身的处理时