

第 3 章

CHAPTER

网络管理体系结构

每个计算机网络都是计算机、连接介质、系统软件和协议的组合,网络之间又互联形成更加复杂的互联网。因此,在进行网络管理系统开发时,必须用逻辑模型来表示这些复杂的网络组件,这就是本章要讲到的网络体系结构。所谓网络体系结构,就是从现实复杂的网络中抽象出逻辑模型,作为网络管理系统开发的支持。本章将介绍网络管理的基本模型、网络管理系统的模式、网络管理的软件结构以及常规网络管理协议。

3.1 网络管理的基本模型

3.1.1 网络管理模型

网络管理系统是用于实现对网络的全面有效的管理,实现网络管理目标的系统。在一个网络的运营管理中,网络管理人员是通过网络管理系统对整个网络进行管理的。概括地说,一个网络管理系统从逻辑上包括管理对象、管理进程、管理信息库和管理协议 4 大部分。网络管理系统的逻辑模型如图 3-1 所示。

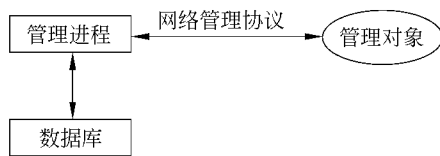


图 3-1 网络管理系统的逻辑模型图

1) 管理对象

管理对象是网络中具体可以操作的数据。例如,记录设备或设施工作状态的状态变量、设备内部的工作参数、设备内部用来表示性能的统计参数等;需要进行控制的外部工作状态和工作参数;为网络管理系统设计,为管理系统本身服务的工作参数等。

2) 管理进程

管理进程是一个或一组软件程序,一般运行在网络管理站(网络管理中心)的主机上,它可以在 SNMP 的支持下命令管理代理执行各种管理操作。

管理进程完成各种网络管理功能,通过各设备中的管理代理对网络内部的各种设备、设施和资源实施监测和控制。另外,操作人员通过管理进程对全网进行管理。因而管理进程也经常配有图形用户接口,以容易操作的方式显示各种网络信息,如给出网络中各管理代理的配置图等。有时管理进程也会对各管理代理中的数据集中存档,以备事后分析。

3) 管理信息库

管理信息库用于记录网络中管理对象的信息。例如,状态类对象的状态代码、参数类管理对象的参数值等。管理信息库中的数据要与网络设备中的实际状态和参数保持一致,达到能够真实地、全面地反映网络设备或设施情况的目的。

管理信息库的结构必须符合使用 TCP/IP 的 Internet 的管理信息结构(SMI)。这个 SMI 实际上是参照 OSI 的管理信息结构制定的。尽管两个 SMI 基本一致,但 SNMP 和 OSI 的 MIB 中定义的管理对象却并不相同。Internet 的 SMI 和相应的 MIB 是独立于具体的管理协议的(包括 SNMP)。

4) 管理协议

管理协议用于在管理系统与管理对象之间传递操作命令,负责解释管理操作命令。通过管理协议来保证管理信息库中的数据与具体设备中的实际状态、工作参数保持一致。

3.1.2 网络管理者与网管代理

在网络管理中,一般采用网络管理者——网管代理模型。网络管理模型的核心是一对相互通信的系统管理实体,它采用一个独特的方式使两个管理进程之间相互作用,即管理进程与一个远程系统相互作用,来实现对远程资源的控制。在这种简单的体系结构中,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,后者称为网管代理。无论是 OSI 的网络管理,还是 IETF 的网络管理,都认为现代计算机网络管理系统是由网络管理者(network manager)、网管代理(managed agent)、网络管理协议(network management protocol,NMP)和管理信息库(management information base,MIB)4 个要素组成的。

网络管理者(管理进程)是管理指令的发出者,它通过各网管代理对网络内的各种设备、设施和资源实施监视和控制。网管代理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。网管代理具有两个基本功能:一是从 MIB 中读取各种变量值;二是在 MIB 中修改各种变量值。MIB 是被管对象结构化组织的一种抽象。它是一个概念上的数据库,由管理对象组成,各个网管代理管理 MIB 中属于本地的管理对象,各网管代理控制的管理对象共同构成全网的管理信息库。网络管理协议是最重要的部分,它定义了网络管理者与网管代理间的通信方法,规定了管理信息库的存储结构信息库中关键词的含义以及各种事件的处理方法。

在系统管理模型中,管理者角色与网管代理角色不是固定的,而是由每次通信的性质所决定的。担当管理者角色的进程向担当网管代理角色的进程发出操作请求,担当网管

代理角色的进程对被管对象进行操作并将被管对象发出的通报传向管理者。

1. 网络管理者

网络管理者是指实施网络管理的处理实体,网络管理者驻留在管理工作站上,管理工作站通常是指那些工作站、微机等,一般位于网络系统的主干或接近于主干的位置,负责发出管理操作的指令,并接收来自网管代理的信息。网络管理者要求网管代理定期收集重要的设备信息。网络管理者定期查询网管代理收集到的有关主机运行状态、配置及性能数据等信息,这些信息将用于确定独立的网络设备、部分网络或整个网络运行的状态是否正常。

网络管理者和网管代理通过交换管理信息来进行工作,信息分别驻留在被管设备和管理工作站上的管理信息库中。这种信息交换通过一种网络管理协议来实现,具体的交换过程是通过协议数据单元(protocol data unit,PDU)进行的。通常是管理站向网管代理发送请求 PDU,网管代理以响应 PDU 回答,管理信息包含在 PDU 参数中。在有些情况下,网管代理也可以向管理站发送消息,这种消息叫做事件报告或通知,管理站可根据报告的内容决定是否做出回答。

管理站作为网络管理员与网络管理系统的接口,其基本构成如下。

- (1) 一组具有分析数据、发现故障等功能的管理程序。
- (2) 一个用于网络管理员监控网络的接口。
- (3) 将网络管理员的要求转变为对远程网络元素实际监控的能力。
- (4) 一个从所有被管网络实体的 MIB 中抽取信息的数据库。

2. 网管代理

网管代理是一个软件模块,驻留在被管设备上。这里的设备可以是工作站、网络打印机,也可以是其他网络设备。通常将主机和网络互联设备等所有被管理的网络设备统称为被管设备。它的功能是把来自网络管理者的命令或信息的请求转换成本设备特有的指令,完成网络管理者的指示或把所有设备的信息返回到网络管理者,包括有关运行状态、设备特性、系统配置和其他相关信息。另外,网管代理也可以将自身系统中发生的事件主动通知给网络管理者。

网管代理就像是每个被管理设备的信息经纪人,它们完成网络管理者布置的信息收集任务。网管代理实际所起的作用就是充当网络管理者与网管代理所驻留的设备之间的信息中介。网管代理通过控制设备的管理信息库中的信息来实现管理网络设备功能。

3.1.3 网管协议

管理站和网管代理者之间通过网络管理协议通信,网络管理者进程通过网络管理协议来完成网络管理。目前最有影响的网络管理协议是 SNMP 和 CMIS/CMIP,它们代表了目前两大网络管理解决方案。其中 SNMP 流传最广,应用最多,获得支持也最广泛,已经成为事实上的工业标准。下面以 SNMP 为例,解释网络管理协议的含义。

SNMP 作为应用层协议,是 TCP/IP 协议簇的一部分。SNMP 在 UDP、IP 及有关的特殊网络协议(如 Ethernet、FDDI 和 X.25)之上实现。SNMP 通过用户数据报协议来操作,所以要求每个网管代理也必须能够识别 SNMP、UDP 和 IP。在管理站中,网络管理

者进程在 SNMP 协议的控制下对 MIB 进行访问,并发布控制指令。在被管对象中,网管代理进程在 SNMP 协议的控制下,负责解释 SNMP 消息和控制 MIB 指令。

3.1.4 管理信息库

管理信息库是一个信息存储库,它是网络管理系统中一个非常重要的部分。

MIB 定义了一种对象数据库,由系统内的许多被管对象及其属性组成。

通常,网络资源被抽象为对象进行管理。对象的集合被组织为管理信息库。MIB 作为设在网管代理者处的管理站访问点的集合,管理站通过读取 MIB 中对象的值来进行网络监控。管理站可以在网管代理处产生动作,也可以通过修改变量值改变网管代理处的配置。现在已经定义了几种通用标准的 MIB,在这些 MIB 中包括了必须在网络设备中支持的特殊对象,使用最广泛、最通用的是 MIB-II。

MIB 中的数据可分为三类:感测数据、结构数据和控制数据。感测数据表示测量到的网络状态,是通过网络的监测过程获得的原始信息,包括结点队列长度、重发率、链路状态和呼叫统计等,这些数据是网络的计费管理、性能管理和故障管理的基本数据。结构数据描述网络的物理和逻辑构成,对应感测数据。结构数据是静态的(变化缓慢的)网络信息,包括网络拓扑结构、交换机和中继线的配置、数据密钥、用户记录等,这些数据是网络的配置管理和安全管理的基本数据。控制数据存储网络的操作设置,控制数据代表网络中那些可调整参数的设置,如中继线的最大流、交换机输出链路业务分流比率和路由表等,控制数据主要用于网络的性能管理。

3.2 网络管理模式

网络管理模式分为集中式网络管理模式、分布式网络管理模式以及混合管理模式三种。它们各有自身的特点,适用于不同的网络系统结构和不同的应用环境。

3.2.1 集中式网络管理模式

集中式网络管理模式是所有的网管代理在管理站的监视和控制下,协同工作实现集成的网络管理模式,如图 3-2 所示。

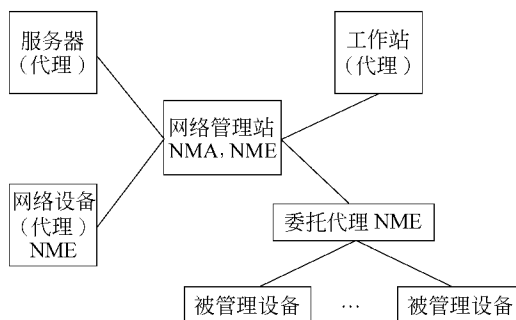


图 3-2 集中式网络管理模式

在集中式网络管理配置图中,有一个叫做委托网管代理的结点,为什么要引入托管代理呢?原因是网络中存在非标准设备,通过委托网管代理来管理一个或多个非标准设备,委托网管代理的作用是进行协议转换。

该配置中至少有一个结点担当管理站的角色,其他结点在网管代理模块(NME)的控制下与管理站通信。其中 NME 是一组与管理有关的软件,NMA 是指网络管理应用,它们之间的关系如图 3-3 所示。

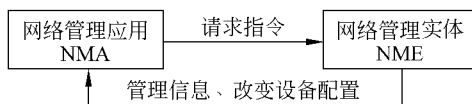


图 3-3 NME 与 NMA 的关系

NME 的主要作用有以下 4 个方面:收集统计信息;记录状态信息;存储有关信息,响应请求,传送信息;根据指令设置或改变参数。

集中式网络管理模式在网络系统中设置专门的网络管理结点。管理软件和管理功能要集中在网络管理结点上,网络管理结点与一般被管结点是主从关系。

网络管理结点通过网络通信信道或专门网络管理信道与所有结点相连。网络管理结点可以对所有结点的配置、路由等参数进行直接控制和干预,可以实时监视全网结点的运行状态,统计和掌握全网的信息流量情况,可以对全网进行故障测试、诊断和修复处理,还可以对一般被管结点进行远程加载、转储以及远程启动等控制。一般被管结点定时向网络管理结点提供自己位置信息和必要的管理信息。

从集中式网络管理模式的自身特点可以看出,集中式网络管理模式的优点是管理集中,有专人负责,有利于从整个网络系统的全局对网络实施较为有效的管理;缺点是管理信息集中汇总到网络管理结点上,导致网络管理信息流比较拥挤,管理不够灵活,管理结点如果发生故障有可能影响全网正常工作。

集中式网络管理模式比较适合于以下几种网络。

- (1) 小型局域网络。这种网络的结点不多,覆盖范围有限,集中管理比较容易。
- (2) 部门专用网络。特别是对于一些行政管理上比较集中的部门,如军事指挥机关、公安系统等,集中式网络管理模式与行政管理模式匹配,便于实施。
- (3) 统一经营的公共服务网。这种网络从经营、经济核算方面考虑,用集中式网络管理模式比较适宜。
- (4) 专用 C/S 结构网。这种结构,客户端和服务端专用化,客户端的结构已经简化,与服务器呈主从关系,网络管理功能往往集中于网络服务器。
- (5) 企业互连网络。在这种网络中,越来越多地引入各种专用网络互联设备,如路由器、桥接器、交换机和集线器等,它们本身已不是一个完整的计算机结点,但又在计算机网络中有着重要的地位,应有集中的网络管理结点对它们进行统一管理。

目前,单纯的集中式网络管理模式的应用并不常见,而分布式网络管理模式由于自身的特点则相对应用得比较广泛。

3.2.2 分布式网络管理模式

为了降低中心管理控制台、局域网连接、广域网连接以及管理信息系统人员不断增长的负担,就必须对被动式的、集中式的网络管理模式进行一个根本的改变。具体的做法是

将信息管理和智能判断分布到网络各处,使得管理变得更加自动,在问题源或靠近故障源的地方能够做出基本的故障处理决策。

分布式管理将数据采集、监视以及管理分散开来,它可以从网络上的所有数据源采集数据而不必考虑网络的拓扑结构。分布式管理为网络管理员提供了针对大型的、地理分布广泛的网络更加有效的管理方案。分布式网络管理模式主要有以下一些功能和特点。

1. 自适应基于策略的管理

自适应基于策略的管理是指对不断变化的网络状况做出响应并建立策略,使得网络能够自动与之适应,提高解决网络性能及安全问题的能力。自适应基于策略的管理减少了网络管理的复杂性,利用它,用户或者应用软件可以确定他们合适的服务质量级别以及带宽需求。例如,一个机构里的某位决策人员或某个敏感的多媒体应用,可以被认定或被确定来接受一个有保障的带宽或是高优先级别的服务。

2. 分布式的设备查找与监视

分布式的设备查找与监视是指将设备的查找、拓扑结构的监视以及状态轮询等网络管理任务从管理网站分配到一个或多个远程网站的能力。这种重分配既降低了中心管理网站的工作负荷,又降低了网络主干和广域网连接的流量负荷。

采用分布式管理,安装网络管理软件的网站可以配置“采集网站”或“管理网站”。采集网站是那些具有监视功能的网站,它们向有兴趣的管理网站通告它们所管理的网络的任何变化或拓扑结构。每个采集网站负责对一组用户可规范地称之为“域”的管理对象进行信息采集。域可以建立在一系列基准之上,包括拓扑或类型。

采集/管理网站跟踪着它们的域内所发生的网络的增加、移动和变化。在有规律的间歇期内,各网站的数据库将与同一级或高一级的网站进行同步调整。这就使得网址的信息系统管理员在监控他们自己资源的同时,也让全网络范围的管理员了解所有设备的现有状况。采集网站与管理网站之间的数据复制实际上也使得在网络上的任何控制台都能够看到整个网络设备的最新状况。

3. 智能过滤

为了在非常大的网络环境中限制网管信息流量超负荷,分布式管理采用了智能过滤器来减少网管数据。通过优先级控制,不重要的或不良的数据就会从系统中排除,从而使网络控制台能够集中处理高优先级的任务,如趋势分析和容量规划等。为了在系统中不同地点排除不必要的数据,分布式管理采用以下4种过滤器。

- 设备查找过滤器:规定采集网站应该查找和监视哪些设备。
- 拓扑过滤器:规定哪些拓扑数据被转发到哪个管理网站上。
- 映像过滤器:规定哪些对象将被包容到各管理网站的映像中去。
- 报警和事件过滤器:规定哪些报警和事件被转发给任意优先级的特定管理,目的是排除掉那些与其他控制台无关的事件。

4. 轮询引擎

轮询引擎可以自动地和自主地调整轮询间隙,从而在出现异常高的读操作或网络出现故障时,获得对设备或网段的运行及性能的更加明了的显示。

5. 分布式管理任务引擎

分布式管理任务引擎可以使网络管理更加自动,更加独立。其典型功能包括分布式软件升级及配置、分布式数据分析、分布式 IP 地址管理。

6. 分布式网络管理模式的优点

(1) 提供了网络的可扩展性,以适应全新的、不断扩大的网络应用。分布式管理的根本属性就是能容纳整个网络的增长和变化,这是因为随着网络的扩展,智能监视及任务职责会同时不断地被分布开来。

(2) 降低了网络管理的复杂性。随着网络结点在数量上的增多,网络结构变得更加复杂,在唯一的一台工作站上监视数以万计的结点显然是行不通的。本地管理控制台能够针对相应网段出现的问题,迅速有效地采取修正行动,能够有效地避免因问题由小变大,最后导致大面积网络瘫痪的状况。

(3) 网络管理的响应时间更快,性能更好。分布式管理还极大地减少了由网络管理生成的流量开销,其结果是网络的总体性能变得更好。

(4) 提供网络管理信息共享能力。分布式管理最重要的特性之一就是能提供共享“状态、监视及拓扑映像”信息的能力,这种智能的分布式网络管理信息共享极大地减轻了中心管理网站对内存及 CPU 资源的需求。同样重要的是,它还使得管理信息系统人员能够在企业网的任何地方,显示特定的状态、监视以及拓扑映像信息。

7. 分布式网络管理模式的适应范围

(1) 通用商用网络。国际上流行很广的一些商用计算机网络,如 DECnet 网、TCP/IP 网和 SNA 网等,就其管理模式而言,都属于上述分布式网络管理模式,因为它们并不设置专门网络管理结点,但仍可保证网络的正常运行,因而可以比较方便地适应各种网络环境的配置和应用。

(2) 对等 C/S 结构网络。对等 C/S 结构意味着网络中各结点基本上是平等、自治的,因而也便于实施分布式网管体制。

(3) 跨地区、跨部门的互联网络。这种网络不仅覆盖范围广、结点数量大,且跨部门甚至跨国界,难以实现集中管理。因此,分布式网络管理模式是互联网络的基础。

3.2.3 混合管理模式

所谓混合管理模式,就是集中式管理模式和分布式管理模式相结合的产物。

现代计算机网络系统正向进一步综合、开放的方向发展。因此,网络管理模式也在向分布式与集中式相结合的方向发展。集中或分布的网络管理模式,分别适用于不同的网络环境,各有优缺点。目前,计算机网络正向着局域网与广域网结合、专用网与公用网结合、专用 C/S 与互动 B/S 结构结合的综合互联网方向发展。计算机网络的这种发展趋势,促使网络管理模式向集中式与分布式相结合的方向发展,以便取长补短,更有效地对各种网络进行管理。按照系统科学理论,大系统的管理不能过分集中,也不能过于分散,宜采用集中式与分布式相结合的混合网络管理模式,应采用以下管理策略和方法。

(1) 以分布管理模式为基础,指定某个或某些结点为网络管理结点,指定专人负责,给予其较高的特权,可以对网络中其他结点进行监控管理,其他结点的报告信息也向指定

结点汇总。

(2) 部分集中,部分分布。网络中计算机结点,尤其是处理能力较强的中、小型计算机,仍按分布式管理模式配置,它们相互之间协同配合,实行网络分布式管理,保证网络的基本运行。同时在网络中又设置专门的网络管理结点,重点管理那些专用网络设备,同时也对全网的运行进行有效的监控,这种集中式与分布式相结合的网络管理模式是在多企业网络中自然形成的一种网管体制。

(3) 联邦制管理模式。这经常出现在一些大型跨部门、跨地区的因特网结构中,各部分有自己的网络,往往各有自己相对集中的管理模式,但整个因特网并没有一个总的集中管理实体,在一般情况下,互相并不干预,当涉及因特网正常运行、安全和性能优化等全局问题时,可通过各部门网络管理之间的通信来协调解决。这类似于一种联邦制国家之间的协调关系。

(4) 分级网中的分级管理。在一些大型部门、企业的行政体制就是一种分级树形管理模式,如政府机关、军事、银行、邮电、石油等部门和系统,它们的内部关系就是一种分级从属关系。因此,这些部门所建的计算机网络,在管理模式上也自然需要一种分级管理模式与之适应。在这种分级管理模式中,基层部门的网络有自己相对独立和集中的管理,它们的上级部门也有自己的网络管理,同时对它们的下属网络还具有一定的指导以及干预能力。

3.2.4 网络管理软件结构

网络管理软件包括三部分:用户接口软件、管理专用软件和管理支持软件。

1. 用户接口软件

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主机上,而且也可能出现在网管代理系统中,以便对网络资源实施本地配置、测试和排错。

若要实施有效的网络管理,用户接口软件应具备下列特点。

(1) 统一的用户接口。不论主机和设备出自何方厂家,运行什么操作系统,都需要统一的用户接口,这样才可以方便地对异构型网络进行监控。

(2) 具备一定的信息处理能力。对大量的管理信息要进行过滤、统计、求和,甚至进行简化,以免传递的信息量太大而阻塞网络通道。

(3) 图形用户界面。具有非命令行或表格形式的用户操作维护界面。

2. 管理专用软件

复杂的网络管理软件可以支持多种网络管理应用,如配置管理、性能管理和故障管理等。这些应用可以适用于各种网络设备和网络配置。

网络管理软件结构还表达了用大量的应用元素支持少量管理应用的设计思想。应用元素实现初等的通用管理功能(例如产生报警、对数据求和等),可以由多个应用程序调用。根据传统的模块化设计方法,还可以提高软件的重用性,产生高效率的实现。网络管理软件利用这种服务接口可以检索设备信息,设置设备参数;网管代理则通过服务接口向管理站通告设备事件。

3. 管理支持软件

管理支持软件包括 MIB 访问模块和通信协议栈。网管代理中的 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 中除保存本地结点专用的管理信息外,还保存着管理站控制的所有网管代理的有关信息。MIB 访问模块具有基本的文件管理功能,使得管理站或网管代理可以访问 MIB,同时该模块还能把本地的 MIB 数据转换成适用于网络管理系统传送的标准格式。通信协议栈支持结点之间的通信。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,虽然具体的实现可能有特殊的通信要求。

3.3 网络管理协议

网络管理系统中最重要的部分就是网络管理协议,它定义了网络管理者与网管代理间的通信方法。

在网络管理协议产生以前,管理者要学习各种从不同网络设备获取数据的方法,因为各个生产厂家使用专用的方法收集数据。相同功能的设备,不同的生产厂商提供的数据采集方法可能大相径庭。在这种情况下,制定一个行业标准的紧迫性越来越明显。

最初研究网络管理通信标准问题的是国际上最著名的国际标准化组织,其对网络管理的标准化工作开始于 1979 年,主要针对 OSI 七层协议的传输环境而设计。

ISO 的成果是 CMIS 和 CMIP。CMIS 支持管理进程和管理代理之间的通信要求,CMIP 则是提供管理信息传输服务的应用层协议,二者规定了 OSI 系统的网络管理标准。基于 OSI 标准的产品有 AT&T 的 Accumaster 和 DEC 公司的 EMA 等,HP 的 OpenView 最初也是按 OSI 标准设计的。

后来,Internet 工程任务组(IETF)为了管理网络数量以几何级数增长的 Internet,决定采用基于 OSI 的 CMIP 协议作为 Internet 的管理协议,并对它做了修改,修改后的协议被称为 CMOT。但由于 CMOT 迟迟未能出台,IETF 决定把已有的简单网关监控协议(SGMP)进一步修改后,作为临时的解决方案。这个在 SGMP 基础上开发的解决方案就是著名的简单网络管理协议,也称 SNMP v1(即 SNMP 协议的第 1 个版本)。

相对于 OSI 标准,SNMP 简单而实用。SNMP v1 最大的特点是简单,容易实现且成本低。此外,它的特点还有:可伸缩性,SNMP 可管理绝大部分符合 Internet 标准的设备;扩展性,通过定义新的“被管理对象”,可以非常方便地扩展管理能力;健壮性,即使在被管理设备发生严重错误时,也不会影响管理者的正常工作。

近年来,SNMP 发展很快,已经超越传统的 TCP/IP 环境,受到更为广泛的支持,成为网络管理方面事实上的标准。支持 SNMP 的产品中最流行的是 IBM 公司的 NetView、Cabletron 公司的 Spectrum 和 HP 公司的 OpenView。除此之外,许多其他生产网络通信设备的厂家,如 Cisco、Crossecomm 和 Proteon 等也都提供基于 SNMP 的实现方法。

如同 TCP/IP 协议簇的其他协议一样,早期的 SNMP 没有考虑安全问题,为此许多用户和厂商提出了修改 SNMP v1,增加安全模块的要求。于是,IETF 从 1992 年开始了具有较高安全性的 SNMP v2 的开发工作。SNMP v2 在提高安全性和更有效地传递管理

信息方面加以改进,具体体现在验证、加密和时间同步机制。1997年4月,IETF成立了SNMP v3工作组。SNMP v3的重点是安全、可管理的体系结构和远程配置。目前,SNMP v3已经是IETF提议的标准,并得到了供应商们的有力支持。

本节将对常规的网络管理协议逐一加以介绍。

3.3.1 简单网络管理协议

SNMP的体系结构分为SNMP管理者(SNMP manager)和SNMP代理者(SNMP agent),每一个支持SNMP的网络设备中都包含一个网管代理,网管代理随时记录网络设备的各种信息,网络管理程序再通过SNMP通信协议收集网管代理所记录的信息。从被管理设备中收集数据有两种方法:一种是轮询(polling)方法,另一种是基于中断(interrupt-based)的方法。

SNMP使用嵌入到网络设施中的代理软件来收集网络的通信信息和有关网络设备的统计数据。代理软件不断地收集统计数据,并把这些数据记录到一个管理信息库中,网络管理员(简称网管员)通过向代理的MIB发出查询信号可以得到这些信息,这个过程就叫轮询。为了能够全面地查看一天的通信流量和变化率,网络管理人员必须不断地轮询SNMP代理,每分钟就要轮询一次。这样,网管员可以使用SNMP来评价网络的运行状况,并揭示通信的趋势。例如,哪一个网段接近通信负载的最大能力或正在使用的通信出错等。先进的SNMP网管站甚至可以通过编程来自动关闭端口或采取其他矫正措施来处理历史的网络数据。

如果只是用轮询的方法,那么网络管理工作站总是在SNMP管理者控制之下,这种方法的缺陷在于信息的实时性,尤其是错误的实时性。多长时间轮询一次,轮询时选择什么样的设备顺序都会对轮询的结果产生重要的影响。轮询的间隔太短,会产生大量的且不必要的通信量;若间隔太长,而且轮询时顺序不对,那么有关一些大的灾难性事件的通知又会太慢,这就违背了积极主动的网络管理的目标。与之相比,当有异常事件发生时,基于中断的方法可以立即通知网络管理工作站,实时性很强。但这种方法也有缺陷,产生错误或自陷需要系统资源,如果自陷必须转发大量的信息,那么被管理设备可能不得不消耗更多的事件和系统资源来产生自陷,这将会影响到网络管理的主要功能。

而将以上两种方法结合的陷入制导轮询方法(trap-directed polling)可能是执行网络管理最有效的方法。一般来说,网络管理工作站轮询在被管理设备中的代理来收集数据,并且在控制台上用数字或图形的表示方法来显示这些数据,被管理设备中的代理可以在任何时候向网络管理工作站报告错误情况,而并不需要等到管理工作站为获得这些错误情况而轮询它的时候才会报告。

简单网络管理协议已经成为事实上的标准网络管理协议。由于SNMP首先是IETF的研究小组为了解决在Internet上路由器的管理问题而提出的,因此许多人认为SNMP只能在IP上运行。事实上,SNMP已被设计成与协议无关的网管协议,所以它可以在IP、IPX和AppleTalk等协议上使用。

简单网络管理协议的体系结构是从早期的简单网关管理协议(simple gateway management protocol,SGMP)发展而来的,是Internet组织用来管理TCP/IP因特网和