第 3 章　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 Internet。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。

知识培养目标

- 了解网络管理的基本架构；
- 了解网络管理的基本模式；
- 了解网络管理的基本协议。

能力培养目标

- 具备网络管理架构设计及应用的能力；
- 具备应用网络管理模式的能力；
- 具备理解和应用网络管理协议的能力。

课程思政培养目标

课程思政及素养培养目标如表 3-1 所示。

表 3-1　课程内容与课程思政培养目标关联表

知 识 点	知识点诠释	思 政 元 素	培养目标及实现方法
网络管理协议	网络管理约定的规范及要求	网络有协议标准、人类有行为规范。没有规矩不成方圆。要讲政治、讲规矩	培养学生的自觉性，并养成用法律、用制度、用社会行为规范约束自己行为的习惯。要求学生要讲政治、讲规矩
UDP 协议和 TCP 协议	TCP 协议能高效、可靠地传输网络数据。但要求对方必须在线并建立连接，若连接不上就不可传输数据；用 UDP 协议传输数据虽然不可靠，但无论对方是否在线都可传输数据。而且，TCP 协议的连接建立是基于 UDP 包的。UDP 协议和 TCP 协议在网络信息传输中各有千秋，缺一不可	人类是社会的组成部分，人与人之间相互信任、相信依存，才能成就大事	培养学生的团队协作精神，同学之间应该团结互助、相互关爱、相互学习、共同进步

3.1　网络管理基础架构

3.1.1　网络管理架构

网络管理系统可实现对网络的全面有效的管理，实现网络管理目标。在网络的运营管

理中,网络管理人员通过网络管理系统管理整个网络。概括地说,网络管理系统从逻辑上包括管理对象、管理进程、管理信息库和网络管理协议4部分。网络管理系统的逻辑架构如图3-1所示。

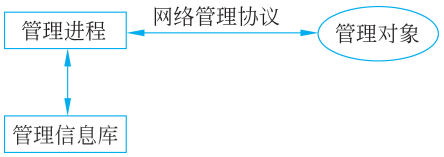

图3-1 网络管理系统的逻辑架构

1. 管理对象

管理对象是网络中具体可操作的数据。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,一般在网络管理站(网络管理中心)的主机上运行,它可以在SNMP的支持下命令管理代理执行各种管理操作。

管理进程负责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(MIB)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,方能达到真实地、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。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. 网络管理协议

网络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。管理协议可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。

管理站和网管代理者之间通过网络管理协议进行通信,网络管理者进程通过网络管理协议完成网络管理。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,获得的支持也最广泛,已经成为事实上的工业标准。

在这里,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、X.25)之上实现。SNMP通过用户数据报协议(UDP)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的控制下,负责解释SNMP消息和控制MIB指令。

3.1.2　网络管理者与网管代理

1. 概述

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。它采用一种独特的方式使两个管理进程之间相互作用，即管理进程与远程系统相互作用，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，都认同现代计算机网络管理系统由以下 4 个要素组成。

（1）网络管理者（Network Manager）；

（2）网管代理（Managed Agent）；

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

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

网络管理者（管理进程）是管理指令的发出者。网络管理者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固定，由每次通信的性质决定。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。

2. 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工作站、PC 等，一般位于网络系统的主干或接近于主干的位置，它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，具体的交换过程通过协议数据单元（Protocol Data Unit，PDU）进行。通常是管理站向网管代理发送请求 PDU，网管代理响应 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，这种消息称为事件报告或通知，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，其基本要素如下。

（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的实际监控的能力;

(4) 一个从所有被管网络实体的 MIB 中抽取信息的数据库。

3. 网管代理

网管代理是一个软件模块,它驻留在被管设备上。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。网管代理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给网络管理者,这些信息包括有关运行状态、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。

网管代理就像是被管理设备的信息经纪人,负责完成网络管理者布置的信息收集任务,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(MIB)中的信息来实现网络设备管理功能。

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 3 种。它们各有特色,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。

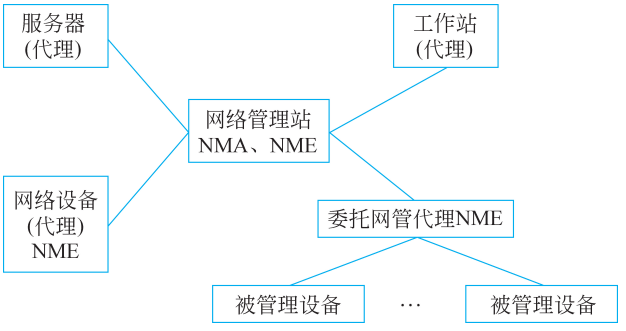

图 3-2 集中式网络管理模式

在集中式网络管理配置图中,有一个叫作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,委托网管代理用于管理一个或多个非标准设备,其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。

NME 的主要作用有以下 4 方面。

（1）收集统计信息；

（2）记录状态信息；

（3）存储有关信息，响应请求，传送信息；

（4）根据指令，设置或改变参数。

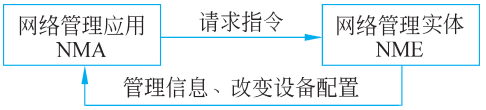

图 3-3　NME 与 NMA 的关系

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的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的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适用于以下几种网络。

（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：这种结构的客户机和服务器专用化，客户机的结构已经简化，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）企业互联网络：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，应由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的不同结点，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最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的更加有效的管理方案。分布式网络管理模式主要有以下功能。

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其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/管理网站跟踪着其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。这使得网址的信息系统管理员在监控自己资源的同时,也让全网络范围的管理员了解所有设备的现状。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查看整个网络设备的最新状况。

3. 智能过滤

为了在庞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,从而使得网络控制台能够集中处理高优先级的事务,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。

(1) 设备查找过滤器:规定采集网站应该查找和监视哪些设备。

(2) 拓扑过滤器:规定哪些拓扑数据被转发到哪个管理网站上。

(3) 映像过滤器:规定哪些对象将被包容到相应的管理网站的映像中去。

(4) 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分布开来。

（2）降低网络管理的复杂性。随着网络结点数量的增多，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行不通。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，有效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。分布式管理极大地减少了由网络管理生成的流量开销，其结果是网络总体性能的提升。

（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具备共享“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，查看特定的状态、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、TCP/IP 网、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的网络管理结点，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管理模式。

3.2.3　混合网络管理模式

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，各有其优缺点。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 Internet 方向发展。计算机网络的这种发展趋势，促使网络管理模式也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则向指定结点汇总。

（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。经常出现在一些大型跨部门、跨地区的 Internet 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 Internet 并没有一个总的集中管

理实体,在一般情况下,相互之间并不干预,当涉及 Internet 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。一些大型部门、企业的行政体制就是一种分级树状管理模式,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,同时对下属网络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 3 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,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 网络管理基本协议

3.3.1 简单网络管理协议

1. SNMP 概述

简单网络管理协议(Simple Network Management Protocol,SNMP)的体系结构分为SNMP 管理者(SNMP Manager)和 SNMP 代理(SNMP Agent),每个支持 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,网络管理进程再通过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(MIB)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,网络管理员必须不断地轮询SNMP 代理,每分钟就要轮询一次。

SNMP 的体系结构从早期的简单网关监控协议(Simple Gateway Monitoring Protocol,SGMP)发展而来,被 Internet 组织用来管理 TCP/IP 互联网和以太网。

2. SNMP 的基本组成

SNMP 管理模型由 3 部分组成:管理代理(Agent)、管理进程(Manager)和管理信息库(MIB),如图 3-4 所示。

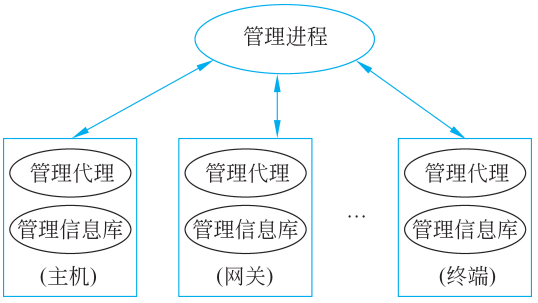

图 3-4　SNMP 基本结构图

1) 管理代理

管理代理是一种软件,在被管理的网络设备中运行,负责执行管理进程的管理操作。管理代理直接操作本地信息库(MIB),如果管理进程需要,它可以根据要求改变本地信息库或提取数据传回到管理进程。管理代理的主要作用列举如下。

每个管理代理均拥有自己的本地 MIB,一个管理代理管理的本地 MIB 不一定具有Internet 的全部内容,而只需要包括与本地设备或设施有关的管理对象。

管理代理有以下两个基本功能。

- 在 MIB 中读取各种变量值;
- 在 MIB 中修改各种变量值。

这里的变量值就是管理对象。

2) 管理进程

管理进程是用于对网络中的设备和设施进行全面管理和控制的软件。

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。

SNMP 更多内容详见第 4 章。

3.3.2 域名系统

1. DNS 的引入

1) DNS 的基本概念

在引入域名系统(Domain Name System,DNS)以前,网络上的用户需要维护一个 HOSTS 配置文件,这个文件包括当此工作站和网络上的其他系统通信时所需要的一切信息。每台机器的 HOSTS 文件均需要手工单独更新,几乎没有自动配置。

HOSTS 文件包括名字和 IP 地址的对应信息。当一台计算机需要定位网络上的另一台计算机时,就会查看本地 HOSTS 文件,如果在 HOSTS 文件中没有关于此计算机的表项,说明其不存在。域名服务 DNS 改变了这一切,DNS 允许系统管理员使用一个服务器作为 DNS 主机。

DNS 就如其组织结构分层一样,从顶级 DNS 根服务器向下延伸,并把名字和 IP 地址传播到遍布世界的各个服务器上。DNS 服务器不在本地存储全部的名字和 IP 地址的映射,一旦 DNS 服务器在自身的数据库中没有找到 IP 地址,它会请求上一级 DNS 服务器查看是否能找到这个 IP 地址,这个过程会继续下去直到找到答案或超时出错。

用户有一个顶级域,如 COM 或 EDU。顶级域又称为通用名,因为它们包含层次在其下面的域和子域,它们非常像树根。从顶级移至中间级,中间域名的例子包括 coke.com、whitehouse.gov 以及 dimey.com。除美国之外,所有网站的域名都必须指定国家和地区域。例如 www.bbc.co.uk 是 BBC 的 Web 站点,它是一个商业站点(这里 co 和 com 相似),位于英国(UK)。

2) DNS 的使用方式

为了把名字映射成 IP 地址,应用程序必须调用一个名叫解析器(Resolver)的库,参数为域名。解析器将用户数据报协议(UDP)分组传送到本地 DNS 服务器上,本地 DNS 查找名字并将 IP 地址返回给解析器,解析器再把它返回给调用者。有了 IP 地址,程序就可以和目的方建立 TCP 连接,或者向它发送 UDP 分组信息。

2. DNS 域名空间

DNS 的域名空间是由树状结构组织的分层域名组成的集合。

DNS 域名空间树的最上面是一个无名的根(root)域,在根域之下就是顶级域名,如 com、edu、gov、org、mil、net 等。所有的顶级域名都由 Internet 网络信息中心(InternetNIC)控制。表 3-2 列出的是常用 DNS 顶级域名。

顶级域名主要分为两类:组织性域和地域性域。

顶级域名之下是二级域名。二级域名通常是由顶级域名管理中心授权的。一个拥有二

表 3-2　常用 DNS 顶级域名

域名字	含　义	域名字	含　义
com	商业组织	net	网络组织和 ISP(Internet 服务供应商)等
edu	教育机构	org	非商业组织
gov	政府部门	cn	用于国家代码的域名,cn 表示中国
mil	军队组织		

级域名的单位可以根据自己的情况,再将二级域名分为更低级的域名授权给单位下面的部门,如图 3-5 所示。

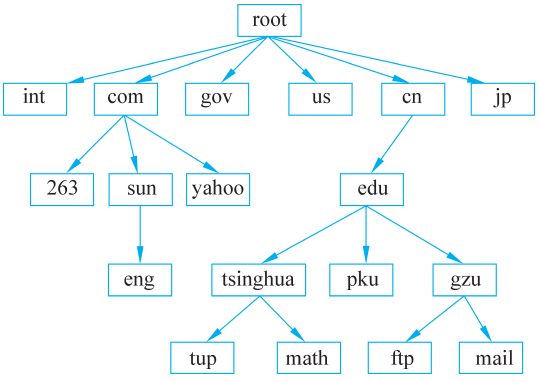

图 3-5　Internet 域名结构

DNS 域名树的最下面的叶结点为单个的计算机,域名的级数通常不多于 5 个。

在 DNS 树中,每一个结点都用一个简单的字符串(不带点)标识。这样,在 DNS 域名空间的任何一台计算机都可以用从叶结点到根的结点标识,中间用点“.”连接的字符串来标识:叶结点名.三级域名.二级域名.顶级域名。

3. 域名服务器

域名服务器负责管理存放主机的 IP 地址以及域名和 IP 地址映射表。域名服务器分布在不同的地域,它们之间通过特定的方式联络,这样可以保证用户通过本地的域名服务器查找到 Internet 上所有的域名信息。

所有域名服务器的数据库文件中的主机和 IP 地址的集合构成 DNS 域名空间。

4. 域名解析服务

DNS 域名服务在 Internet 中起着至关重要的作用,其他任何服务都依赖于域名服务。因为任何服务都需要进行域名到 IP 地址,或 IP 地址到域名的转换,也就是所谓的域名解析。

Internet 上的域名服务器也是按照层次来安排的。每个域名服务器只对域名体系中的一部分进行管理。例如,根服务器(Root Server)用来管理顶级域(如 com)。根服务器并不直接对顶级域下面所属的所有域名进行转换,但根服务器一定能够找到所有的二级域名服务器,如图 3-5 所示。

Internet 允许各个单位和部门根据本单位的具体情况,将本单位的域名划分为若干域

名服务器管理区,并在各个管理区设置相应的授权服务器。

3.3.3 网间网协议

1. IP协议概述

网间网协议(Internet Protocol,IP),又称网际协议,是通过网络连接的源计算机和目的计算机之间的信息传送协议。它提供对数据大小的重新组装功能,以适应不同网络对报文的要求。IP的任务是把数据从源传送到目的地,不负责保证传送的可靠性和流量控制。

IP分组分为头和数据区。分组的头包含源地址和目的地址(IP地址)。IP分组可以为任意长度(1~256B),当它们从一台机器移动到另一台机器时,必须经由物理网络帧传输。

IP地址是一个逻辑地址。它独立于任何特定的网络硬件和网络配置,不管物理网络的类型如何,它都有相同的格式。IP地址分为4字节,由两部分合成,第一部分是IP网络号,第二部分是主机号。

2. 子网

同一网络中的所有主机都必须有相同的网络号。当网络扩容时,这种IP编址特性会引发问题。例如,某公司在Internet上有一个C类地址局域网。一段时间后,其机器数超过了254台,因此需要分配另一个C类地址;或该公司又有了一个不同类型的局域网,需要使用与原先网络不同的IP地址。其结果可能是要创建多个局域网,各个局域网都有它自己的路由器和C类网络地址。

随着局域网的增加,管理成为一件很困难的工作。每次安装新网络时,系统管理员都要向网络信息中心NIC申请一个新的网络号。然后向全世界公布该网络号;当把机器从一个局域网上移到另一个局域网上时,必须更改IP地址,同时修改其配置文件并向全世界公布其IP地址。

解决这个问题的办法是:在网络内部分组,对外仍保留之前的单一网络。该内部分组称为子网。

一个被子网化的IP地址实际包含3部分:网络号、子网号、主机号。其中,子网号和主机号由原先IP地址的主机地址部分分割成两部分得到。因此,用户分子网的能力取决于被子网化的IP地址类型。IP地址中主机地址位数越多,划分的子网和主机就越多。然而,子网减少了能被寻址的主机数量,这是因为主机地址的一部分用于子网号。子网由伪IP地址(又称"子网掩码")标识。

对网络的外部而言,子网是不可见的,因此分配一个新子网不必与NIC联系,也不需改变外部数据库。

使用A类和B类IP地址的单位可以把它们的网络划分成若干部分,每部分称为一个子网。每个子网对应于一个下属部门或一个地理范围(如一座或一个小院的数栋办公楼),或者对应一种物理通信介质(如以太网,点到点连接线路或X.25网)。它们通过网关互联或进行必要的协议转换。

划分子网以后,每个子网看起来就像一个独立的网络。对于远程的网络而言,它们不知道这种子网的划分。在单位网络内部,IP软件识别所有以子网作为目的地的地址,将IP分组通过网关从一个子网传输到另一个子网。当一个IP分组从一台主机送往另一台主机时,它的源地址和目标地址被掩码,子网掩码的主机号部分是0,网络号部分的二进制表示码全

是 1，子网号部分的二进制表示码也全是 1。因此，使用 4 位子网号的 B 类地址的子网掩码是 255.255.240.0。

3. IP 地址转换

对于小型网络，可以使用 TCP/IP 体系提供的叫作 HOSTS 的文件来进行从主机域名到 IP 地址的转换。文件 HOSTS 上有许多主机名字到 IP 地址的映射，供主叫主机使用。

对于大型网络，则可在网络的多个地方放置域名系统（DNS）服务器，分层次存放主机域名到 IP 地址转换的映射表。

IP 地址到物理地址的转换由地址转换协议（ARP）来完成。由于 IP 地址是 32 位，而局域网的物理地址（即 MAC 地址）是 48 位，因此它们之间不是简单的转换关系。

3.3.4　传输控制协议

1. TCP 的基本概念

传输控制协议（Transmission Control Protocol，TCP）是一个基于连接的可靠传输协议，TCP 处于应用层和网络层之间，实现端到端的通信，也可以说传输控制协议是端服务协议。

如果一个报文段较大，路由器会将其分解为多个报文段，每个新的报文段都有自己的 TCP 头和 IP 头，所以通过路由器对报文段进行分解会增加系统的总开销。

TCP 实体的基本协议是滑动窗口协议。当发送方传送一个报文段时，还要启动计时器。当该报文段到达目的地后，接收方的 TCP 实体给发送端发送一个报文段，其中包括一个确认序号，该序列号与收到的下一个报文段的顺序号相同。如果发送方的定时器在确认信息到达之前超时，发送方会重发该报文段。

TCP 会为它的高层协议数据流中的每一字节分配一个顺序号。在与对等 TCP 交换报文段时，它会给这些段附加控制信息，包括该段中第一字节的顺序号以及该段中所有数据字节的个数。这样就使得接收端 TCP 能将这些段还原成一个不间断的数据流发送给它的高层协议。

当需要重传一系列报文段时，TCP 可以方便地对数据进行重新封装。为了提高线路通信效率，往往传输的段应尽可能大一些，从而降低报文段头部信息在用户数据中的占比。

图 3-6 展示了从发送方的高层协议通过 TCP 到达接收方的高层协议的数据传输过程。

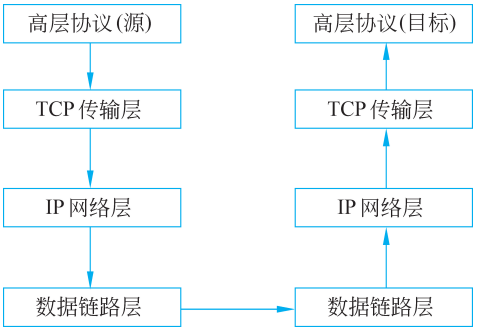

图 3-6　TCP/IP 报文段传输过程

TCP/IP 报文段的传输过程说明如下。

(1) 发送方的高层协议发出一个数据流给它的 TCP 实体进行传输。

(2) TCP 将数据流分段。可提供的传输措施包括：全双工式的定时重传、顺序传递、安全性指定和优先级指定、流量控制、错误检测等。

(3) IP 对这些报文段执行其服务过程，包括创建 IP 分组、数据报分割等，并在数据报通过数据链路层和物理层后经过网络传给接收方的 IP。

(4) 接收方的 IP 在校验和重组分段后，将数据报以段的形式发送给接收方的 TCP。

(5) 接收方的 TCP 完成它自己的服务，将报文段恢复成原来的数据流形式，发送给接收方的高层协议。

TCP 的特点如下。

- 面向连接；
- 可靠的数据传递；
- 具有流量控制能力；
- 具有拥塞控制能力；
- 只支持点到点的连接，不支持点到多点(组播)的连接。

2. 端口和套接字

UDP 和 TCP 都使用了应用层接口处的端口与上层的应用进程进行通信。为了识别不同的应用进程，TCP 中引进了端口和套接字的概念，每个端口均有一个称为端口号的 16 位标识符。当传输层收到了互联网络层提交上来的数据时，就要根据其首部中的端口号来决定应当通过哪一个端口把数据上交给接收此数据的应用进程。

TCP 连接由通信双方的套接字确定。套接字为通信双方的输入和输出所用，因而是全双工式的。TCP 规定，端口可与任何进程自由连接，且由实现 TCP 的各操作系统环境自行决定。端口还有一些基本的约定，例如，对一些公共的服务规定使用固定的端口号，FTP 的端口号为 20 和 21、Telnet 的端口号为 23、SMTP 的端口号为 25、HTTP 的端口号为 80。

3. TCP 服务

尽管 TCP 和 UDP 都使用相同的网络层(IP)，TCP 却向应用层提供与 UDP 完全不同的服务。TCP 提供一种面向连接的、可靠的字节流服务。

面向连接表明两个使用 TCP 的应用(通常是一个客户和一个服务器)在彼此交换数据之前必须先建立一个 TCP 连接会话。这一过程与打电话很相似，先拨号振铃，等待对方摘机应答后，才自我介绍和交流。

在一个 TCP 连接中，仅有两方进行通信。TCP 通过下列方式保证传输的可靠性。

(1) 应用数据分割成 TCP 认为最适合发送的数据块。而 UDP 应用程序产生的数据报长度将保持不变。由 TCP 传递给 IP 的信息单位称为报文段或段。

(2) 当 TCP 发出一个段后，启动定时器，等待目的端确认收到这个报文段。如果不能及时收到一个确认(即超时)，将重发这个报文段。

(3) 当 TCP 收到发自 TCP 连接另一端的数据，将发送一个确认。

(4) TCP 将保持其首部和数据的校验和。这是一个端到端的校验和，目的是检测数据在传输过程中是否发生了变化。如果收到段的校验和有差错，TCP 将丢弃这个报文段并否认应答，希望发送端在超时后重发。

(5) 由于 TCP 报文段作为 IP 数据报来传输，而 IP 数据报的到达可能会失序，因此 TCP 报文段的到达也可能会失序。如果必要，将对收到的数据进行重新排序，并将收到的数据以正确的顺序交给应用层。

(6) 由于 IP 数据报会发生重复(这是由于未及时收到“确认”消息所引起的)，TCP 的接收端必须丢弃重复的数据。

(7) TCP 还能提供流量控制。TCP 连接的每一方都有固定大小的缓冲空间。TCP 的接收端只允许另一端发送接收端缓冲区所能接纳的数据，这将能有效地防止快发慢收而致使接收方主机的缓冲区溢出。

3.3.5　用户数据报协议

用户数据报协议(User Datagram Protocol，UDP)采取无连接方式提供高层协议间的事务处理服务，允许互相发送数据报。也就是说，UDP 是在计算机上规定用户以数据报方式进行通信的协议。UDP 与 IP 的差别在于，一般用户无法直接使用 IP，而 UDP 是普通用户可直接使用的，故称为用户数据报协议。UDP 必须在 IP 上运行，即它的下层协议是以 IP 作为前提的。

由于 UDP 是一种无连接的数据报投递服务，所以不能保证可靠投递。它与远方的 UDP 实体不建立端到端的连接。而只是将数据报送上网络，或者从网上接收数据报。UDP 根据端口号对若干个应用程序进行多路复用，并能利用校验和检测数据的完整性。

与传输控制协议 TCP 类似，计算机上的应用程序和 UDP 的接口是 UDP 端口。这些端口是从 0 开始的数字编号，每种应用程序都在属于它的固定端口上等待来自其他计算机的客户的服务请求。例如，简单网络管理协议(SNMP)服务方(又称代理)总是在 161 号端口上等待远方客户的服务请求。一台计算机只能有一个 SNMP 代理程序。当某台计算机的客户请求 SNMP 服务时，就把请求发到备有这一服务的目标计算机的 161 号 UDP 端口。

UDP 保留应用程序定义的报文边界，它从不把两个应用报文组合在一起，也不把单个应用报文划分成几部分。也就是说，当应用程序把一块数据交给 UDP 发送时，这块数据将作为独立的单元到达对方的应用程序。例如，如果应用程序把 5 个报文交给本地 UDP 端口发送，那么接收方的应用程序就需要从接收方的 UDP 端口读 5 次，而且接收方收到的每个报文的大小都和发出的报文大小一致。

TCP/IP 主机的 UDP 模块必须具备产生和验证 UDP 校验和的功能。应用程序使用服务时可以选择是否生成 UDP 校验和，默认值是生成。当 IP 模块收到一个 IP 分组并且发现该分组的头部类型(type)段标明为 UDP 时，就将其中的 UDP 数据报传给 UDP 模块。UDP 模块接收由 IP 模块传来的 UDP 数据报，并检测 UDP 校验和。如果校验和是 0，就表明发送方没有计算 UDP 校验和。如果校验和非 0，且检测的结果不正确，那么 UDP 模块就会抛弃该数据报。如果校验和有效，UDP 模块就检测该数据报的目标端口号，如果其端口号与本地的一个应用程序被指定的端口号符合，就将数据中的应用报文放入队列，让相关的应用程序来读取。

UDP 数据报的格式如图 3-7 所示。

字段说明如下。

(1) UDP 源端口号：发送端端口号是任选项。该端口号若被指定，当接收进程返回数

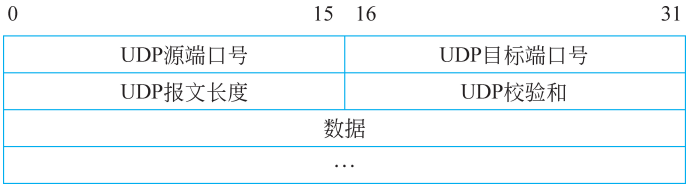

图 3-7　UDP 数据报格式

据时,这些数据就不会被别人得到。若不想指定这个域时,将其值设置为 0 即可。

(2) UDP 目标端口号:该端口号用以在等待数据报的进程之间进行多路分离,也就是具有接收主机内与特定应用进程相关联的地址的意义。

(3) UDP 报文长度:表示数据报头及其后面数据的总长度。最小值是 8 字节,即 UDP 数据报头长度。

(4) UPD 校验和:根据 IP 分组头中的信息作出伪数据报头,跟 UDP 数据报头和数据一起进行 16 位的校验和计算。对数据为奇数字节的情况,增加一个全 0 字节使其成为偶数字节后再行计算。校验和计算的方法与 IP 中所使用的校验和计算方法相同。当校验和的结果为 0 时,将其所有位都置成 1。伪报头是放在 UDP 报头前边的,其格式如图 3-8 所示。

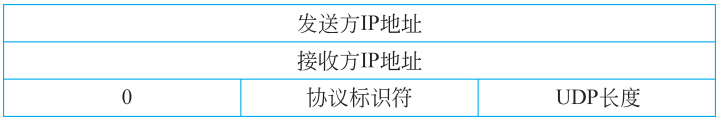

图 3-8　计算 UDP 校验和使用的 12 字节的伪报头

使用伪报头的目的在于验证 UDP 数据报是否已到达它的正确报宿。理解伪报头的关键是,要认识到正确报宿的组成中包括一台唯一的计算机和这个计算机上唯一的协议端口。UDP 报头本身只确定了协议端口的编号,因而,为验证报宿,发送方计算机的 UDP 要计算一个校验和,这个校验和包括报宿主机的 IP 地址,也包括 UDP 数据报。

在目的地,UDP 使用从运载 UDP 报文的 IP 分组头中得到的目标 IP 地址验证校验和,如果校验和一致,那么数据报确实已到达所希望的报宿主机和这个主机内的正确协议口。

在伪报头中标有发送方 IP 地址和接收方 IP 地址的字段,分别包括报源 IP 地址和报宿 IP 地址,这两个地址在发送 UDP 数据报时都要用到。协议标识符段包括 IP 分组的协议类型码,对于 UDP 应该是 17。标明 UDP 长度的段包括 UDP 数据报长度(不包括伪报头)。为验证校验和,接收者必须从当前 IP 分组头中提取这些段,把它们汇集到伪 UDP 报头格式中,再重新计算这个校验和。

UDP 在 TCP 及 Internet 的名字服务等应用中使用。在 UNIX 中,UDP 也在一些检测网络用户的命令中使用。Sun Microsystems 公司开发的 NFS(Network File System)也是在 UDP 上实现的。由于 UDP 简单,在每个系统中运行时网络负载很轻,故有利于大量数据的高速传送。

UDP 的特点如下。

- 无连接操作;
- 传输不可靠;

- 无流量控制和拥塞控制；
- 在 UDP 分组头中的源端口号及目的端口号提供了一种简单的复用/解复用服务；
- 支持点到点和点到多点(组播)的传输。

3.3.6　Internet 控制报文协议

如果一个网关不能为 IP 分组选择路由，或者不能递交 IP 分组，或者这个网关测试到某种不正常状态，例如，网络拥挤影响 IP 分组的传递，就需要使用 Internet 控制报文协议(Internet Control Message Protocol，ICMP)来通知源主机采取措施，避免或纠正这类问题。

ICMP 是在网络层中与 IP 一起使用的协议，ICMP 通常由某个监测到 IP 分组中错误的站点产生。从技术上说，ICMP 是一种差错报告机制，这种机制为网关或目标主机提供一种方法，使它们在遇到差错时能把差错报告给原始报源。例如，如果 IP 分组无法到达目的地，那么就可能使用 ICMP 警告分组的发送方：网络、机器或端口不可到达。ICMP 还会通知发送方网络出现拥挤。

ICMP 是网间网协议(IP)的一部分，ICMP 通过 IP 发送。ICMP 的使用主要包括下面 3 种情况。

(1) IP 分组不能到达目的地；

(2) 接收设备接收 IP 分组时，缓冲区大小不够；

(3) 网关或目标主机通知发送方主机，如果这种路径确实存在，应该选用较短的路径。

ICMP 数据报和 IP 分组一样不能保证可靠传输，因此，ICMP 信息有可能丢失。为了防止 ICMP 信息无限地连续发送，ICMP 数据报传输的问题不能再使用 ICMP 传输。另外，对于被划分成片的 IP 分组而言，只对分组偏移值等于 0 的分组片(也就是第一个分组片)使用 ICMP。

ICMP 报文有两种：一种是错误报文，另一种是信息报文。错误报文是当报文在传输过程中发生错误时(如超时)所产生的 ICMP 报文，而信息报文则用于查询(请求)或通告(应答)网络运行状态而产生的 ICMP 报文(如 ping 命令的请求报文与应答报文、路由的请求与应答报文)。每个 ICMP 报文的开头都包含 4 个字段：1 字节的类型字段、1 字节的编码字段和 2 字节的校验和字段。8 位的类型字段标志，表示不同的 ICMP 报文。16 位的校验和的算法与 IP 头的校验和算法相同，但检查范围限于 ICMP 报文结构。

表 3-3 列出了 ICMP 8 位类型字段定义的部分常用报文的名称，每一种都有自己的 ICMP 头部格式。

表 3-3　常用 ICMP 报文类型表

类 型 字 段	ICMP 报文
0	回送应答(用于 ping 命令)
3	无法到达目的地
4	抑制报源(拥挤网关丢弃一个 IP 分组时发给报源)
5	重定向路由
8	回送请求(用于 ping 命令)

续表

类 型 字 段	ICMP 报文
11	IP 分组超时
12	一个 IP 分组参数错
13	时间戳请求
14	时间戳应答
15	信息请求已过时
17	地址掩码请求(发给网关或广播)
18	地址掩码应答(网关回答的子网掩码)

回送请求报文(类型=8)用来测试发送方到达接收方的通信路径。在许多主机上,这个功能叫作 ping。发送方发送一个回送请求报文,里面包含一个 16 位的标识符及一个 16 位的序列号,也可以将数据放在报文中传输。当目的地址机器收到报文时,把源地址和目标地址倒过来,重新计算校验和,并传回一个回送应答(类型=0)报文。在有的情况下,数据字段中的内容也要返回给发送方。

3.3.7 Internet 组管理协议

TCP/IP 传送形式有 3 种:单目传送、广播传送和多目传送(组播)。

单目传送是一对一的,广播传送是一对多的,组内广播也是一对多的,但组员往往不是全部成员,因此可以说组内广播是一种介于单目与广播传送之间的传送方式,称为多目传送,也称为组播。

对于一个组内广播应用来说,假如用单目传送实现,则采用端到端的方式完成,如果小组内有 n 个成员,组内广播需要 $n-1$ 次端到端传送,组外对组内广播需要 n 次端到端传送;假如用广播方式实现,则会有大量主机收到与自己无关的数据,造成主机资源和网络资源的浪费。因此,IP 协议对其地址模式进行扩充,引入多目编址机制以解决组内广播应用的需要。

IP 协议引入组播之后,有些物理网络技术开始支持多目传送,如以太网技术。当多目跨越多个物理网络时,便存在多目组的寻径问题。传统的网关是针对端到端而设计的,不能完成多目寻径操作,于是多目路由器用来完成多目数据报的转发工作。

IP 采用 D 类地址支持多点传送。每个 D 类地址代表一组主机。共有 28 位可用来标识小组。当一个进程向一个 D 类地址发送分组信息时,会尽最大努力将它发送给小组成员,有些成员可能收不到这个分组。

Internet 支持两类组地址:永久组地址和临时组地址。永久组地址总是存在而且不必创建,每个永久组都有一个永久组地址。永久组地址的实例如表 3-4 所示。

临时组必须先创建后使用,一个进程可以要求其主机加入或脱离特定的组。当主机上的最后一个进程脱离某个组后,该组就不再在这台主机中出现。每个主机都要记录它当前的进程属于哪个组。

表 3-4　永久组地址

永久组地址	描　　述
224.0.0.1	局域网上的所有系统
224.0.0.2	局域网上的所有路由器
224.0.0.5	局域网上的所有开放最短路径优先(OSPF)路由器
224.0.0.6	局域网上的所有指定 OSPF 路由器

组播路由器可以是普通的路由器。各个多点播送路由器周期性地将一个硬件多点播送信息发送给局域网上的主机(目的地址为 224.0.0.1),要求它们报告其进程当前所属的是哪一组,各主机将选择的 D 类地址返回。

多目路由器和参与组播的主机之间交换信息的协议称为 Internet 组管理协议,简称为 IGMP(Internet Group Management Protocol)。IGMP 提供一种动态参与和离开多点传送组的方法。它让一个物理网络上的所有系统知道主机当前所在的组播组。组播路由器需要这些信息以便知道组播数据报应该向哪些接口转发。

IGMP 与 ICMP 的相似之处在于它们都使用 IP 服务的逻辑高层协议。事实上,因为 IGMP 影响了 IP 协议的行为,所以 IGMP 是 IP 的一部分,并作为 IP 的一部分来实现。为了避免网络通信量问题,当投递到多点传送地址中的消息被接收时,不生成 ICMP 错误消息。

当路由器有一个 IGMP 消息需要发送时,首先会创建一个 IP 数据报,然后再把该 IGMP 消息封装在 IP 数据报中进行传输。

IGMP 工作过程如下。

目的 IP 地址 224.0.0.1 被称为全主机组地址。它涉及物理网络中的所有具备组播能力的主机和路由器。当接口初始化后,所有具备组播能力接口上的主机均自动加入这个组播组。这个组的成员无须发送 IGMP 报告。

主机通过组地址和接口来识别组播组。主机必须保留一张表,该表中包含所有含有一个以上进程的组播组以及组播组中的进程数量。

IGMP 工作过程分为以下两个阶段。

第 1 阶段:某主机加入一个新的多目组时,会将其全主机多目地址组员身份传播出去。本地多目路由器收到该信息后,一方面将此信息记录到相应表格中;另一方面向 Internet 上的其他多目路由器通知此组员身份信息,建立必要的路径。

第 2 阶段:为适应组员身份的动态变化,本地多目路由器会周期性地查询本地主机,以确定哪些主机仍然属于哪些多目组。假如查询结果表明某多目组中已无本地主机成员,多目路由器一方面将停止通告相应的组员身份信息,另一方面不再接收相应的多目数据报。

组播是一种将报文发往多个接收者的通信方式。在许多应用中,它比广播更好,因为组播降低了不参与通信的主机的负担。简单的主机成员报告协议是组播的基本模块。同一局域网的组播或跨越邻近局域网的组播需要使用这些技术。广播通常局限在单个局域网中,目前许多使用广播的应用,都可采用组播来替代。

3.3.8 公共管理信息协议

1. 概述

ISO制定的公共管理信息协议(Common Management Information Protocol,CMIP)主要针对OSI 7层协议模型的传输环境设计而成。在网络管理过程中,CMIP不通过轮询而是通过事件报告开展工作,网络中的各个监测设施在发现被检测设备的状态和参数发生变化后将及时向管理进程进行事件报告。管理进程先对事件进行分类,根据事件发生时对网络服务影响的大小来划分事件的严重等级,再产生相应的故障处理方案。

CMIP与SNMP相比,两种管理协议各有所长。SNMP是Internet组织用来管理TCP/IP互联网和以太网的,由于实现、理解和排错很简单,所以受到很多产品的广泛支持,但是安全性较差。CMIP是一个更为有效的网络管理协议。一方面,CMIP采用了报告机制,具有及时性的特点;另一方面,CMIP把更多的工作交给管理者去做,减轻了终端用户的工作负担。此外,CMIP建立了安全管理机制,提供授权、访问控制、安全日志等功能。但由于CMIP涉及面太广,大而全,所以实施起来比较复杂且花费较高。

CMIP的所有功能都要映射到应用层的相关协议上实现。管理联系的建立、释放和撤销是通过联系控制协议(Association Control Protocol,ACP)实现的。操作和事件报告是通过远程操作协议(Remote Operation Protocol,ROP)实现的。

2. 管理模型

CMIP管理模型有以下3种。

(1) 组织模型:用于描述管理任务如何分配。

(2) 功能模型:用以描述各种网络管理功能和它们之间的关系。

(3) 信息模型:提供描述被管对象和相关管理信息的准则。

从组织模型来说,所有CMIP的管理者和被管代理者位于一个或多个域中,域是网络管理的基本单元。从功能模型来说,CMIP主要实现故障管理、配置管理、性能管理、计费管理和安全管理,每种管理均由一个特殊管理功能领域(Special Management Functional Area,MFA)负责完成。从信息模型来说,CMIP的MIB库是面向对象的数据存储结构,每一个功能领域作为一个"对象"存入MIB库的存储单元。

CMIP是一个完全独立于下层平台的应用层协议,它的5个特殊管理功能领域由多个系统管理功能(SMF)支持。相对来说,CMIP是一个相当复杂和具体的网络管理协议。它的设计宗旨与SNMP相同,但用于监视网络的协议数据报文相对更多。CMIP共定义了11类PDU。在CMIP中,变量以非常复杂和高级的对象形式出现,每一个变量都包含变量属性、变量行为和通知。CMIP中的变量体现了CMIP MIB库的特征,并且这种特征表现了CMIP的管理思想,即基于事件而不是基于轮询。每个代理独立完成一定的管理工作。

3.3.9 远程监控协议

1. 概述

远程网络监控(Remote Network Monitoring,RMON)协议最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON的网络监视数据包含一组统计数据和性能指标,它们在不同的监视器(或称探测器)和控制台系统之间相互交换。结果数据