

第 2 章 局域网规划与设计

知识目标

- ◎ 了解网络需求分析的内容和方法
- ◎ 掌握网络逻辑结构设计的内容和方法
- ◎ 掌握网络物理结构设计的内容和方法
- ◎ 了解网络工程实施方法和施工验收方法
- ◎ 掌握局域网的总体设计思路和方法

技能目标

- ◎ 能够进行网络的需求分析
- ◎ 能够进行网络逻辑结构设计
- ◎ 能够进行网络物理结构设计
- ◎ 能够独立地进行局域网的规划和设计,并写出设计规划方案

要使用局域网,必须建设局域网,建设局域网的首要条件就是要规划和设计局域网。任何单位和个人组建局域网都有特定的目的和要求。网络设计人员在具体施工之前应该做到完全理解客户的需求,从而避免日后出现组建的网络不能满足用户需求或者性能要求的现象。在详细需求分析以后,根据需求进行网络规划,为网络设计提供理论依据。

2.1 网络需求分析

需求分析是从软件工程和管理信息系统中引入的概念,是任何一个工程实施的第一个环节,也是关系一个网络工程成功与否最重要的砝码。对网络设计人员来说,网络组建的目的是为客户设计一个在性能和扩展性等方面都良好的网络。为了达到这个目的,需要进行深入的分析,与客户多进行沟通。如果网络工程应用需求分析做得透,网络工程方案的设计就会赢得用户方青睐;如果网络系统体系结构架构得好,网络工程实施及网络应用实施就相对容易得多。反之,如果网络工程设计方没有对用户方的需求进行充分的调研,不能与用户方达成共识,那么随意需求就会贯穿整个工程项目的始终,并破坏工程项目的计划和预算。由此可见,需求分析奠定了项目管理的基础。需求分析的目的在于明确所组建网络的目标。

2.1.1 网络需求分析概述

设计一个网络,首先要为用户分析目前面临的主要问题,确定用户对网络的真正需求,

并在结合未来可能的发展要求的基础上选择、设计合适的网络结构和网络技术,提供用户满意的高质服务。也就是说,首先必须做好需求分析。需求分析阶段主要完成用户方网络系统调查,了解用户方建设网络的需求,或用户方对原有网络升级改造的要求。需求分析是整个网络设计过程中的难点。要做好网络需求分析,必须按照如下步骤进行分析:

(1)明确用户目标。在需求分析中,首先就是要明确用户设计网络的目标,即用户设计网络是用来干什么的,主要有哪些功能,是升级旧网络还是新建网络等。

(2)需求调研。在需求调研中通过与用户交谈和实地考察,确定用户需求中的功能,通过成本估算来明确用户投资的额度范围。需求调研应考虑网络的物理布局、网络性能需求、设备配置及网络服务功能、网络安全级别选择、延时性要求等。通过对这些方面问题的调查和分析,初步形成网络设计方案,然后再和用户进行沟通,论证方案的可行性。

(3)需求分析报告。在需求分析及需求调研后,需要形成一份完整的报告文档。该文档将详细地说明系统必须完成的功能要求和必须达到的性能要求,文档的大小以网络系统的规模来确定。

2.1.2 网络需求分析的具体内容

网络需求分析是网络开发过程的起始部分,这一阶段应明确客户所需的网络服务和网络性能需求。在了解了需求分析的基本情况之后,就开始介绍需求分析所涉及的具体内容。

1. 网络建设目标

在用户需求分析中,首先要确定网络建设的目标。目标通常可以按照工期角度来分,主要分为近期目标和远期目标。无论是近期目标还是远期目标,都应该由专业人士和用户共同讨论研究。

2. 网络应用和网络服务

需求分析中需要明确用户网络系统应用范围和网络提供的服务。网络工程设计人员需要在用户的帮助下,通过对网络应用调查表进行分类汇总后,确定网络应用和网络服务。用户网络应用调查表可采用如表 2-1 所示的样式,其内容填写可由网络工程设计人员、用户和相关人员共同讨论完成。

表 2-1 网络应用和网络服务调查表

应用名称	应用类型	是否为新增	重 要 性	备 注

在调查表中,“应用名称”可以填入用户提供的应用名(如在线电视、网上购物、电子报刊),也可以是一种比较规范的名称,如 E-mail;“应用类型”可以是相似名称或标准化的名称,可以将其简单地分成下面两类:

- (1) Internet/intranet 网络公共服务。
- WWW 服务。
 - 电子邮件系统。
 - FTP 文件服务。
 - 电子商务系统。

- 政府、金融、电信等公共在线查询系统。

(2) 后台数据库系统。

- 关系数据库系统:这种数据库以 Oracle、SQL Server 等为主,提供后台数据库支持,支持 OA 系统、MIS 系统等。
- 非结构化数据库系统:该系统是以 Lotus Domino、MS Exchange Server 为主的平台,支持政府、金融等部门的公文流传输系统、档案系统。
- 网络专用应用系统:该系统包括金融、电信、交通、学校等部门的项目管理系统、人力资源管理系统、财务管理系统、教务管理系统等。
- 多媒体应用系统:该系统包括目前流行的在线视频点播系统、视频会议、远程视频教学及监控系统等。
- 网络基础服务:常见的网络基础服务就是 DNS、SNMP 等。
- 信息安全平台:信息安全平台指网络安全和系统信息安全方面,包括 CA 证书认证系统、防火墙、加密系统等。

3. 计算机平台需求

收集计算机平台需求是网络需求分析过程中一个不可缺少的步骤,需要调查的计算机平台主要分为个人计算机、服务器、小型机、中型机和大型机等,设计人员可根据用户对业务的需求来决定计算机平台的数量和类型。

4. 网络需求

需求分析的最后工作是考虑网络需求,这些需求包括以下内容。

1) 局域网功能

传统局域网网络由二层交换机构成局域网骨干,整个网络是一个广播域。在这样的网络中,网段由交换机的一个端口与下连的共享设备组成,网段内部用户之间的通信不需要通过交换设备,而段间通信需要通过交换设备进行存储转发。现代局域网网络由三层交换设备构成局域网骨干,这种网络中存在多个广播域,其实就是多个小型局域网,这些小型局域网通过三层设备的路由交换功能互连。在这种局域网络中,网段其实就是一个独立的广播域,一个典型的 VLAN。无论是哪种网段,都是计算机结点的一种划分方式,但是基于三层交换技术的网段划分方式逐渐成为主流。一般情况下,局域网网段和用户群的分布是一致的,但是也存在一定的差异,允许一个网段内部存在多个用户群,也允许一个用户群占据多个网段。对于升级的网络,可以对现有网段划分方式进行改进,形成新的划分方案。对于新建的网络,要和网络管理员一起商量网段划分的方式,最终所形成的网段分布需求就是用户群和网段的关系需求。

局域网网段的分布主要是依据业务上的特殊要求,这会导致不同的网段存在不同的功能要求。在进行网络需求收集时,应该找到各网段所需要的功能清单,并明确各个网段中功能的重要性。

局域网的负载是和应用有关联的。根据局域网络的功能需求,可以分析出局域网络的负载。在进行网络负载分析时,要针对各种应用和功能服务,评估服务的平均业务量和文件传输的大小,同时估算用户的访问频率,经过简单计算就可以估算网络的负载。

2) 网络性能

针对网络的性能需求,主要考虑的是吞吐量、网络时延、网络路由和网络带宽等。

(1)吞吐量。吞吐量是指在单位时间内传输无差错数据的能力。吞吐量采用每秒包数(packets per second,PPS)、每秒字节数(characters per second,CPS)或每秒事务数(transactions per second,TPS)来度量网络的总体性能。吞吐量也是网络互连设备中的指标之一,常用PPS(ATM设备采用CPS)度量,这种指标是指在不丢失任何分组数据的情况下,该设备所能转发的最大分组数量。如Cisco WS-C2950-24的包转发率为3.6 MPPS。

(2)网络时延。网络时延是指网络一端发送一个比特到网络另外一端所花费的时间。影响网络时延的因素主要与网络设备、传输媒体有关。在网络系统工程中使用最为普遍的传输媒体就是双绞线和光缆。根据用户需求可以估算网络时延的大小,根据用户的地理环境来确定选择哪类双绞线和光缆。网络时延根据不同情况可以得到不同的种类,有传播时延、发送时延、重传时延、分组交换时延和排队时延。其中的分组交换时延和排队时延主要指网络设备的响应和处理时间。

(3)网络路由。Internet和企业内部网络、局域网之间互连主要都是通过IP路由器实现的。路由器的主要功能是负责接收各个网络入口的分组,并把分组从其相应的出口转发出去。路由器使用各种路由协议,提供网络路径选择,并对流量、访问进行控制。

在网络需求分析时,依据用户需求和网络服务形式等确定网络间路由的选择,以及这种路由算法应采用哪种路由协议。

(4)网络带宽。网络带宽与网络的传输容量和传输能力息息相关,主要用频率来表示。而通常网络系统中带宽用兆比特每秒来描述。建立网络系统,就应该对各种网络产品和传输媒体以及网络服务提供商的接入带宽标准有一定的了解,否则网络工程的规划设计可能会因为接入不匹配而导致错误。关于目前的一些线路对应的服务商提供的传输媒体、传输率如表2-2所示。

表 2-2 常见网络传输率参数表

技术类型	数据传输率	传输媒体
拨号线路	14.4~56 Kb/s	电话线
ISDN	128 Kb/s	电话线
ADSL	1.544~8 Mb/s	双绞线
帧中继	56 Kb/s~1.544 Mb/s	双绞线
电缆调制解调器	512 Kb/s~52 Mb/s	同轴电缆
以太网	10 Mb/s	同轴电缆或双绞线
快速以太网	100 Mb/s	同轴电缆或双绞线、光纤
千兆以太网	1 000 Mb/s	光纤、双绞线
FDDI	100 Mb/s	光纤
CDDI	100 Mb/s	双绞线
令牌环网	4 Mb/s 或 16 Mb/s	同轴电缆或双绞线
T1、T3	1.544 Mb/s、45 Mb/s	双绞线和光纤、同轴电缆
E1、E3	2.048 Mb/s、34.368 Mb/s	双绞线和光纤
OC-1、OC-3、OC-24、 OC-48、OC-192	51.84 Mb/s、155.52 Mb/s、1.244 Gb/s、 2.488 Gb/s、约 10 Gb/s	OC-1 为同轴电缆 OC-3、OC-24、OC-48、OC-192 为光纤

3)数据备份和容灾需求

数据备份和容灾需求是网络工程中的重点内容。对于一些特定行业来说,数据是至关重要的,数据一旦丢失,将会造成不可挽回的损失。根据不同的网络工程规模,存在两种建设情况,一种是建设复杂的数据备份中心和容灾备份中心,另一种是仅建立数据备份和容灾机制。设计人员可根据用户需求选择。

4)网络管理需求

网络管理人员的管理思路、产品喜好、管理要求是决定网络管理平台的关键。由于网络管理是网络工程中较为复杂、牵涉面较广的建设内容,需要与网络管理人员重点进行交流,获取明确的管理需求。网络管理建设要从以下方面进行调查:

(1)明确网络管理的目的。企业网络管理的主要目的是提高网络可用性、改进网络性能、减少和控制网络费用以及增强网络安全性等,网管员可以根据自身需要进行补充与调整。

(2)掌握网络管理的要素。网络管理平台的建设要注意与业务需求结合,建立完整而理想的网络管理解决方案应该根据应用环境和业务流程,以及用户需求的端到端关联来管理网络及其所有设备。

(3)明确管理的网络资源。网络资源就是指网络中的硬件设备、网络环境中运行的软件以及所提供的服务等。网络管理员必须明确需要管理的网络资源。

(4)注重软件资源管理和软件分发。网络管理系统的软件资源管理和软件分发功能是指优化管理信息的收集。软件资源管理是对企业所拥有的软件授权数量和安装地点进行管理;软件分发则是通过网络把新软件分发到各个站点,并完成安装和配置工作。这些特定的需求必须让管理员进行明确。

5)网络安全需求

网络安全体系是建设网络工程的重要内容之一,不管网络工程规模如何,都应该满足一定的安全级别,这样才能保证网络的平稳运行和数据安全。网络安全需求主要应考虑以下几点:

(1)网络的基本安全需求。满足基本的安全要求,是该网络成功运行的必要条件,在此基础上提供强有力的安全保障,是网络系统安全的重要原则。网络内部部署了众多的网络设备、服务器,保护这些设备的正常运行,维护主要业务系统的安全,是网络的基本安全需求。对于各种各样的网络攻击,如何在提供灵活且高效的网络通信及信息服务的同时,抵御和发现网络攻击,并且提供跟踪攻击的手段,是网络安全需求的基本目标。网络基本安全需求主要表现为:

- 网络正常运行。在受到攻击的情况下,能够保证网络系统继续运行。
- 网络管理/网络部署的资料不被窃取。
- 具备先进的入侵检测及跟踪体系。
- 提供灵活而高效的内外通信服务。

(2)应用系统的安全需求。与普通网络应用不同的是,应用系统是网络功能的核心。对于应用系统应该具有最高的网络安全措施。应用系统的安全体系应包含:

- 访问控制。通过对特定网段、服务建立的访问控制体系,将绝大多数攻击阻止在到达攻击目标之前。
- 检查安全漏洞。通过对安全漏洞的周期检查,保证即使攻击可到达攻击目标,也可使

绝大多数攻击无效。

- 攻击监控。通过对特定网段、服务建立的攻击监控体系,可实时检测出绝大多数攻击,并采取相应的行动(如断开网络连接、记录攻击过程、跟踪攻击源等)。
- 加密通信。主动的加密通信,可使攻击者无法了解、修改敏感信息。
- 认证。良好的认证体系可防止攻击者假冒合法用户。
- 多层防御。攻击者在突破第一道防线后,延缓或阻断其到达攻击目标。
- 隐藏内部信息。隐藏内部信息使攻击者不能了解系统内的基本情况。
- 设立安全监控中心。设立安全监控中心为信息系统提供安全体系管理、监控、维护及紧急情况服务。

5. 编写需求说明书

通过需求收集工作,网络设计人员获取了大量的需求信息,这些信息由各种独立的表格、散乱的文字以及部分统计数据构成,这些需求信息应整合成正式的需求说明书,以便于后期设计、实施、维护工作的开展。需求说明书是网络设计过程中第一个正式的可以传阅的重要文件,其目的在于对收集到的需求信息进行清晰的概括整理。

1) 数据准备

数据准备工作是开始需求说明书编制的前期工作,主要由两个步骤构成:第一步是要将原始数据制成表,从各个表看其内在的联系及模式;第二步是要把大量的手写调查问卷或表格信息转换成电子表格或数据库,由于录入工作量较大,可以求助于用户单位或雇用临时工。另外,对于需求收集阶段产生的各种资料,包括手册、报表和原始单据等,无论其介质是纸质还是电子的,都应该编辑目录并归档,便于后期查阅。

2) 需求说明书的组成

编写需求说明书的目的是向管理人员提供决策用的信息,因此说明书应该做到尽量简明且信息充分,以节省管理人员的时间。网络需求说明书不存在国际或国家标准,即使存在一些行业标准,也只是规定了需求说明的大致内容要求。这主要是由于网络工程需求涉及内容较广,个性化较强,而且不同的设计队伍对需求的组织形式也不一样。一般情况下,需求说明书应该包括以下内容:

(1) 综述。需求说明文档书的第一部分内容是综述,对网络工程项目的主要内容、重要性等进行简单的描述。综述应包括的内容如下:

- 对项目的简单概述。
- 设计过程中各个阶段的清单。
- 项目各个阶段的状态,包括已完成的阶段和现在正进行的阶段。

(2) 需求分析阶段总结。需求分析阶段总结主要是总结需求分析阶段的工作,总结内容如下:

- 接触过的群体和代表人名单。
- 标明收集信息的方法(访谈、集中访谈和调查等)。
- 访谈、调查总次数。
- 取得的原始资料数量(调查问卷、报表等)。
- 在调查工作中遇到的各种困难等。

(3) 需求数据总结。对需求调查中获取的数据需要认真总结并归纳出信息,并通过多种形式进行展现。

2.2 逻辑网络设计

网络的逻辑结构设计来自于用户需求中描述的网络行为和性能等要求。逻辑设计要根据网络用户的分类和分布,选择特定的技术,形成特定的网络结构。网络结构大致描述了设备的互连及分布,但是不对具体的物理位置和运行环境进行描述。

2.2.1 逻辑网络设计概述

网络工程设计中的逻辑网络设计是建设网络过程中的重要工作,从整体上影响或决定了网络的建设规模、基本结构、主要应用内容与模式、资金投入和建设周期等重大问题,是网络工程技术人员不可或缺的必备专业技术。逻辑网络设计是在掌握网络建设的任务与工作程序,理解网络工程建设的技术指标等基本概念的基础之上,根据用户需要确定的网络建设方案,包括网络结构规划、地址分配等。

1. 逻辑网络设计目标

逻辑网络的设计目标主要来自分析说明书中的内容,尤其是网络需求部分,由于这部分内容直接体现了网络管理部门和人员对网络设计的要求,因此需要重点考虑。一般情况下,逻辑网络设计的目标如下:

(1)合适的应用运行环境。逻辑网络设计必须为应用系统提供环境,并可以保障用户能够顺利访问应用系统。

(2)成熟而稳定的技术选型。在逻辑网络设计阶段,应该选择较为成熟稳定的技术,越是大型的项目,越要考虑技术的成熟度,以避免错误投入。

(3)合理的网络结构。合理的网络结构不仅可以减少一次性投资,而且可以避免网络建设中出现各种复杂问题。

(4)合适的运营成本。逻辑网络设计不仅决定了一次性投资,技术选型、网络结构也直接决定了运营维护等周期性投资。

(5)逻辑网络的可扩充性。网络设计必须具有较好的可扩充性,以便于满足用户增长、应用增长的需要,保证不会因为这些增长而导致网络重构。

(6)逻辑网络的易用性。网络对于用户是透明的,网络设计必须保证用户操作的单纯性,过多的技术性限制会导致用户对网络的满意度降低。

(7)逻辑网络的可管理性。对于网络管理员来说,网络必须提供高效的管理手段和途径,否则不仅会影响管理工作本身,也会直接影响用户的使用。

(8)逻辑网络的安全性。网络安全应提倡适度安全,对于大多数网络来说,既要保证用户的各种安全需求,又不能给用户带来太多限制。但是对于特殊的网络,也必须采用较为严格的网络安全措施。

2. 逻辑网络设计需要关注的问题

逻辑设计过程,就是根据用户的需求,不违背设计限制,对现有网络进行改造或新建网络,最终达到设计目标的工作。逻辑网络设计工作中,设计目标是一个复杂的整体,由不同难度的子目标构成。这些子目标独立考虑时,存在较为明显的优劣关系。例如,最低的安装

成本、最低的运行成本、最高的运行性能、最大的适应性、最短的故障时间、最大的可靠性、最大的安全性等。这些子目标相互之间可能存在冲突,不存在一个网络设计方案,能够使得所有的子目标都达到最优。为了解决这些子目标的冲突,找到较为优秀的方案,可以采用两种方法:第一种方法较为传统,由网络管理人员和设计人员一起建立这些子网之间的优先级,尽量让优先级比较高的子目标达到较优;第二种方法是对每种子目标建立权重,对子目标的取值范围进行量化,通过评判函数决定哪种方案最优,而子目标的权重关系直接体现了用户对不同目标的关心度。

成本与性能是最为常见的冲突目标,一般来说,网络设计方案的性能越高,也就意味着成本(包括建设成本和运行成本)越高。设计方案时,所有不超过成本限制、满足用户要求的方案,都称为可行方案。设计人员只能从可行方案中依据用户对性能和成本的喜好进行选择。

网络建设的成本分为一次性投资和周期性投资。在初期建设过程中,如何合理规划一次性投资的支付是比较关键的。过早支付费用,容易造成建设单位的风险,对于未按设计方案实施的情况,无法形成制约机制;过晚支付费用,容易造成承建单位的资金压力,导致项目实施质量等多方面的问题。较为合理的支付方式,必须是依据逻辑网络设计的特点,将网络工程划分为各个阶段,在每个阶段后实施验收,并支付相应的阶段费用,在工程建设完毕并试运行一段时间后,才能支付最后的质量保证费用。运营维护等周期性费用的支付,也应考虑合理性,这主要体现在周期划分方式、支付方式等方面。

3. 主要的网络服务

网络设计人员应该依据网络提供的服务要求来选择特定的网络技术,不同的网络,其服务的要求不同,但是对于大多数网络来说,都存在着两种主要的网络服务——网络管理和网络安全,这两种服务在设计阶段是必须考虑的。

1) 网络管理

网络管理可以根据网络的特殊需要,将其划分为几个不同的大类,其中的重点内容是网络故障诊断、网络配置及重配置和网络监视。

(1)网络故障诊断。网络故障诊断主要借助于网管软件、诊断软件和各种诊断工具。对于不同类型的网络和技术,需要的软件和工具是不同的,应在设计阶段就考虑到网络工程中所需的各种诊断软件和工具。

(2)网络配置及重配置。网络配置及重配置是网络管理的另一个问题,各种网络设备都提供了多种配置方法,同时也提供了配置重新装载的功能。在设计阶段,充分考虑网络设备的配置保存和更新需要,提供特定的配置工具以及配置管理工具,这可以使管理人员的工作更加便利。

(3)网络监视。网络监视的需求随着网络规模和复杂性的不同而不同,网络监视是为了预防灾难,使用监视服务来防止和监测网络的运行情况。

2) 网络安全

网络安全是网络逻辑设计的固有部分,网络设计者进行安全设计时应遵循以下原则:

(1)明确需要安全保护的系统。首先要明确网络中需要重点保护的关键系统,通过该项工作,可以找出安全工作的重点,避免全面铺开而又无法面面俱到的局面。

(2)确定潜在的网络弱点和漏洞。对于这些重点防护的系统,必须通过对这些系统的数据存储、协议传递和服务方式等的分析,找出可能存在的网络弱点和漏洞。在设计阶段,应

依据工程经验对这些网络弱点和漏洞设计特定的防护措施;在实施阶段,再根据实施效果进行调整。

(3)尽量简化安全。安全设计要注意简化问题,不要盲目扩大安全技术和措施的重要性,采用一些传统而有效、成本低廉的安全技术来提高安全性是非常有必要的。

(4)安全制度。单纯的技术措施是无法保证网络的整体安全的,必须匹配相应的安全制度。逻辑设计阶段,尚不能制定完备的安全制度,但是对安全制度的大致性要求,包括培训、操作规范和保密制度等框架性要求是必须明确的。

4. 技术评价

根据用户的需求设计逻辑网络,选择正确的网络技术是比较关键的,在进行选择时应考虑如下因素。

1)通信带宽

所选择的网络技术必须保证足够的带宽,能够为用户访问应用系统提供保障。在进行选择时,不能仅局限于现有的应用要求,还要考虑适当的带宽增长需求。

2)技术成熟性

所选择的网络技术必须是成熟稳定的技术,有些新的应用技术在尚没有大规模投入应用时,还存在着较多不确定因素,而这些不确定因素将会为网络建设带来很多不可估量的损失。虽然新技术的自身发展离不开工程应用,但是对于大型网络工程来说,项目本身不能成为新技术的试验田。因此,尽量使用较为成熟、拥有较多案例的技术是明智的选择。同时,在面对技术变革的特殊时期,可以通过采用试点的方式,缩小新技术的应用范围,规避技术风险,待技术成熟后再进行大规模应用。

3)连接服务类型

连接服务类型是逻辑设计时必须考虑的问题,传统的连接服务分为面向连接服务与非连接服务,逻辑设计需要在无连接和面向连接服务的协议之间进行权衡。由于当前广泛应用的网络协议主要是 TCP/IP 协议簇,其网络层协议是提供非连接服务的 IP 协议,因此选择连接服务类型,主要是对 IP 协议底层的承载协议进行选择。

4)可扩充性

网络设计者的设计依据是较为详细的需求分析,但是在选择网络技术时,不能仅考虑当前的需求,而忽视未来的发展。在大多数情况下,设计人员都会在设计中预留一定的冗余,在带宽、通信容量、数据吞吐量和用户并发数等方面,网络实际需要和设计结果之间的比例应小于一个特定值以便于未来的发展。一般来说,这个值为 70%~80%,在不同的工程中,可根据需要进行调整。

5)高投资产出比

选择网络技术最关键的一条,不是技术的扩展性、高性能,也不是成本最低等,而是技术的投入产出比,尤其是一些借助于网络来实现营运的工程,只有通过投入产出比分析,才能最后决定技术的使用。

2.2.2 逻辑网络设计内容

1. 网络结构设计

传统意义上的网络拓扑是将网络中的设备和结点描述成点,将网络线路和链路描述成

线。随着网络的不断发展,单纯的网络拓扑结构已经无法全面描述网络。因此,在逻辑网络设计中,网络结构的概念正在取代网络拓扑结构的概念成为网络设计的框架。网络结构是对网络进行逻辑抽象,描述网络中主要连接设备和网络计算机结点分布而形成的网络主体框架。网络结构与网络拓扑结构的最大区别在于:网络拓扑结构中,只有点和线,不会出现任何的设备和计算机结点;网络结构主要是描述连接设备和计算机结点的连接关系。局域网结构主要讨论数据链路层的设备互连方式,以下是在进行局域网设计时常见的局域网结构。

1) 单核心局域网结构

单核心局域网结构主要由一台二层或三层交换设备构建局域网的核心,通过多台交换机接入计算机结点,该网络一般通过与核心交换机互连的路由设备(路由器或防火墙)接入广域网中。

典型的单核心局域网结构如图 2-1 所示。

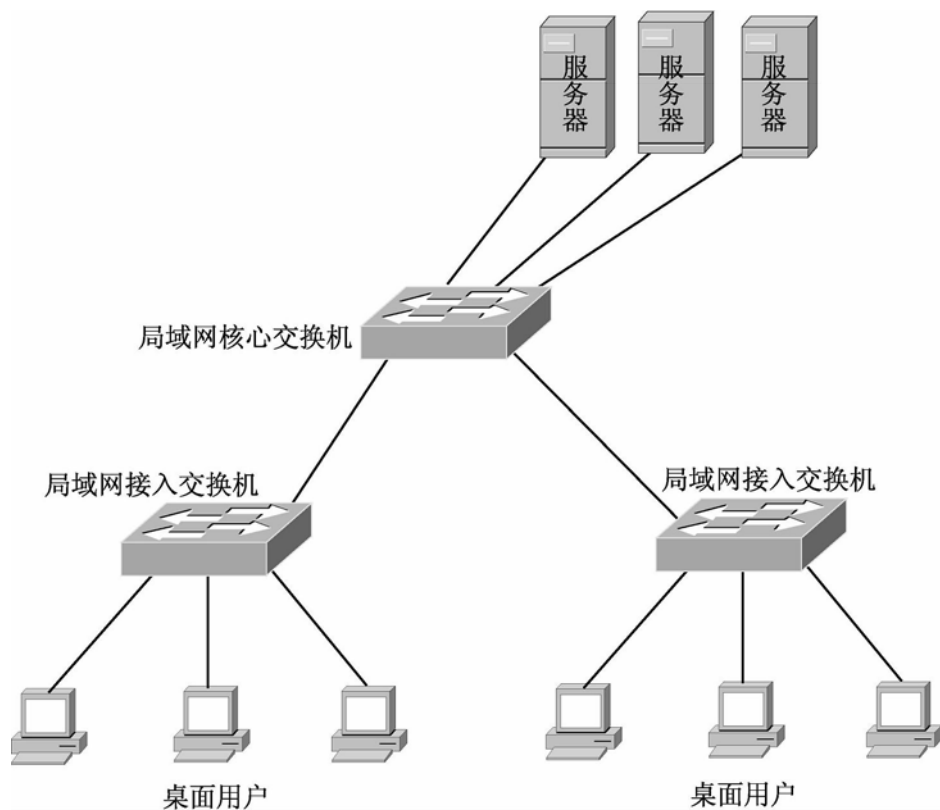


图 2-1 单核心局域网结构

单核心局域网结构分析如下:

- (1) 核心交换设备在实现上多采用二层、三层交换机或多层交换机。
- (2) 如采用三层或多层设备,可以划分成多个 VLAN(虚拟局域网),VLAN 内只进行数据链路层帧转发。
- (3) 网络内各 VLAN 之间访问需要经过核心交换设备,并且只能通过网络层数据包转发方式实现。
- (4) 网络中除核心交换设备之外,不存在其他的带三层路由功能的设备。
- (5) 核心交换设备与各 VLAN 设备可以采用 10/100/1 000 Mb/s 以太网连接。
- (6) 节省设备投资。
- (7) 网络结构简单。

(8)部门局域网访问核心局域网以及相互之间访问效率高。

(9)在核心交换设备端口富余的前提下,部门网络接入较为方便。

(10)网络地理范围小,要求部门网络分布比较紧凑。

(11)核心交换机是网络的故障单点,容易导致整网失效。

(12)网络扩展能力有限。

(13)对核心交换设备的端口密度要求较高。

(14)除非规模较小的网络,否则推荐桌面用户不直接与核心交换设备相连,也就是核心交换机与用户计算机之间应存在接入交换机。

2)双核心局域网结构

双核心局域网结构主要由两台核心交换设备构建局域网核心,该网络一般也是通过与核心交换机互连的路由设备接入广域网,并且路由器与两台核心交换设备之间都存在物理链路。

典型的双核心局域网结构如图 2-2 所示。

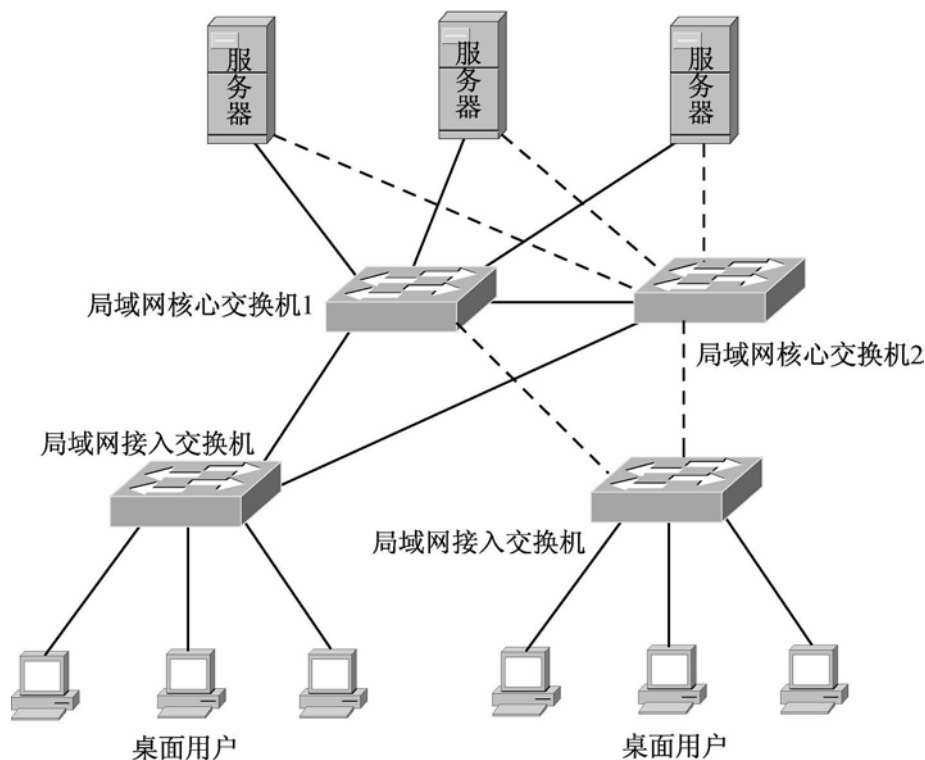


图 2-2 双核心局域网结构

双核心局域网结构分析如下：

(1)核心交换设备在实现上多采用三层交换机或多层交换机。

(2)网络内各 VLAN 之间访问需要经过两台核心交换设备中的一台。

(3)网络中除核心交换设备之外,不存在其他具备路由功能的设备。

(4)核心交换设备之间运行特定的网关保护或负载均衡协议,如 HSRP(热备份路由器协议)、VRRP(虚拟路由器冗余协议)、GLBP(网关负载均衡协议)等。

(5)核心交换设备与各 VLAN 设备间可以采用 10/100/1 000 Mb/s 以太网连接。

(6)网络拓扑结构可靠。

(7)路由层面可以实现无缝热切换。

(8)部门局域网络访问核心局域网以及相互之间访问,有多条路径选择,可靠性更高。

(9)在核心交换设备端口富余的前提下,部门网络接入较为方便。

(10)设备投资比单核心局域网高。

(11)对核心路由设备的端口密度要求较高。

(12)核心交换设备和桌面计算机之间,存在接入交换设备,接入交换设备同时和双核心存在物理连接。

(13)所有的服务器都直接同时连接至两台核心交换机,借助于网关保护协议,实现桌面用户对服务器的高速访问。

3)环型局域网结构

环型局域网结构由多台核心三层设备连接而成,构建整个局域网络的核心。该网络通过与环上交换设备互连的路由设备接入广域网网络。典型的环型局域网结构如图 2-3 所示。

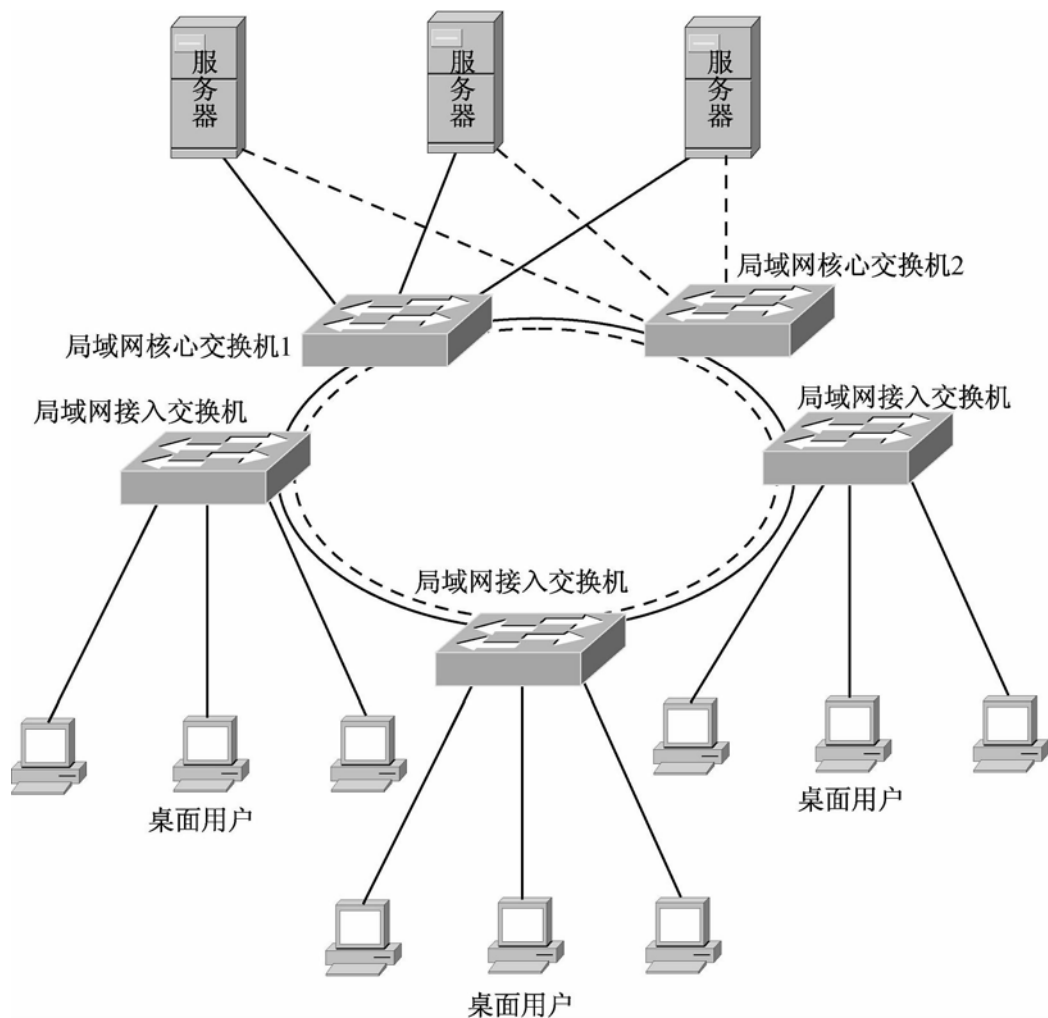


图 2-3 环型局域网结构

环型局域网结构分析如下：

(1)核心交换设备在实现上多采用三层交换机或多层交换机。

(2)网络内各 VLAN 之间访问需要经过 RPR(弹性分组环)。

(3)RPR 技术能提供 MAC 层的 50 ms 自愈时间,能提供多等级、可靠的 QoS(服务质量)。

(4)RPR 有自愈保护功能,节省光纤资源。

(5)RPR 协议中没有提及相交环、相切环等组网结构,当利用 RPR 组建大型城域网时,多环之间只能利用业务接口进行互通,不能实现网络的直接互通,因此它的组网能力相对同步数字体系较弱。

(6)由两根反向光纤组成环型拓扑结构。其中,一根顺时针,另一根逆时针,结点在环上可从两个方向到达另一结点。每根光纤可以同时用来传输数据和同向控制信号,RPR 双向可用。

(7)利用空间重用技术实现的空间重用,使环上的带宽得到更为有效的利用。RPR 技术具有空间复用、环自愈保护、自动拓扑识别、多等级 QoS、带宽公平机制和拥塞控制机制、物理层介质独立等技术特点。

(8)设备投资比单核心局域网高。

(9)核心路由冗余设计实施难度较高,容易形成路由环路。



请注意

弹性分组环(resilient packet ring,RPR)是一种新型的媒体访问控制(media access control,MAC)协议,可运行于光同步网络或同步数字体系、密级波分复用技术和以太网之上,为宽带 IP 城域网运营商提供灵活高效的组网方案。

4)层次局域网结构

层次局域网结构主要定义了根据功能要求不同将局域网划分层次构建的方式,从功能上定义为核心层、会聚层、接入层。层次局域网一般通过与核心层设备互连的路由设备接入广域网络。典型的层次局域网结构如图 2-4 所示。

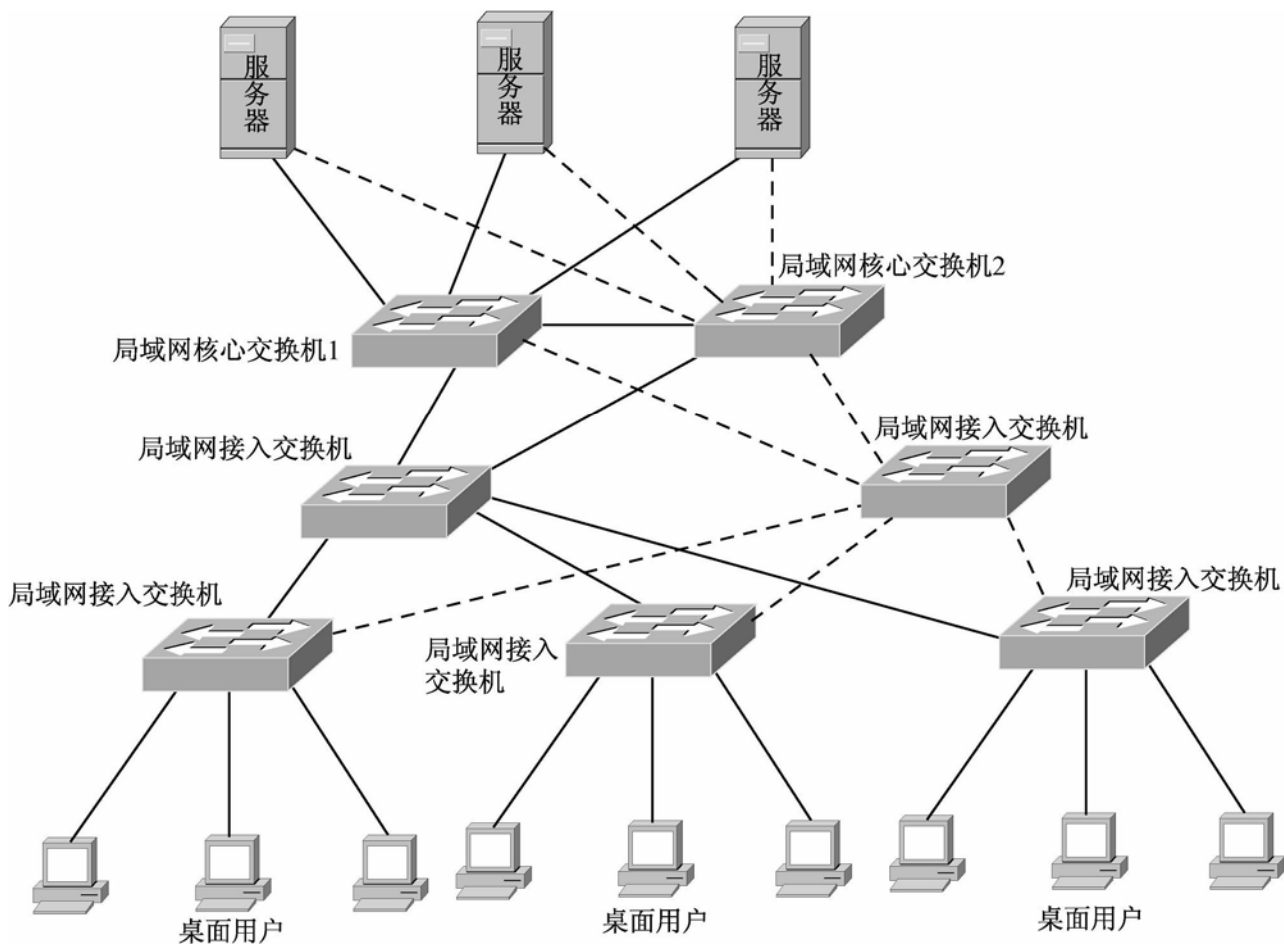


图 2-4 层次局域网结构

层次局域网结构分析如下:

(1)核心层实现高速数据转发。

- (2) 会聚层实现丰富的接口和接入层之间的互访控制。
- (3) 接入层实现用户接入。
- (4) 网络拓扑结构故障定位可分级,便于维护。
- (5) 网络功能清晰,有利于发挥设备最大效率。
- (6) 网络拓扑利于扩展。

在进行网络结构设计过程中,设计人员可以根据用户的需求和网络规模考虑网络结构的设计,也可以综合使用这几种网络结构。

2. 物理层技术及网络设备选择

1) 物理层技术选择

在确定了大致的网络结构之后,需要对网络中物理层技术进行选择,这些技术选择内容包括缆线类型、选用网卡等。选择物理层技术时,不能仅局限于当前的需要,还要考虑到网络升级所带来的需求。

以下是对满足需求说明书要求的技术进行选择时的一些通用原则:

(1) 可扩展性与可伸缩性。选择底层技术时,一定要考虑扩展性,否则将导致大量物理层设备的替换。例如,尽管需求说明书中提出了带宽的要求小于 10 Mb/s,但是在设计时,仍可以采用第五类非屏蔽线和百兆网卡,以避免当应用升级后导致的网络重新布线以及网卡淘汰,这样当整个网络升级至快速以太网时,仅需要更换交换设备。

(2) 可靠性、可用性和可恢复性。物理层的可靠性、可用性和可恢复性主要来自于应用的需求,如果物理层不稳定,必然导致承载的应用出现故障,应尽量选择较为稳定、可靠的物理层技术。例如,在实现远程用户的接入时,不选择基于模拟信号调制的语音拨号接入方式,而选择基于数字信号编码的 ISDN 或者 ADSL 方式。再如,在专网建设中,如果用户存在变动或升级带宽的需求,则不能采用带宽固定的 SDH 信道,而是采用可以动态变化带宽的 ATM PVC 方式。

(3) 安全性。物理层的不安全因素是指未经授权而非法访问网络介质,通常的做法是利用监听线缆来监视传输。不同的物理介质有不同的内在安全特征,所以客户的安全需求决定了对物理层设备的选择。例如,针对一些特殊部门的接入,采用光缆以避免信号窃听;或者是采用屏蔽线缆替代非屏蔽线缆。

(4) 节约成本。节约成本也是需要着重考虑的一个问题。例如,在经济上考虑是否使用现存的线缆或网卡,从成本上考虑是需要内部安装人员还是专业的承包人。

2) 物理介质和网卡的选择

对有关物理层的需求了解清楚后,就可以选择物理介质和网卡了。

物理介质包括有线介质和无线介质,表 2-3 是对各种介质的比较,直接体现了其在设计中的应用范围,设计人员应根据需求和表 2-3 的介绍选择大致适合的物理介质类型。

表 2-3 物理介质对照表

要素	双绞线	光纤	细缆	粗缆	无线
距离	较短	较长	适中	适中	适中(视距传播)
抗干扰性	低(UTP)	适中(STP)	非常高	适中	低
安装难易	简单	专业人员	简单	专业人员	微波专业安装人员

续表

要素	双绞线	光纤	细 缆	粗 缆	无 线
费用	低	高	较低	较低	高
拓扑结构	总线、星型、环型	星型	总线	总线	—
MAC 协议	以太网、令牌环、CDDI	FDDI、ATM、SONET、以太网	以太网、令牌总线	以太网、令牌总线	以太网、令牌环网络、FDDI
数据速率	100 Mb/s	>100 Mb/s	100 Mb/s	10 Mb/s	微波:5.7 Mb/s 扩频:1~2 Mb/s

确定了表 2-3 中的物理介质类型之后,还需要根据实际需要确定具体的产品类型。例如,双绞线分为屏蔽线和非屏蔽线,其中非屏蔽线主要应用的有 3 类线、5 类线、6 类线;同轴电缆分为粗缆和细缆;光纤分为单模与多模,产品则以纤径、光缆内纤数、外壳材质不同而区分;卫星根据通信频段和天线口径,分为甚小口径卫星终端站(very small aperture terminal, VSAT)和宽带全球网络(broadband global area network,BGAN)。

网卡是在介质确定后的物理层元素之一,因为网卡必须与网络的物理介质、拓扑结构和 MAC 层协议相匹配。在选择网卡或者确定现存的网卡是否满足需要时,可以参考表 2-4 的物理层规范和表 2-5 的网卡特征。

表 2-4 物理层规范表

类 型	信令技术	物理介质	速率/(Mb/s)	最大分段距离/m	最大分段数	最大中继器数	最大中继器间距离/km
802.3 10Base-5 粗缆	基带	50 Ω 粗同轴电缆	10	500	100	4	2.4
802.3 10Basc-2 细缆	基带	50 Ω 细同轴电缆	10	200	30	4	0.9
802.3 10Base-T 双绞线	基带	非屏蔽双绞线	10	100	—	—	—
802.3 10Broad-36 CATV 缆	宽带	75 Ω CATV 同轴电缆	10	3 600	—	—	3.6
FDDI	调幅	光缆	100	—	—	1 000	2
802.5 屏蔽令牌环	曼码	光缆	16	300	—	12	0.2
802.5 非屏蔽令牌环	曼码	光缆	14	100	—	2	0.12

表 2-5 网卡特征表

指 标	特 征 值
所支持的 LAN	以太网、快速以太网、千兆以太网、FDDI、ISDN、Arcnet、令牌环
所支持的计算机总线	MCA、ISA、EISA、PCI、NuBus、VME、USB
RAM 缓冲	8 Kb/s、16 Kb/s、32 Kb/s
总线大小	8 b、16 b、32 b

续表

指 标	特 征 值
数据速率	4 Mb/s、10 Mb/s、16 Mb/s、100 Mb/s、1Gb/s
介质类型	10Base-2、10Base-T、UTP、STP、光缆
所支持的旧版本	Vines、NetWare、AppleTalk 等
价格/功能	参看供应商的说明书

3)网络设备选择

组建计算机网络,特别是 LAN 范畴的网络,正确选择网络设备是重要的任务之一。这里所说的网络设备的选择有两种含义:一种是从应用需要出发所进行的选择;另一种是从众多厂商的产品中选择性价比高的产品。在 LAN 环境下,通常涉及的网络设备有:用于连接到 LAN 的网卡;构成 LAN 的集线器;用于进行 LAN 互连的交换机和路由器等。

逻辑网络设计必须指定连接 LAN 各端或者跨区域的多个 LAN 连接的设备类型。交换机和路由器在网络设计中经常被组合使用,建立高性能、可升级性网络。所以这里只介绍交换机和路由器的选择。

(1)交换机选择。交换机是一个多端口的网桥,每个端口都有桥接功能,它能够在任意一对端口间转发帧。其内部是依靠专用集成电路(application specific IC,ASIC)连接起来的,ASIC 可以把任意端口的网段与别的端口的网段在数据链路层上相连。交换机允许多组端口同时交换帧,相当于多个网桥同时工作,可以实现帧转发的并行操作。要进行交换机选择,首先要了解交换机的主要性能指标:

- 转发技术。存储转发技术要求交换机在接收到全部数据包后再决定如何转发,采用该技术的交换机可以在转发之前检查数据包的完整性和正确性,减少了不必要的数据转发。直通转发则是在交换机收到整个帧之前就已经开始转发数据了,这样可以有效地降低交换延迟。但是,交换机在没有完全接收并检查数据包的正确性之前就已经开始了数据转发。在通信质量不高的环境下,交换机会转发所有的完整数据包和错误数据包,这实际上是给整个交换网络带来了许多垃圾通信包。因此,直通转发技术适用于网络链路质量较好、错误数据包较少的网络环境。
- 端口类型。交换机的端口类型有双绞线端口和光纤端口两种类型。对于局域网用户大多使用的都是双绞线类型端口的交换机。
- 管理功能。通常交换机厂商都提供管理软件或第三方管理软件远程管理交换机。有的交换机还允许外接设备监视可选端口的网络状况。
- 延时。采用直通转发技术的交换机有固定的延时,因为直通式交换机不管数据包的整体大小,而只根据目的地址来决定转发方向。所以,它的延时是固定的。采用存储转发技术的交换机必须要接收完完整的数据包才开始转发。因此,数据包大,则延时大;数据包小,则延时小。
- 全双工。全双工端口可以同时发送和接收数据,具有全双工功能的交换机可以获得两倍于单工模式通信的吞吐量,并且避免了数据发送与接收之间的碰撞。目前市场上的主流千兆交换机如 Cisco、3Com 的产品均支持全/半双工模式的自动转换。
- 单/多 MAC 地址类型。单 MAC 交换机主要设计用于连接最终用户、网络共享资源或非桥接路由器,它们不能用于连接集线器或含有多个网络设备的网段。多 MAC

交换机在每个端口有足够存储体,记忆多个硬件地址。多 MAC 交换机的每个端口可以看做是一个集线器,而整个交换机就可以看做是集线器的集线器。此时,关注的指标应该是交换机端口支持 MAC 地址的数目。

- 能否支持 VLAN。通过将局域网划分为虚拟网络 VLAN 网段,可以强化网络管理和网络安全,控制不必要的数据广播。在虚拟网络中,广播域可以是一组任意选定的 MAC 地址组成的虚拟网段。这样,网络中工作组可以突破共享网络中的地理位置限制,而根据管理功能来划分。
- 安全性。安全性越来越为人们所重视,交换机可以在底层把非法的客户隔离在网络之外。这些可以管理的网络交换机都支持 MAC 地址过滤的功能,还可以将 MAC 地址与固定的端口绑定在一起,或将 MAC 地址和它所在的 VLAN 绑定在一起。

在了解了交换机的主要性能指标后,再根据网络设计的具体情况选择交换机。在选择交换机的时候还要注意品牌和性价比等因素。

(2)路由器选择。路由器是整个网络与外界的通信出口,也是联系内部子网的桥梁。在网络组建的过程中,路由器的选择是极为重要的。在所有网络设备中,路由器的价格也是相当的昂贵,是网络设备的重头戏。不同的路由器的性能相差很多,价格也各不相同。所以用户在选择时一定要注意路由器的各种性能参数和功能的含义。

要选择路由器就必须了解路由器的结构,路由器的结构分为硬件部分和软件部分,硬件部分主要由 CPU(处理器)、RAM(存储正在运行的配置文件)、flash(负责保存 OS 的映像和路由器的微码)、NVRAM(保存配置件)、ROM(加载 OS)、输入/输出端口(完成路由器与其他设备的数据交换)等组成;软件部分主要由 boot ROM(主要功能是路由器加电后完成有关初始化工作,并向内存中加入操作系统代码)和 VRP(通用路由平台:路由器上运行的软件平台)组成。

路由器的主要参数:

- CPU。CPU 是路由器最核心的组成部分。不同系列、不同型号的路由器,其中的 CPU 也不尽相同。CPU 的好坏直接影响路由器的吞吐量(路由表查找时间)和计算能力(影响网络路由收敛时间)。一般来说,处理器主频在 100 MHz 及以下的属于较低主频,这样的低端路由器适合普通家庭和 SOHO 用户的使用;100~200 MHz 属于中等主频;200 MHz 以上则属于较高主频,适合网吧、中小企业用户以及大型企业的分支机构。
- 内存。路由器中可能有多种内存,如 flash、DRAM 等。内存用做存储配置、路由器操作系统、路由协议软件等内容。在中低端路由器中,路由表可能存储在内存中。通常来说路由器内存越大越好(不考虑价格)。但是与 CPU 能力类似,内存同样不直接反映路由器性能与能力。因为高效的算法与优秀的软件可以大大节约内存。
- 吞吐量。网络中的数据是由一个个数据包组成,对每个数据包的处理都要耗费资源。吞吐量是指在不丢失数据包的情况下单位时间内通过的数据包数量,也就是指设备整机数据包转发的能力,是设备性能的重要指标。路由器吞吐量表示的是路由器每秒能处理的数据量,是路由器性能的一个直观上的反映。
- 支持网络协议。在网络上的各台计算机之间也有一种语言,这就是网络协议,不同的计算机之间必须共同遵守一个相同的网络协议才能进行通信。常见的协议有 TCP/IP、IPX/SPX、NetBEUI 等。在局域网中用得比较多的是 IPX/SPX。用户如果访问

Internet,就必须在网络协议中添加 TCP/IP。

- VPN 支持能力。通常路由器都能支持 VPN。其性能差别一般体现在所支持 VPN 数量上。专用路由器一般支持的 VPN 数量较多。
- 无故障工作时间。该指标按照统计方式指出设备无故障工作的时间。一般无法测试,可以通过主要器件的无故障工作时间计算或者根据大量相同设备的工作情况计算。
- 带机数量。带机数量就是路由器能负载的计算机数量。在厂商介绍的性能参数表上经常可以看到标称自己的路由器能带 200 台 PC、300 台 PC 的。但是很多时候路由器的表现与标称的值都有很大的差别。这是因为路由器的带机数量直接受实际使用环境的网络繁忙程度影响,不同的网络环境带机数量相差很大。例如,在网吧里,几乎所有的人都同时在网上聊天、打游戏、看网络电影,这些数据都要通过 WAN 口,路由器的负载很重。而在企业网上经常同一时间只有小部分人在使用网络,路由器负载很轻。因此,把一个能带 200 台 PC 的企业网中的路由器放到网吧,可能连 50 台 PC 都带不动。
- 接口类型。路由器的接口类型有:通用串行接口,10 Mb/s 以太网接口、快速以太网接口、10/100 Mb/s 自适应以太网接口、千兆以太网接口、万兆以太网接口,ATM 接口(2、25、155、633 Mb/s 等),POS 接口(155、622 Mb/s 等),令牌环接口,FDDI 接口,E1/T1 接口、E3/T3 接口,ISDN 接口等。

路由器的选择比交换机的选择要复杂得多,设计人员在选择路由器时,除了考虑路由器的主要参数外,还需考虑路由器的外形结构尺寸、管理能力、网络安全控制能力等。

3. IP 地址和子网划分

在互联网中,A、B、C 三类标准 IP 地址是经常使用的网络地址,由于经过网络号和主机号的层次划分,它们能适应于不同的网络规模。但是,随着计算机技术的发展和网络技术的进步,个人计算机迅速普及,小型网络(特别是小型局域网)越来越多。这些网络多则拥有几十台主机,少则只有两三台主机。对于这样一些小规模网络即使使用 C 类 IP 地址仍然是一种浪费(一个 C 类网络最多可容纳 254 台主机)。在实际应用中,网络技术人员开始寻找新的解决方案以克服 IP 地址浪费的现象,子网划分及子网编址就是解决方案之一。下面用实例来讲解怎样进行子网划分。

【例 2-1】 假如给你一个 C 类的 IP 地址段:192.168.0.1~192.168.0.254,其中 192.168.0 属于网络号码,而 1~254 表示这个网段中最大能容纳 254 台计算机主机。现在要做的就是把这 254 台主机再次划分一下,将它们区分开来。

例题解析:192.168.0.1~192.168.0.254 默认使用的子网掩码为 255.255.255.0,其中的 0 在二进制中表示 8 个 0。因此有 8 个位置没有被网络号码占用, 2^8 就是表示有 256 个地址,去掉一个头(网络地址)和一个尾(主机地址),表示有 254 个计算机主机地址,因此,要对这 254 来划分,就是占用最后 8 个 0 中的某几位。

假如占用第一个 0,那么二进制表示的子网掩码为 11111111.11111111.11111111.10000000,转换为十进制为 255.255.255.128,这时计算机主机应该是 2^7 ,因此假如子网掩码为 255.255.255.128,这个 C 类地址可以被区分为两个网络,每个网络中最多有 128 台主机。192.168.0.1~192.168.0.127 为第一个网络,192.168.0.128~192.168.0.254 为第二个网络。

【例 2-2】 假如还是 C 类地址,其 IP 范围为 192.168.0.1~192.168.0.254,子网掩码为 255.255.255.192(也就是最后 8 位为主机位,被占用了 2 位,二进制表示为 11111111.11111111.11111111.11000000),那么这个网段的计算机主机数目就是 2^6 ,总共有 2^2 个网段。第一个网段为 192.168.0.1~192.168.0.63;第二个网段为 192.168.0.64~192.168.0.127;第三个网段为 192.168.0.128~192.168.0.191;第四个网段为 192.168.0.192~192.168.0.254。

通过**【例 2-1】**和**【例 2-2】**可以总结出一个规律,就是主机被占用了 n 位数,那么就有 2^N 个网络,也就有 2^{8-N} 个主机数目。

【例 2-3】 假如有一个 B 类地址网段,172.16.0.0~172.16.255.255,子网掩码为 255.255.0.0,现在需要将这个网段进行子网划分。不划分子网,那么就只有一个网络,这个网络里面包含 2^{16} ,也就有 6 万多台主机。因此,假如需要划分子网,网络地址就需要向主机地址借位。

例题解析:这种子网划分需分情况处理。

(1)先把 172.16.0.0 和 255.255.0.0 转换为二进制:

10101100 00010000 00000000 00000000 172.16.0.0

11111111 11111111 00000000 00000000 255.255.0.0

假如网络地址向主机地址借了 2 位,那么子网掩码就是:

11111111 11111111 11000000 00000000 255.255.192.0

因为借了 2 位,所以子网的个数为 $2^2 - 2$ 个,即 2 个子网。因为子网标识位不能为全“0”或全“1”,所以每个子网都有 $2^{14} - 2$ 台主机:172.16.64.1~172.16.127.254;172.16.128.1~172.16.191.254。

(2)划分更小的子网,网络地址向主机地址总共借用 10 位。

借用 10 位数后用二进制表示的子网掩码为 11111111.11111111.11111111.11000000,用十进制表示为 255.255.255.192,那么总共有 $2^{10} - 2$ 个子网数目,每个网络中有 $2^6 - 2$ 台主机,下面用十进制来表示。

前面 6 个:

172.16.0.65~172.16.0.126

172.16.0.127~172.16.0.190

172.16.0.193~172.16.0.254

172.16.1.1~172.16.1.62

172.16.1.65~172.16.1.126

172.16.1.127~172.16.1.190

最后 6 个:

172.16.254.65~172.16.254.126

172.16.254.127~172.16.254.190

172.16.254.193~172.16.254.254

172.16.255.1~172.16.255.62

172.16.255.65~172.16.255.126

172.16.255.127~172.16.255.190

从以上例子中可以看出,划分 B 类子网地址,其实和划分 C 类子网地址是一样的,只不过划分 C 类的时候是将第四段地址划分,而划分 B 类的时候可以划分第三段,也可以划分第四段而已。在网络设计过程中,设计人员可以根据网络信息点的数量决定是否划分子网以及采用什么方式来划分子网。

4. 路由选择协议

路由选择协议是使路由器能够自动连接到目的网络,并与其他路由器交换路由信息,以达到全网路由选择的目的。路由选择协议的选择是网络设计中的重要内容,直接决定了网络的连通性、稳定性。

路由协议选择遵循以下原则:

(1)路由协议类型选择。路由选择协议分为两大类:距离向量协议和链路状态协议。网络设计人员可以依据以下条件在两种类型中进行选择。

当满足下列条件时,可以选择使用距离向量路由选择协议:

- 网络使用一种简单的、扁平的结构,不需要层次化设计。
- 网络使用的是简单的中心辐射状结构。
- 管理人员缺乏对路由协议的了解,路由操作能力差。
- 收敛时间对网络的影响较小。

当满足下列条件时,可以选择使用链路状态路由选择协议:

- 网络采用层次化设计,尤其是大型网络。
- 管理员对链路状态路由协议理解较深。
- 快速收敛时对网络的影响较大。

(2)路由选择协议度量。当网络中存在多条路径时,路由协议使用度量值来决定用哪条路径。不同的路由选择协议的度量值是不同的,传统协议以路由器的跳数作为度量值。新一代的协议还将参考延迟、带宽、可靠性及其他因素。

(3)路由选择协议顺序。路由器上可能会存在多个不同的路由协议,针对一个目标网络,这些路由协议都会选举出具有最小度量值的路径,但是不同协议的度量值不同,可比较性不大。设计人员建立的协议度量值的转换关系只是用于不同路由协议之间的路由补充,不能用于具体路径的选择。因此,设计人员可以在网络中运行多个路由选择协议,并约定这些协议之间的顺序,这些顺序可以用路由协议权值来表示,权值越小的协议顺序越靠前。一旦多个路由协议都选举出了最优路径,则具有最小权值的路由协议的路径生效。

(4)层次化与非层次化路由选择协议。路由协议从层次化角度可以分为支持和不支持两种;在非层次化协议中,所有路由器的角色都是一样的。层次化协议中,不同路由器的角色不同,需要处理的路由信息量也不同。对于采用层次化设计的网络来说,最好采用层次化路由选择协议。

(5)内部与外部路由选择协议。路由协议根据自治区域的划分以及作用,可以分为内部网关协议和外部网关协议,设计人员需要选择正确的、合适的协议类型。例如,对于内部网关协议,较为常见的是 RIP、OSPF、IGRP;对于外部网关协议,多选择 BGP。

(6)分类与无分类路由选择协议。分类与无分类路由协议的选择是进行网络路由设计时必须考虑的内容。

(7)静态路由选择协议。静态路由是指手工配置并且不依赖于路由选择协议进行更新

的路由,它经常用于连接一个末梢网络(只能通过一条路径到达的网络部分),其最常见的使用方法就是默认路由。网络设计人员应该对设计网络中的末梢网络进行区分,并设定这些末梢网络的默认路由。静态路由一般情况下要比其他动态路由协议级别高,也就是说即使通过动态路由协议选举出一条最优路径,数据包仍然会依据静态路由制定的路径进行传递,因此设计人员需要根据实际需要来确定静态路由选择协议的范围,以免使得动态路由协议失效。最后,静态路由信息可以导入动态路由选择协议形成的路由表项中,形成路由信息的互补关系。

5. 网络管理

网络管理并不是单纯的技术工作,而是行政管理与技术管理共同组成的复杂体。在目前网络管理技术快速发展的同时,行政管理明显出现了滞后的现象,导致网络运行故障的原因很大一部分并不是来自于网络管理技术上的漏洞,而是来自于行政管理上的疏忽或错误。

在进行网络设计时,为加强网络管理工作有效性,可将网络的管理手段分为两大类,即行政管理和技术管理。其中技术管理又依据管理技术的层次性划分为 TMS (传输管理系统)、NMS (网络管理系统)、RMS (资源管理系统)和 AMS (应用管理系统)。网络管理手段的构成情况如图 2-5 所示。

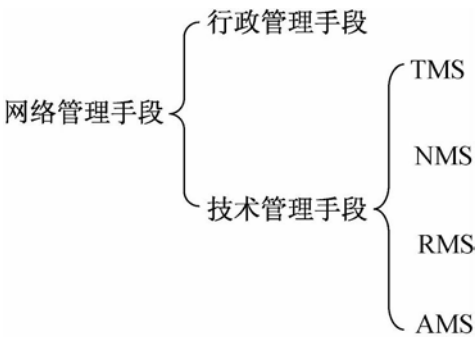


图 2-5 网络管理手段的构成

1)行政管理手段

通常情况下网络管理中心是企业网络管理、维护的核心部门,在网络管理中心设计和建立完善的行政管理制度是保证网络平台稳定运行的关键。各行政部门都有自己的岗位职责和管理制度,在管理的过程中必须严格遵守自己的岗位职责和管理制度。

2)技术管理手段

(1)TMS 是网络平台传输线路管理的主要管理工具。在一个大型网络中,大量的传输线路构成了网络的基础,而 TMS 就是对这些传输线路进行管理的系统,它对光纤资源、SDH 电路等物理或逻辑线路状态、参数等进行实时管理与监控。

(2)NMS 是较为经典的网络管理方式,在 ISO 规定的网络管理基本功能中,网络管理功能被划分为配置管理、安全管理、故障管理、费用管理和性能管理五大部分。

(3)RMS 是要建立一个完整的网络视图,包括传输网络、信令网络和数据网络(能体现各个网络之间的关联关系,并能管理网络资源和地理信息之间的关联关系,使操作人员很方便地了解网络资源在地理上的分布情况)以及机房、管线等非智能的设备的视图。

(4)目前 AMS 的概念较为模糊,与 RMS 有一定的重合,但是 AMS 更加注重对用户服务的管理,通过对运行于服务器上的用户服务进程实施监视,来实现对应用资源的管理。

6. 网络安全

1) 网络安全设计原则

在对一个企业局域网网络系统安全方案进行设计、规划时,应遵循以下原则:

(1)综合性、整体性原则。一个较好的安全措施往往是多种方法适当综合应用的结果。一个计算机网络,包括个人、设备、软件、数据等,这些环节在网络中的地位 and 影响作用,也只有从系统整体的角度去看待、分析,才能取得有效、可行的措施,即计算机网络安全应遵循整体安全性原则,根据规定的安全策略制定出合理的网络安全体系结构。

(2)一致性原则。一致性原则主要是指网络安全问题应与整个网络的工作周期(或生命周期)同时存在,制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计(包括初步或详细设计)、实施计划、验证、验收及运行等,都要有保证网络安全的内容及措施。实际上,在网络建设的开始就考虑网络安全对策,比在网络建设好后再考虑安全措施更容易,且花费也小得多。

(3)易操作性原则。安全措施需要人为完成,如果措施过于复杂,对人的要求过高,本身就降低了安全性。另外,措施的采用不能影响系统的正常运行。

(4)分步实施原则。由于网络系统及其应用扩展范围广阔,随着网络规模的扩大及应用的增加,网络脆弱性也会不断增加,一劳永逸的想法是不现实的。同时由于实施信息安全措施需相当的费用支出,因此分步实施,既可满足网络系统及信息安全的基本需求,又可节省费用开支。

(5)多重保护原则。任何安全措施都不是绝对安全的,都可能被攻破。但是建立一个多重保护系统,各层保护相互补充,当一层保护被攻破时,其他层仍可保护信息的安全。

(6)可评价性原则。如何预先评价一个安全设计并验证其网络的安全性,这需要通过国家有关网络信息安全测评认证机构的评估来实现。

2) 网络安全措施

局域网是基于广播技术构建的。局域网的数据截取和窃取成了局域网安全的主要问题。另外,ARP 地址欺骗等问题、TCP/IP 固有的不安全因素、网络操作系统的安全缺陷等,都使得基于局域网的安全防范非常关键。局域网安全措施主要从两方面做起,即局域网本身的安全和网络操作系统的安全。

(1)局域网本身的安全。要保证局域网本身的安全需采取的措施有:

- 网络分段。网络分段可以有效地阻隔网络资源的窃取和网络病毒的传播。可对网络进行物理分段和逻辑分段。
- 组建交换式以太网。对交换机进行网络分段后,建立交换式局域网,可以仅在两个结点间传送单播包,从而防止非法窃听。
- 虚拟局域网。采用交换式局域网技术组建的局域网,可以运用 VLAN 技术来加强内部网络管理。
- 网络访问权限设置。局域网中的主机访问进行权限和用户身份设置,则可以完全被局域网中的用户访问而不被外网用户访问,实现数据的加密服务。
- 网络设备安全控制。局域网中的路由器和交换机内置防火墙功能,对数据进行过滤且限制出入网络的数据,从而增强网络的安全性。
- 防火墙控制。防火墙用于执行两个网络之间的访问控制策略,有效地监控了内部网和 Internet 之间的任何活动。

(2)网络操作系统的安全。网络操作系统的安全主要涉及以下几个方面:

- 安全密码控制。对使用网络操作系统的用户设置一个足够强壮的账号和密码非常关键。
- 安全漏洞扫描和补丁安装。目前的网络操作系统,时常出现新的漏洞和安全威胁,所以用户在使用的时候一定要进行定期的安全漏洞扫描和补丁安装。这个可以借助一些软件来完成,如 360 安全卫士等。
- 防火墙和杀毒软件的使用。因为防火墙和杀毒软件本身定位不同,所以在安装反病毒软件之后,还不能阻止黑客攻击,用户须再安装防火墙等软件来保护系统安全。

7. 编写逻辑设计文档

逻辑设计文档是所有网络设计文档中技术要求最详细的文档之一。该文档是需求、通信分析到实际的物理网络建设方案的一个过渡阶段文档,也是指导实际网络建设的一个关键性文档。

在该文档中,网络设计者针对通信规范说明书中所列出的设计目标,明确描述网络设计的特点,所制定的每项决策都必须有通信规范说明书、需求说明书、产品说明书以及其他事实作为凭证。编写逻辑设计文档必须使用非技术性描述的语言,并与客户就业务需求方面详细讨论,从而设计出符合用户需要的网络方案。

需要注意的是,在正式编写逻辑网络设计文档之前,需要进行数据准备。例如,需求说明书、通信规范说明书、设备说明书、设备手册、设备售价、网络标准以及其他设计者在选择网络技术时所用到的信息等,这些可能都是逻辑设计阶段需要的原始数据。

2.3 物理网络设计

物理网络设计是网络设计过程中,紧随逻辑网络设计的一个重要设计部分。物理网络设计通过对逻辑网络设计的物理化,提供了网络实施所必需的信息。物理网络设计的任务是为所设计的逻辑网络设计特定的物理环境平台,主要包括结构化布线系统设计、机房设计、设备选型和网络实施,这些内容要有相应的物理设计文档。由于逻辑网络设计是物理网络设计的基础,因此逻辑网络设计的商业目标、技术需求和网络通信特征等因素都会影响物理网络设计。

2.3.1 结构化布线系统设计

结构化布线系统是一个能够支持任何用户选择的语音、数据、图形、图像应用的电信布线系统。系统应能支持语音、图形、图像、数据多媒体、安全监控和传感等各种信息的传输,支持 UTP、光纤、STP 和同轴电缆等各种传输载体,支持多用户多类型产品的应用,支持高速网络的应用。

结构化布线系统分为工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统共 6 个子系统,如图 2-6 所示。

1. 工作区子系统

工作区子系统是一个从信息插座延伸至终端设备的区域。工作区布线要求相对简单,

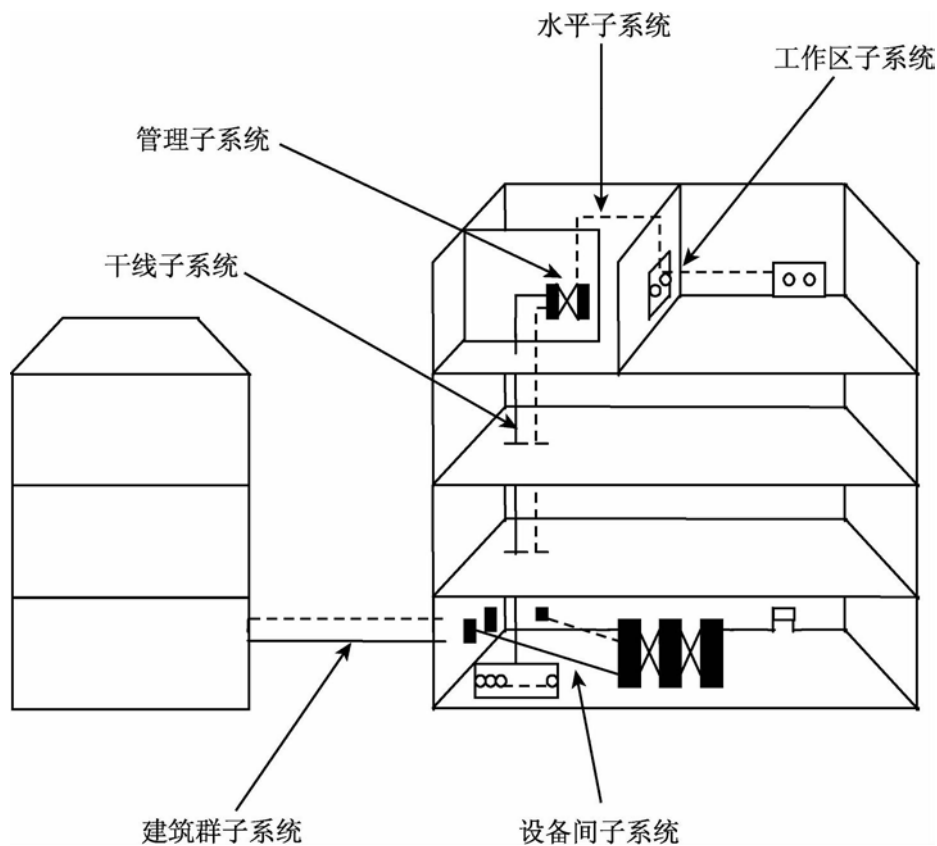


图 2-6 结构化布线系统

这样就容易移动、添加和变更设备。该子系统包括水平配线系统的信息插座、连接信息插座和终端设备的跳线以及适配器。

工作区子系统的设计要点如下：

- (1) 工作区内线槽的敷设要合理、美观。
- (2) 信息插座设计在距离地面 30 cm 以上。
- (3) 信息插座与计算机设备的距离保持在 5 m 范围内。
- (4) 网卡接口类型要与线缆接口类型保持一致。
- (5) 所有工作区所需的信息模块、信息插座、面板的数量要准确。
- (6) 所需的 RJ-45 水晶头数量要准确。

工作区设计时，具体操作可按以下 3 步进行：

- (1) 根据楼层平面图计算每层楼布线面积。

(2) 估算信息引出插座数量，一般设计两种平面图供用户选择：为基本型设计出每 9 m^2 一个信息引出插座的平面图；为增强型或综合型设计出两个信息引出插座的平面图。

- (3) 确定信息引出插座的类型。

2. 水平子系统

水平子系统也称水平在线子系统，是整体布线系统的一部分，一般在一个楼层上，是从工作区的信息插座开始到管理子系统的配线架。

1) 水平子系统设计要求

- (1) 用户对工程提出的近期和远期的终端设备要求。
- (2) 每层需要安装的信息插座数量及其位置。
- (3) 终端设备将来可能要增加、移动和重新安排的详细情况。

(4)一次性建设和分期建设的方案比较。

2)水平子系统线缆选择的一般原则

(1)产品选型必须与工程实际相结合。

(2)选用的产品应符合我国国情和有关技术标准(包括国际标准、我国国家标准和行业标准)。

(3)近期和远期相结合。

(4)符合技术先进和价格合理相统一的原则。

3)水平子系统布线方案

设计者要根据建筑物的结构特点,从路由(线)最短、造价最低、施工方便、布线规范等几个方面考虑。水平子系统布线一般可采用以下 3 种类型:

(1)直接埋管式。

(2)先走吊顶内线槽,再走支管到信息出口的方式。

(3)适合大开间及后打隔断的地面线槽方式。

3. 干线子系统

干线子系统由设备间的建筑物配线设备、跳线以及设备间至各楼层交接间的干线电缆组成。它既要满足当前的需要,又要适应今后的发展。干线子系统包括供各条干线接线间的电缆,走线用的竖向或横向通道和主设备间与计算机中心间的电缆。

1)干线子系统设计时应该考虑的问题

(1)确定每层楼的干线要求。

(2)确定整座楼的干线要求。

(3)确定从楼层到设备间的干线电缆路由。

(4)确定干线接线间的接合方法。

(5)选定干线电缆的长度。

(6)确定敷设附加横向电缆时的支撑结构。

2)干线子系统设计原则

(1)在确定干线子系统所需要的电缆总对数之前,必须确定电缆中语音和数据信号的共享原则。

(2)应选择干线电缆最短,最安全、最经济的路由。

(3)干线电缆可采用点对点端接,也可采用分支递减端接以及电缆直接连接的方法。

(4)如果设备间与计算机房处于不同的地点,而且需要把语音电缆连至设备间,把数据电缆连至计算机房,则宜在设计中选干线电缆的不同部分来分别满足语音和数据的需要。

3)干线子系统布线设计的步骤

(1)确定每层楼的干线电缆要求。根据不同的需要和经济因素选择干线电缆类别。

(2)确定干线电缆路由。

(3)绘制干线路由图。采用标准中规定的图形与符号绘制垂直子系统的线缆路由图,图纸应清晰、整洁。

(4)确定干线电缆尺寸。干线电缆的长度可用比例尺在图纸上实际量得,也可用等差数列计算。每段干线电缆长度要有备用部分(约 10%)和端接容差。

4. 设备间子系统

设备间子系统由设备室的电缆、连接器和相关支撑硬件组成,通过电缆把各种公用系统

设备互连起来。它是一个公用设备存放的场所,也是日常管理设备的地方。设备间可与计算机机房合用,也可单独设置。

1) 设计设备间子系统时的注意事项

- (1) 设备间应设在位于干线综合体的中间位置。
- (2) 尽可能靠近建筑物电缆引入区和网络接口。
- (3) 设备间应在服务电梯附近,便于装运笨重设备。
- (4) 室内无尘土,通风良好,要有较好的照明度。
- (5) 要安装符合机房规范的消防系统。
- (6) 使用防火门,墙壁使用阻燃漆。
- (7) 提供合适的门锁,至少要有安全通道。
- (8) 防止可能的水害(如暴雨成灾、自来水管爆裂等)。
- (9) 尽量远离有害气体源、腐蚀物、易燃物、易爆物和电磁场的干扰。

2) 设备间子系统的主要设备

设备间子系统的硬件大致同管理子系统的硬件相同,主要设备有数字程控交换机、路由器、计算机等。

3) 设备间子系统的使用面积

对于设备间的主要设备的使用面积,必须有一个通盘的考虑。目前,对设备间的使用面积可用两种方法来确定。

方法一: $S = K \sum S_i (i = 1, 2, \dots, n)$

其中: S 为设备间使用的总面积,单位为 m^2 ; K 为系数,指每一个设备预占的面积,一般选择 5、6、7 三种(根据设备大小来选择); $\sum$ 为求和; S_i 为设备件; i 为变量; n 为设备间内共有设备总数。

方法二: $S = KA$

其中: S 为设备间使用的总面积,单位为 m^2 ; K 为系数,为 $(4.5 \sim 5.5) \text{m}^2/\text{台(架)}$; A 为设备间所有设备的总数。

4) 设备间子系统设计的环境条件

(1) 温度和湿度。网络设备间一般将温度和湿度分为 A、B、C 三级,设备间可按某一级执行,也可按某几级综合执行。

(2) 尘埃。设备对设备间内的尘埃量是有要求的,一般可分为 A、B 两级。

(3) 照明。设备间内在距地面 0.8 m 处,照明度不应低于 200 lm(亮度单位)。还应设事故照明,在距地面 0.8 m 处,照明度不应低于 5 lm。

(4) 噪声。设备间的噪声应小于 65 dB。如果长时间在 65~80 dB 噪声的环境下工作,不但影响人的身心健康和工作效率,还可能造成人为的噪声事故。

(5) 电磁场干扰。设备间内无线电干扰场强,在频率为 0.15~1 000 MHz 范围内不大于 120 dB;设备间内磁场干扰场强不大于 800 A/m。

(6) 供电。设备间供电电源应满足以下条件:

- 频率: 50 Hz。
- 电压: 380/220 V。
- 相数: 三相五线制或三相四线制/单相三线制。

(7)安全。按照 GB/T 9361—1988《计算机场地安全要求》的规定,设备间的安全可分为 A 类、B 类、C 类 3 个基本类别。

- A 类:对设备间的安全有严格的要求,设备间有完善的安全措施。
- B 类:对设备间的安全有较严格的要求,设备间有较完善的安全措施。
- C 类:对设备间有基本的要求,设备间有基本的安全措施。

5. 管理子系统

管理子系统设备设置在每层配线设备的房间内,管理子系统由交接间的配线设备、输入/输出设备等组成。在不同类型的建筑物中管理子系统常采用单点管理单交连、单点管理双交连和双点管理双交连 3 种方式。

1) 管理子系统的设计原则

(1)干线配线管理宜采用双点管理双交连方式,网络中有两个连接点可以进行线路交连操作,其他连接点直接连接。

(2)楼层配线管理应采用单点管理方式,网络中只有一个连接点可以进行线路交连操作,其他连接点采用直接连接。

(3)配线架的结构取决于信息点的数量、综合布线系统网络性质和选用的硬件。

(4)端接线路模块化系数合理。

(5)设备跳接线连接方式要符合下列规定:对配线架上相对稳定一般不经常进行修改、移位或重组的线路,宜采用卡接式接线方法;对配线架上经常需要调整或重新组合的线路,宜使用快接式插接线方法。

(6)管理接线间墙面材料清单应全面,并画出详细的墙面结构图。

2) 管理子系统的设计步骤

(1)确认线路模块化系数是 2 对线还是 3 对线。将每个线路模块当做一条线路处理,线路模块化系数视具体系统而定。

(2)确定语音和数据线路要端接的电缆对总数,并分配好语音或数据数线路所需的墙场或终端条带。

(3)决定采用何种 110 型(一种工业标准)交连硬件。

- 如果线对总数超过 6 000(即 2 000 条线路),则使用 110A 交连硬件。
- 如果线对总数少于 6 000,则可使用 110A 或 110P 交连硬件。
- 110A 交连硬件点占用较少的墙空间或框架空间,但需要一名技术人员负责线路管理。
- 决定每个接线块可供使用的线对总数,主布线交连硬件的白场接线数目取决于 3 个因素:硬件类型、每个接线块可供使用的线对总数和需要端接的线对总数。
- 由于每个接线块端接行的第 25 对线通常不用,故一个接线块极少能容纳全部线对。
- 决定白场的接线块数目。为此,首先把每种应用(语音或数据)所需的输入线对总数除以每个接线块的可用线对总数,然后取更高的整数作为白场接线块数目。
- 选择和确定交连硬件的规模——中继线/辅助场。
- 确定设备间交连硬件的位置。
- 绘制整个布线系统即所有子系统的详细施工图。

(4)管理间的信息点连接是非常重要的工作,它的连接要尽可能简单,主要工作是跳线。

6. 建筑群子系统

连接各建筑物之间的传输媒介和各种支持设备(硬件)组成一个建筑群综合布线系统。连接各建筑物之间的缆线及相应设备组成了建筑群子系统。

1) 建筑群子系统设计步骤

(1) 确定敷设现场的特点。

- 确定整个施工工地的大小。
- 确定施工工地的地界。
- 确定共有多少座建筑物。

(2) 确定电缆系统的一般参数。

- 确认起点位置。
- 确认端结点位置。
- 确认涉及的建筑物和每座建筑物的层数。
- 确定每个端结点所需的双绞线对数。
- 确定有多个端结点的每座建筑物所需的双绞线总对数。

(3) 确定建筑物的电缆入口。

- 对于现有建筑物,要确定各个入口管道的位置;确定每座建筑物有多少入口管道可供使用;确定入口管道数目是否满足系统的需要。
- 如果入口管道不够用,要确定在移走或重新布置某些电缆时是否能腾出某些入口管道,以及在不够用的情况下应另装多少入口管道。
- 如果建筑物尚未建起来,则要根据选定的电缆路由完善电缆系统设计,并标出入口管道的位置;选定入口管道的规格、长度和材料;在建筑物施工过程中安装好入口管道。

(4) 确定明显障碍物的位置。

- 确定土壤类型:砂质土、黏土、砾土等。
- 确定电缆的布线方法。
- 确定地下公用设施的位置。
- 查清拟定的电缆路由中沿线的各个障碍物位置或地理条件。
- 确定对管道的要求。

(5) 确定主电缆路由和备用电缆路由。

- 对于每一种待定的路由,确定可能的电缆结构。
- 所有建筑物共用一根电缆。
- 对所有建筑物进行分组,每组单独分配一根电缆。
- 每座建筑物单用一根电缆。
- 查清在电缆路由中哪些地方需要获准后才能通过。
- 比较每个路由的优缺点,从而选定最佳路由方案。

(6) 选择所需电缆类型和规格。

- 确定电缆长度。
- 画出最终的结构图。
- 画出所选定路由的位置和挖沟详图,包括公用道路图或任何需要经审批才能动用的地区草图。

- 确定入口管道的规格。
- 选择每种设计方案所需的专用电缆。
- 应保证电缆可进入口管道。

(7) 确定每种方案所需的劳务成本。

(8) 确定每种方案所需的材料成本。

- 确定电缆成本。
- 确定所有支持结构的成本。
- 确定所有支撑硬件的成本。

(9) 选择最经济、最实用的设计方案。

- 把每种选择方案的劳务费成本加在一起, 得到每种方案的总成本。
- 比较各种方案的总成本, 选择成本较低者。
- 确定该方案是否有重大缺点以致抵消了经济上的优点。如果发生这种情况, 应取消此方案, 考虑经济性较好的设计方案。

2) 建筑群子系统的设计要点

(1) 建筑群数据网主干线缆一般应选用多模或单模室外光缆。

(2) 建筑群数据网主干线缆需使用光缆与电信公用网连接时, 应采用单模光缆, 芯数应根据综合通信业务的需要确定。

(3) 建筑群主干线缆宜采用地下管道方式进行敷设, 设计时应预留备用管孔, 以便扩充使用。

(4) 当采用直埋方式时, 电缆通常在离地面 60.96 cm 以下的地方或按当地法规敷设。

2.3.2 机房设计

机房的设计应参照 GB 50174—2008《电子信息系统机房设计规范》, 需要遵循的设计要求如下。

1) 中心机房位置选择

(1) 中心机房的物理位置在多层建筑或高层建筑物内应设于第 1~8 层, 更高层次不适合作为机房建设楼层。

(2) 机房位置选择应符合以下要求:

- 水源充足, 电力比较稳定可靠, 交通、通信方便, 自然环境清洁。
- 远离产生粉尘、油烟、有害气体以及生产或储存具有腐蚀性、易燃、易爆物品的工厂、仓库、堆场等。
- 远离强振源和强噪声源。
- 避开强电磁场干扰。

(3) 若无法避开强电磁场干扰或为保障计算机系统信息安全, 可采取有效的电磁屏蔽措施。

2) 中心机房组成

(1) 中心机房组成应按计算机运行特点及设备具体要求确定, 一般应由主机房、基本工作间、第一类辅助房间、第二类辅助房间和第三类辅助房间等组成。

(2) 中心机房的使用面积应根据网络与计算机设备的外形尺寸布置确定。

3) 设备布置

(1) 网络与计算机设备宜采用分区布置,一般可分为服务器区、存储器区、网络设备区、安全设备区、通信区和监控区等。

(2) 需要经常监视或操作的设备应布置于方便行走、便于操作的位置。

(3) 产生尘埃及废物的设备应远离对尘埃敏感的设备,并宜集中布置在靠近机房的回风口处。

(4) 主机房内通道与设备间的距离应符合:两个相对机柜正面之间的距离应不小于 1.5 m,机柜侧面或不用面与墙的距离应不小于 0.5 m;当需要维修测试时,距墙应不小于 1.2 m;走道净宽应不小于 1.2 m。

2.3.3 设备选型

1. 设备选型的原则

(1) 必须和工程实际相结合。

(2) 选用的产品应符合我国的国情以及国际、国内和行业的有关技术标准。

(3) 近期与远期相结合。

(4) 技术先进和价格合理相统一。

2. 设备选型的具体步骤和方法

(1) 充分了解需求的前提条件,收集基础资料。

(2) 设备选型之前应该进行调查或者收集产品资料,访问已经使用过该产品的单位,充分掌握其使用效果;听取各种反馈意见,以便对产品进行分析;认真筛选两三种产品,为进一步考察评估做好准备。

(3) 对初选设备客观公正地进行技术价格的比较和全面评估,选出理想的产品。

(4) 重点考察初选设备的生产厂家的技术力量、生产装备、工艺流程和售后服务等,实地考察设备的使用情况,对某些基本性能进行现场测试,以求得第一手资料。

(5) 经过上述工作后,对所选的设备应该有了比较全面的综合性认识,本着经济实用、切实可行的原则,提出最后选用设备的意见,提请建设单位或者有关领导决策部门确定。

(6) 最后应该将网络设计工程所需要的主要设备、各种缆线、布线部件以及其他附件的规格数量进行计算和汇总,与生产厂商洽谈具体订购产品的细节,特别是产品质量、供货日期、地点和付款方式等,这些都应该在订货合同中明确规定,以保证综合布线系统工程能够按计划顺利进行。

2.3.4 编写物理设计文档

物理设计文档用于说明在怎样的特定物理位置实现逻辑设计方案,怎样有逻辑地开展每步设计,以及要进行哪些新安装,以便工程施工人员明白施工内容和要求。物理设计文档必须是正确的和完整的。它应包括以下内容:

(1) 工程概述。

(2) 物理设计图表。

(3) 注释和说明。

(4) 资产清单。

(5)最终费用估算。

(6)批文。

网络设计的每个阶段,都要清楚地将文字和图表排列清楚。收集阶段产生的是需求,物理设计阶段产生的主要是图表。物理设计图是一张详细的比例草图,是设计网络的结构蓝图,可以用它来估算所需线缆的长度,决定每部分线缆长度是否满足要求。由于施工人员和管理人员都要用到这张图,它必须正确、清楚、明晰。

为了防止图纸上表示不清,产生歧义,应对图表作适当的注释说明,尤其应说明所需线缆的类型、遵循的布线标准、物理施工安全问题和安装要点。

资产清单应包括 3 种类型的信息:新的工具和零件,网络中已有的设备,未应用的设备。

物理设计中应该详细说明新的网络安装需要多少软、硬件及其费用。这些费用应包括人力工时估计、整个安装时间进度安排和费用合计。

2.4 网络工程施工与测试

在进行完网络的逻辑设计和物理设计后,施工人员就可以按照所设计的网络结构和布线方案进行网络施工阶段的工作,在施工过程中必须严格按照网络设计的规范和要求进行操作。工程实施完成后,必须请专业人员进行工程的测试工作,以保证所组建的网络能够达到规定的要求。

2.4.1 网络工程实施

网络工程经过调研,确定方案后,下一步就是工程的实施,而工程实施的第一步就是开工前的准备工作。

1)准备工作要求做到以下几点

(1)设计综合布线实际施工图。设计综合布线实际施工图确定布线的走向位置,供施工人员、督导人员和主管人员使用。

(2)备料。网络工程施工过程需要许多施工材料,这些材料有的必须在开工前就备好料,有的可以在开工过程中备料,主要有以下几种:

- 光缆、双绞线、插座、信息模块、服务器、稳压电源、集线器等落实购货厂商,并确定提货日期。
- 不同规格的塑料槽板、PVC 防火管、蛇皮管等布线用料就位。
- 如果集线器是集中供电,则准备好导线、铁管和制定好电气设备安全措施(供电必须按民用建筑标准规范进行)。
- 制定施工进度表(要留有适当的余地,施工过程中意想不到的事情随时可能发生,并要求立即协调)。

(3)向工程单位提交开工报告。

2)施工过程中要注意的事项

(1)在工程实施过程中必须严格按照工程实施的有关标准进行施工。

(2)施工现场督导人员要认真负责,及时处理施工过程中出现的各种情况,协调处理各方意见。

(3)如果现场施工碰到未预知的问题,应及时向工程单位汇报,并提出解决办法供工程单位当场研究解决,以免影响工程进度。

(4)对工程单位计划不周的问题,要及时妥善解决。

(5)对工程单位新增加的点要及时在施工图中反映出来。

(6)对部分场地或施工段要及时进行阶段检查验收,确保工程质量。

(7)制定工程进度表。在制定工程进度表时,要留有余地,还要考虑其他工程施工时可能对本工程带来的影响,避免出现不能按时完工、交工的问题。

2.4.2 网络工程测试

当网络工程实施完成后,需要借助各种工具对网络进行分析测评,包括分析网络协议、监视网络运行状况、测量和统计网络流量、分析网络性能等。网络工程测试工具按照其在网络实施过程中所起的作用及功能可分为6类:测试和接口检测工具、协议分析仪、网络检测工具、网络管理工具和平台、网络仿真工具和网络设计辅助工具。

1. 测试和接口检测工具

测试和接口检测工具用来测试传输媒介和网络接口上的物理信号,它分为模拟测试装置和数字测试装置。模拟测试装置用来检测在模拟系统中的信号状态,而数字测试装置用来检测数字传输通道和设备接口。图2-7是FLUKE 125工业网络测试仪。网络测试仪的应用范围通常被限制在一个局域网内。



图 2-7 FLUKE 125 工业网络测试仪

2. 协议分析仪

协议分析仪就是能够捕获网络报文的设备。协议分析仪的正常用处在于捕捉分析网络的流量,以便找出所关心的网络中潜在的问题。例如,假设网络的某一段运行得不是很好,报文的发送比较慢,而又不知道问题出在什么地方,此时就可以用协议分析仪来作出精确的问题判断。它在功能和设计方面有很多不同。有些只能分析一种协议,而有能够分析几百种协议,大多数协议分析仪至少能够分析以太网协议、TCP/IP、IPX/SPX、DECnet 协议等。

协议分析仪能够监听、存储和分析网络流量,协议分析仪应具有的功能如下:

(1)完整的记录和存储网络流量。

- (2)网络分组过滤功能,且具有使用语音或图像信号报警的功能。
- (3)具有良好的用户界面,使用文本、图形等方式显示信息。
- (4)能检测不同类型的传输媒介,并能进行多信道测量。
- (5)能显示测试线路物理状态。
- (6)具有网络负载和差错率的统计功能。
- (7)能够自动检测到网络配置的变化。
- (8)能够在可控条件下执行负载测试。
- (9)能够远程操作,且可对测试结果进行在线和离线分析。

协议分析仪通常是软、硬件的结合,通常使用专用硬件或设置为专用方式的网卡实施对网络中的数据捕捉。捕获在网络中传输的数据信息方法称为 sniffing(嗅探)。图 2-8 是 FLUKE 集成式协议分析仪,它将用户所需的所有网络监测和故障诊断功能集成在一个用电池供电的手持式工具中。配件组成为一个高性能协议分析仪、一个快速电缆测试仪和一个 RMON2 探头等,用户可以迅速通过这些配件来透视整个网络。该分析仪共有 3 种型号,分别是标准型、增强型和千兆型,功能各不相同。



图 2-8 FLUKE 集成式协议分析仪

FLUKE 集成式协议分析仪具有全面的七层测试分析能力,可以进行自动 IP 配置、自动网络测试,能对交换环境网络设备进行主动搜寻,并提供对以太网的全面支持。此外也可支持 1 000Base-T/SX/LX、SNMP 设备分析及 RMON2 流量分析、数据包捕获和解码、网络数据吞吐能力测试、在线电缆测试、远程遥控测试、详尽的网络测试报告生成等功能。

3. 网络监测工具

随着 Internet 的发展,出现了大量的网络监测工具,被列在“TCP/IP Internet 和互连设备监测与调试工具”(RFC 1470)中的工具超过了 100 个。

支持网络故障监测的常用工具有:

- ping:使用 ICMP(因特网控制消息协议)进行网络连通性测试。
- netmon:使用轮询和中断对网络配置数据进行查询。
- snmpset:对每个互联网资源的参数进行设置。
- traceroute:对路径可达性进行分析。

支持网络性能测量及监视的工具有:

- spray:负载产生器。
- netstat:能够显示网络管理信息。
- tcpdump:能对 Ethernet、FDDI、ARP、RARP、TCP 和 IP 进行分析。
- tcptrace:能跟踪每一个连接的持续时间、每段发送和接收的字节数、重传及往返时延、窗口通告、吞吐量等。
- flstats:是从 tcpdump 文件中抽取流量统计的一个工具。

4. 网络管理工具和平台

网络管理功能包括故障管理、性能管理、配置管理、安全管理和记账管理五大功能,网络管理工具一般都是基于网络管理协议(如 SNMP)开发的。现在的网络管理平台软件非常多,但价格也非常贵。所以在许多中小企业中,这些网络管理软件并没得到广泛应用。目前主流的网络管理平台产品有:

- HP OpenView:HP 公司开发的网络管理平台,是一种当前网络管理领域比较流行的开放式、模块化、分布式的网络管理平台。
- AT-SNMPc:一个分布式的通用网络管理平台,可以直观显示、监控和前瞻性地管理网络,能有效地监控整个网络的基础架构,并支持 SNMP v3。
- CA Unicenter:功能完善、高度集成,而且十分开放,可支持包括 Linux 在内的所有主流平台。
- CiscoWorks:Cisco 公司为网络管理系统提供的一个基于 SNMP 的软件系列,它可继承在多个现行的网络管理系统上。
- IBM Tivoli NetView:为网络管理人员提供了一种功能强大的解决方案,应用也非常广泛。

5. 网络仿真工具

网络仿真是一种利用数学建模和统计分析的方法模拟的网络行为,从而获取特定的网络特性参数的技术。数学建模包括网络建模(网络设备、通信链路等)和流量建模两个部分。模拟网络行为是指模拟网络流量在实际网络中传输、交换和复用的过程。网络仿真获取的网络特性参数包括网络全局性能统计量、网络结点性能统计量、网络链路的流量和延迟等,由此既可以获取某些业务层的统计数据,也可以得到协议内部的某些特殊参数的统计结果。

从网络仿真工具的应用上,网络仿真软件可分为高端和低端两类产品。高端产品一般具有复杂的建模机制、比较完备的模型库、完善的外部接口、强大的功能,并能得到可靠的仿真结果,其主流产品如 MIL3 公司的 OPNET,CACI 公司的 COMNET 等。低端产品一般只有简单的建模机制、较小的模型库、简单的外部接口,功能单一且仿真结果的可靠性较差。

6. 网络设计辅助工具

网络设计辅助工具可用于网络规划与设计过程的需求分析和逻辑设计阶段,也可用于对所设计的网络进行性能评价。目前,国外已经有了一些成功的网络设计辅助工具,如 AUTONET、NPAT 等,这些网络设计辅助工具在网络设计中都发挥了很大作用。

2.5 组网实例——中小型规模办公局域网建设

前面讲解了局域网的组建方法和流程,下面就用实例来进行说明局域网组网的过程和方法。

2.5.1 需求分析

1. 背景

现有一公司共 3 栋楼:1 号楼,2 号楼,3 号楼。每栋楼之间直线距离为 100 m。

1 号楼:3 层,为行政办公楼,20 台计算机,分散分布。

2 号楼:5 层,为产品研发部,供销部,30 台计算机。其中,20 台集中在三楼的研发部的设计室中,专设一个机房;其他 10 台分散分布。这里要求供销部的计算机能够连接 Internet,单位生产的产品的信息能向网上发布,其他的一律不能上网。

3 号楼:5 层,为生产车间,每层一个车间,每个车间 3 台计算机,共 15 台。

2. 未来发展

未来的 3~5 年,单位计算机会增加到 150 台左右,主要增加在 2 号楼的研发部,计划该部门增加两间专用机房用于新产品的研发和设计。

3. 用户需求分析

为了能让公司更好地与现代社会的发展接轨,更快地获取市场信息以及让外界了解该公司的相关信息,特组建企业网,以实现对公司档案管理、产品信息、供求信息等方面进行计算机网络化管理。

4. 网络功能

根据公司现有规模、业务需要及发展范围建立的网络有如下功能:

- (1)建立公司自己的网站,可向外界发布信息,并进行电子商务活动。
- (2)要求供销部可以连接 Internet,与各企业保持联络,接收订单和发布本公司产品信息。其他部门都不能连接 Internet,但在本公司内部可以相互访问。
- (3)公司内部网络实现资源共享,以提高工作效率。
- (4)建立网络时应注意网络的扩展性,以方便日后的网络升级和增加计算机的操作。
- (5)在公司内部建立公司的数据库,如员工档案、业务计划、会议日程等。

2.5.2 网络结构设计

1. 现场勘察分析

根据公司大楼的结构特点制定详细的网络连接图,其中包括如下信息:

- (1)网络上各信息点(即办公点)的分布图,工作空间大小与距离。
- (2)电源插座的位置,包括目前正在使用插座的设备。
- (3)所有不可移动的物品的位置(如支撑柱、分隔墙、内置柜等)。
- (4)所有办公设备的当前位置。

(5)所有计算机和打印机等外部设备的位置。

(6)门和窗口的位置。

(7)通风管道和目前电线的位置。

2. 确定 Internet 的接入方式

建议租用专线与外界互连,用一台配置较先进的计算机作为代理服务器,进行 Internet 的连接。

3. 确定网络互连方式

首先要确定网络的拓扑结构,建议采用星型结构。100Base-T 星型结构以其速度快的优势成为以太网的理想选择。用双绞线作为传输线缆,星型总线网的物理结构采用星型连接,逻辑结构采用总线型的,采用 IEEE 的 802.3 协议标准。网卡、集线器和双绞线应选 100 Mb/s 的。当用户扩展过多时,可采用堆叠式集线器。

然后确定互连方式,因为有一部分用户可以连接 Internet,另一部分不可以,所以通常有两种方式可供选择:

(1)分成两个子网,各连接一个交换机,并连接到服务器的不同的网卡上,在服务器上设置一个网卡可以连接 Internet,另一个不可以,结构如图 2-9 所示。

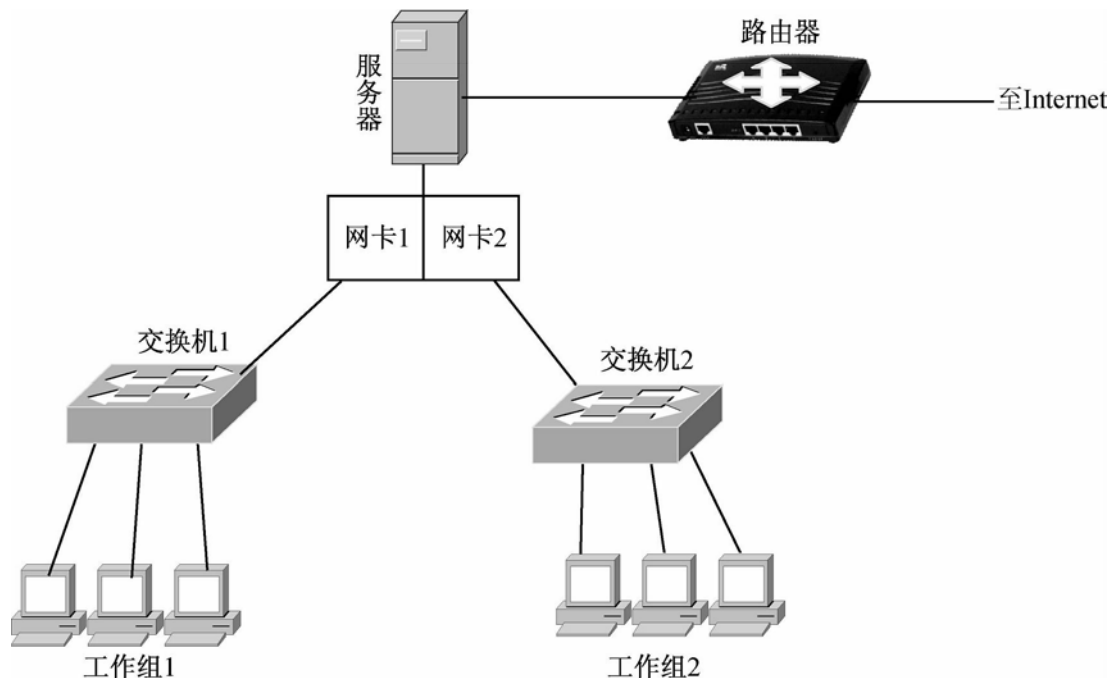


图 2-9 星型结构

(2)分成三个子网,都连接到路由器上,在路由器上设置 IP,其中两个子网的 IP 设置为内部 IP,不允许访问 Internet,结构如图 2-10 所示。

综合以上两种网络互连方式,选择第二种互连方式。这种连接结构条理清晰,结构划分明确,而且上网速度不受服务器配置的影响,但相对第一种方式设备投资稍大。

因为公司所有的计算机加起来不足 250 台,因此局域网内部的 IP 地址全部使用 C 类地址,局域网通过一台路由器连接 Internet,以后内部信息点的增加可以通过增加堆叠交换机的数量来满足需求。

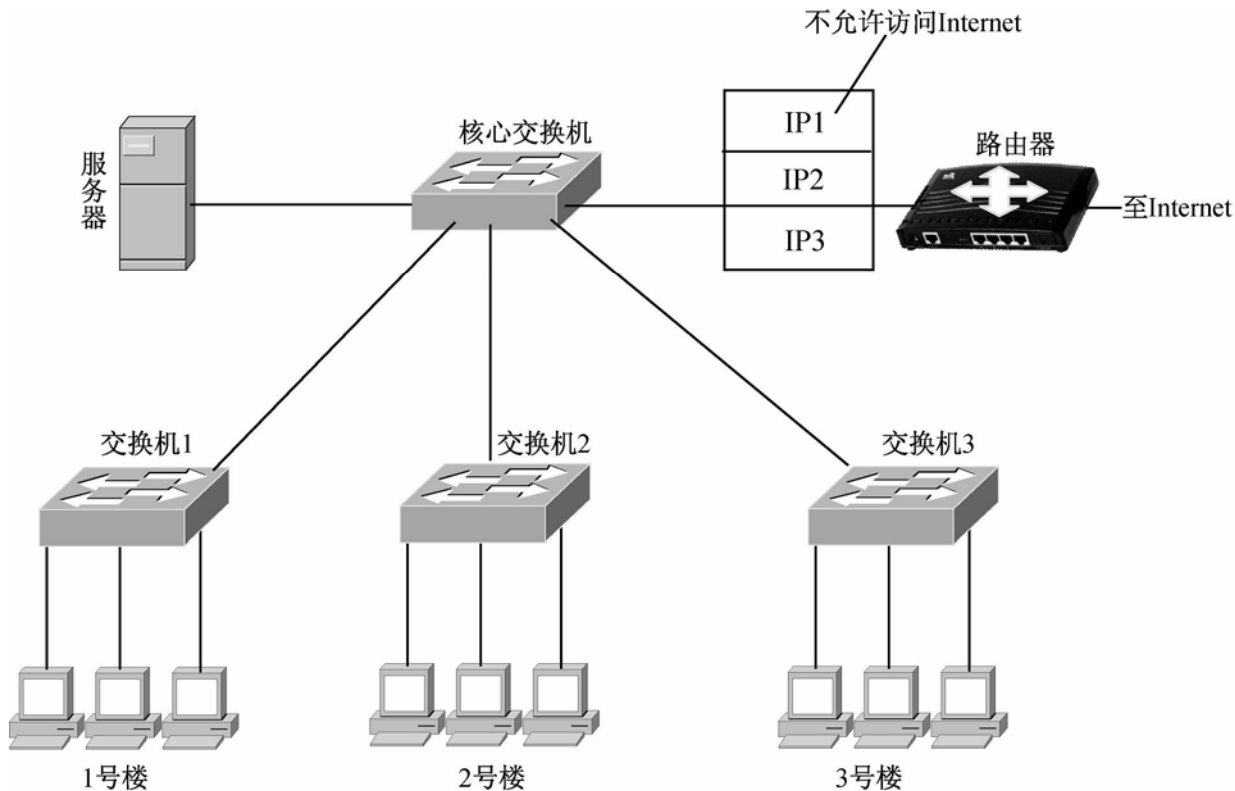


图 2-10 子网划分

2.5.3 布线系统设计

综合布线要符合楼宇管理自动化、办公自动化、通信自动化和计算机网络化等多功能的需要。系统应能支持语音、图像、图形、数据多媒体、安全监控、传感等各种信息传输,支持光纤、非屏蔽双绞线、屏蔽双绞线、同轴电缆等各种传输媒介,支持多用户多类型产品的应用,支持高速网络的应用。综合布线系统设计要根据建筑结构和用户需求来确定,这一过程主要包括以下几个要点:

- (1) 尽量满足用户的通信要求。
- (2) 了解建筑物内部的通信环境。
- (3) 确定合适的通信网络拓扑结构。
- (4) 选取将要使用的传输媒介。
- (5) 以开放式为基础,尽量与大多数厂家的产品和设备兼容,按照通用的标准进行设计。
- (6) 系统初步设计成本估算。
- (7) 将系统初步设计和建设费用预算告知用户。
- (8) 在征得用户意见并签订合同后,制定详细的设计方案。

综合布线可采用 UTP、STP 或者光缆,在欧洲综合布线所采用的线缆中,占主流的是屏蔽系统;而在北美广泛使用的是非屏蔽系统,在高容量主干及严重干扰的情况下就使用光缆作为屏蔽系统。但 STP 系统若使用不当,非但达不到整体屏蔽的完整性,其性能也会比 UTP 系统更差。UTP 是目前较为成熟、可靠的商用建筑综合布线系统所采用的线缆,通常情况下也可以满足在干扰环境下的使用需求。所以建议使用 UTP 或光缆。

在建筑物内部布线通常有 3 种方式:走墙壁、走屋顶、走地板。走线有两种选择:明线和暗线。当布线房间或走道比较狭窄且层高较低时,宜选择明线,用 PVC 线槽走墙壁。采用

明线费用较低,采用暗线不仅昂贵,而且需要架顶,架地板或打夹层,不过比较美观。若房间的高度允许,可以选择架顶或架地板。其中架地板便于安装,不过维护更贵一些。若房间的宽度允许,可以通过给墙壁打夹层走暗线,这样不仅将墙壁装饰得很漂亮,也易于维护。在楼层过道,三种方式都可以使用,但站点较集中的房间建议采用架地板的方式,会使安装和维护都更方便。

建议把主机设在 2 号楼的三楼,建筑群间采用地下管道敷设方式,管道内敷设室外用 12 芯多模光缆。安装时至少要预留 1~2 个备用管孔,以供扩充之用。在 1 号楼和 3 号楼放置光缆收发器,以确保信号正常传输。室内连接为节约资金可采用双绞线,同一楼层上的水平系统多采用四对双绞线,电缆长度宜在 90 m 以内,垂直干线子系统总是位于垂直的弱电间,并采用大对数双绞线。

2.5.4 设备选型

建议服务器配置(假设本公司已经有其他计算机)如表 2-6 所示。

表 2-6 建议服务器配置表

服务器配件	推荐配件型号
CPU	Intel Xeon 3220 2.4G
内存	金士顿 2GB DDR2 800
硬盘	320 GB 和 SCSI 接口硬盘
光驱	华硕 DVD-RM-E818A4 静音王
显卡	NVIDIA GeForce GT 240

组网相关设备及配件推荐设备如表 2-7 所示。

表 2-7 组网相关设备及配件推荐设备表

网络配件	推荐使用参数
网卡	采用 100/1 000 Mb/s 自适应全双工网卡
交换机	采用 24 口交换机,便于日后扩展
网线	使用超五类非屏蔽双绞线
网络接头	RJ-45
信息插座	AMP 双口信息插座面板
服务器操作系统	建议使用 Windows Server 2003

网络建设硬件及软件型号、单价及数量清单如表 2-8 所示。

表 2-8 硬件及软件清单

设备名	型号	单价/元	数量
服务器	略	25 000	1 个
交换机	BENQ-SS0224	2 200	4 个
网卡	神州数码 DCN-550GT	690	1 个

续表

设备名	型号	单价/元	数量
路由器	Cisco-7513	11 800	1 个
光纤	室外用 12 芯多模	37	300 m
光纤配线架	—	580	4 个
光纤配线面板	—	75	5 个
光纤耦合器	—	50	10 个
光纤收发器	10/100Mb/s	2 000	2 个
接地夹	—	200	2 个
光纤套管	—	950	1 个
ST 光纤接头	—	80	10 个
PVC 管材	室外用	3	330 m
AMP 信息面板	—	4	70 个
RJ-45	—	1.5	300 个
双用打线工具	—	250	1 个
双绞线	超五类非屏蔽	780	25 箱
PVC 管材	室内用	3	900 m
标签条	—	25	4 包
Windows Server 2003	—	1 957	1 套
Microsoft Office XP	简体中文标准版	3 940	1 套
金山毒霸 6	—	198	1 套

预计硬件花费 91 005 元,软件花费 6 095 元,合计 97 100 元。

2.5.5 网络施工和验收

工程立项审批同意后应由专业的网络工程公司组织施工和管理。施工过程中要根据技术要求、工程量、工程难度等确定施工方式,并于计划开工前 3 日下达施工任务书给工程申报主体。各施工主体必须严格按审核通过后的技术方案、施工图纸进行施工,不得擅自变更技术方案或施工图纸。若遇特殊情况,中途需作较大变更的,必须报工程主体单位,经技术部会同相关部门论证同意后,方可变更,同时调整材料预算和工程量预算。施工过程中,各施工主体必须做到科学组织,合理调度,尽可能缩短工期。各施工主体及人员必须强化安全意识,严格按照广播电视安全操作规程进行作业,消除各种施工安全隐患,确保工程施工安全无事故。

工程完工后施工方提交工程验收申请。提交申请时,工程竣工图、材料决算表、工程量决算表等材料必须齐全,否则不予验收。工程申报主体要组织专业团队进行工程的验收工作。验收根据需要分为全面验收和抽样验收。验收工作必须严格按照国家有关规定进行。

习 题 2

一、选择题

1. 通常网络系统中带宽都用传输率来描述,其单位为()。
A. Kb/s B. Mb/s C. KB D. MB
2. 如果既要传输距离远,又要抗干扰性能好,应选择()为传输媒介。
A. 双绞线 B. 同轴电缆 C. 光纤 D. 红外线
3. 主机房内两相对机柜正面之间的距离应不小于()。
A. 1.5 m B. 2.0 m C. 2.5 m D. 3.0 m

二、填空题

1. 影响用户网络性能的因素有:通信距离、_____、_____、_____和核心干线吞吐量。
2. _____设计要根据网络用户的分类和分布选择特定的技术,形成特定的网络结构。

三、问答题

1. 网络需求分析的具体内容包括哪些?
2. 逻辑网络设计的工作内容是什么?
3. 物理设计文档应该包括哪些内容?
4. 影响需求分析的因素包括哪些?

第 3 章 局域网接入 Internet

知识目标

- ◎ 了解局域网接入 Internet 的接入技术
- ◎ 了解局域网接入 Internet 的方式
- ◎ 了解远程桌面技术
- ◎ 掌握局域网代理型接入 Internet 的方式

技能目标

- ◎ 熟悉常用代理软件的使用方法
- ◎ 能够进行网络地址转换的设置和地址分配
- ◎ 能够根据不同的网络类型,选择合理的局域网接入 Internet 方式

Internet 是目前世界上最大的计算机互连网络,它提供了丰富的信息资源,并使得企业与外界的联系变得简单、方便、准确、高效。它最大的优势之一就是使用便捷,入网用户不必具备计算机网络的专门知识,便可自由使用网络。因此,可以说加入 Internet 是时代发展的需要。

3.1 Internet 的接入技术与方式

接入技术要解决的问题是如何将用户连接到各种网络上。作为网络中与用户相连的最后一段线路上所采用的技术,接入技术已成为目前网络技术的一大热点。为了提供端到端的宽带连接,接入技术是必须要解决的问题。

3.1.1 Internet 的接入技术

按传输媒介分,目前主要的接入技术有以下几种。

1. 光纤接入

光纤是目前传输速率最高的传输媒介。在主干网中已大量采用了光纤。如果将光纤应用到用户环路中,就能满足用户将来各种宽带业务的要求。可以说,光纤接入是宽带接入网的最终形式。但目前要完全抛弃现有的用户网络而全部重新铺设光纤,对于大多数国家和地区来说是不经济、不现实的。

2. 同轴电缆接入

同轴电缆是传输带宽比较大的一种传输媒介。目前的 CATV 网就是一种混合光纤同轴(HFC)网络,主干部分采用光纤,用同轴电缆经分支器接入各家各户。混合光纤同轴接入技术的一大优点是可以利用现有的 CATV 网,从而降低网络接入成本。

3. 铜线接入

铜线接入是指以现有的电话线为传输媒介,利用各种先进的调制技术、编码技术和数字信号处理技术来提高铜线的传输速率和传输距离。但是铜线的传输带宽毕竟有限,铜线接入方式的传输速率和传输距离一直是难以调和的矛盾。从长远的观点来看,铜线接入方式很难适应将来宽带业务发展的需要。

4. 无线接入

无线用户环路是指利用无线技术为固定用户或移动用户提供电信业务。因此无线接入可分为固定无线接入和移动无线接入,采用的无线技术有微波、卫星等。无线接入的优点:初期投入小,能迅速提供业务,不需要铺设线路,因而可以省去大量的铺线费用和时间;比较灵活,可以按照需要随时进行变更、扩容;抗灾难性比较强。当然,无线用户环路也有许多缺点,如性能不如有线方式、质量不稳定、受环境影响大,目前还难以提供高宽带的接入等。

3.1.2 Internet 的接入方式

目前主要的 Internet 接入方式有电话线拨号接入、ISDN(综合业务数字网)、DDN(数字数据网)专线接入、ADSL(非对称数字用户环路)接入、基于光纤到楼的 LAN(以太网)接入、cable modem(线缆调制解调器,借助有线电视网)接入、PON(无源光纤网络)接入和 LMDS(区域多点传输服务)接入。

1. 电话线拨号接入

拨号入网费用较低,比较适于个人和业务量小的单位使用。用户所需的设备简单,只需在计算机前增加一台调制解调器和一根电话线,再到 ISP 申请一个上网账号即可使用。拨号上网的连接速率一般为 14.4~56 Kb/s,其网络结构如图 3-1 所示。

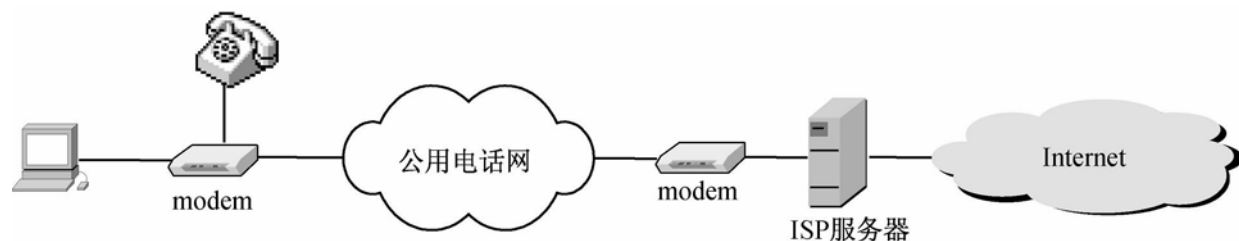


图 3-1 拨号上网网络结构

拨号接入 Internet 的一般步骤为:

- (1)向 ISP 申请入网用户名、密码、拨号入网的电话号码。
- (2)根据说明书安装与配置 modem,包括物理连接与软件设置。
- (3)在系统中建立 Internet 连接。
- (4)双击已建立的拨号连接图标,连接到 Internet。

2. ISDN 接入

ISDN(Integrated services digital network)将语音、数据、图像等业务综合在一个网内,吸收、综合现在的各种公用网的业务,并以数字的形式统一处理各种通信业务,通过一条线用各种通信媒介进行通信。ISDN 实际上也是通过拨号方式接入 Internet,但与普通的电话线有本质的区别,它提供 2B+D 服务,即两个 64 Kb/s 的 B 信道和一个 16 Kb/s 的 D 信道。用户可以用一个 B 信道打电话,同时用另一个 B 信道接入 Internet。如果不打电话,则两个 B 信道同时用于上网可达到 128 Kb/s 数据吞吐量。此外,如果用户的交换机、电话局和 ISP 都支持,还可以利用 D 信道(控制信号通道)的空闲免费(电话局和 ISP 都是按 B 信道收费的)带宽接入 Internet。

3. DDN 专线接入

DDN(digital data network)是随着数据通信业务的发展而迅速发展起来的一种新型网络。DDN 的主干网传输媒介有光纤、数字微波、卫星信道等,用户端多使用普通电缆和双绞线。DDN 将数字通信技术、计算机技术、光纤通信技术以及数字交叉连接技术有机地结合在一起,提供了高速度、高质量的通信环境,可以向用户提供点对点、点对多点透明传输的数据专线出租电路,为用户传输数据、图像、语音等信息。DDN 的通信速率为 $N \times 64 \text{ Kb/s}$ ($N=1 \sim 32$),可根据用户需要进行选择,当然速度越快租用费用也越高。

用户租用 DDN 业务需要申请开户。DDN 的收费一般可以采用包月制和计流量制,这与一般用户拨号上网的按时计费方式不同。DDN 的租用费较贵,普通个人用户负担不起,主要面向集团公司等需要综合运用的单位。DDN 按照不同的速率带宽收费也不同。例如,在中国电信申请一条 128 Kb/s 的区内 DDN 专线,月租费大约为 1 000 元。因此它不适合社区住户的接入,只对社区商业用户有吸引力。

4. ADSL 接入

ADSL(asymmetrical digital subscriber line)被欧美等发达国家誉为“现代信息高速公路上的快车”,因具有下行速率高、频带宽、性能优等特点而深受广大用户的喜爱,成为继 modem、ISDN 之后的一种全新的更快捷、更高效的接入方式。

ADSL 是一种非对称的 DSL 技术。所谓非对称是指用户线的上行速率与下行速率不同,上行速率低,下行速率高,特别适合传输多媒体信息业务,如视频点播(VOD)、多媒体信息检索和其他交互式业务。ADSL 在一对铜线上支持上行速率为 512 Kb/s $\sim$ 1 Mb/s,下行速率为 1 $\sim$ 8 Mb/s,有效传输距离为 3 $\sim$ 5 km。

现在比较成熟的 ADSL 标准有两种:G. DMT 和 G. Lite。G. DMT 是全速率的 ADSL 标准,支持 8 Mb/s 或 1.5 Mb/s 的高速下行或上行速率,但是它要求客户端安装 POTS 分离器,比较复杂且价格昂贵;G. Lite 标准速率较低,下行或上行速率为 1.5 Mb/s 或 512 Kb/s,省去了复杂的 POTS 分离器,成本较低且便于安装。就适用领域而言,G. DMT 比较适用于小型或家庭办公室,而 G. Lite 则更适用于普通家庭用户。

经 ADSL 调制解调器编码后的信号通过电话线传到电信局后,再通过 ADSL 交换机的信号识别/分离器,如果是语音信号就传到电话交换机上,如果是数字信号就接入 Internet。用户端接入 ADSL 的网络结构如图 3-2 所示。

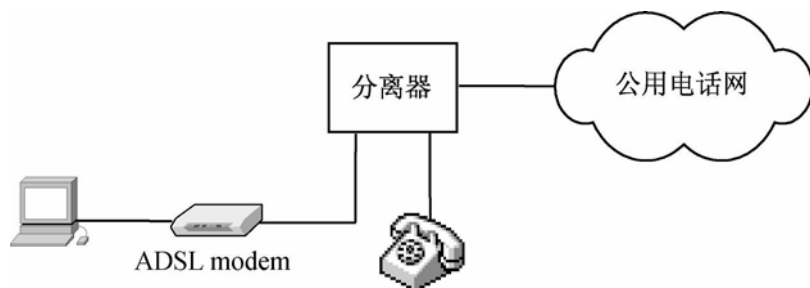


图 3-2 用户端接入 ADSL 的网络结构

当电话线两端连接 ADSL 调制解调器时,在这段电话线上便产生了 3 个信息通道:一个用于用户下载信息;一个用于 ADSL 控制信号的传输和上行的信息;还有一个是普通的电话服务通道,这 3 个通道可以同时工作。ADSL 可以满足各种语音、数据业务的需求,提供了非常高的传输速度,因此被称做“超级一线通”。

ADSL 是众多 DSL 技术中较为成熟的一种,其带宽较大,连接简单,投资较小,因此发展很快。目前国内大中城市的电信部门已先后推出了 ADSL 宽带接入服务。ADSL 方案的最大特点是不需要改造信号传输线路,可以完全利用普通铜质电话线作为传输媒介,配上专用的 modem 即可实现数据高速传输。国内采用的 ADSL 连接有两种方式:专线上网方式和虚拟拨号方式。专线方式采用包月计费,主要提供给单位用户使用;虚拟拨号方式采用按时间收费的方式,主要提供给家庭和个人用户使用。

5. LAN 接入

LAN 接入是利用以太网技术,采用光缆加双绞线的方式对社区进行综合布线。具体实施方案是:从社区机房敷设光缆至住户单元楼,楼内布线采用五类双绞线敷设至用户家里,双绞线总长度一般不超过 100 m,用户家里的计算机通过超五类跳线接入墙上的超五类模块就可以实现上网。社区机房的出口通过光缆或其他介质接入城域网。LAN 方式接入示意图如图 3-3 所示。

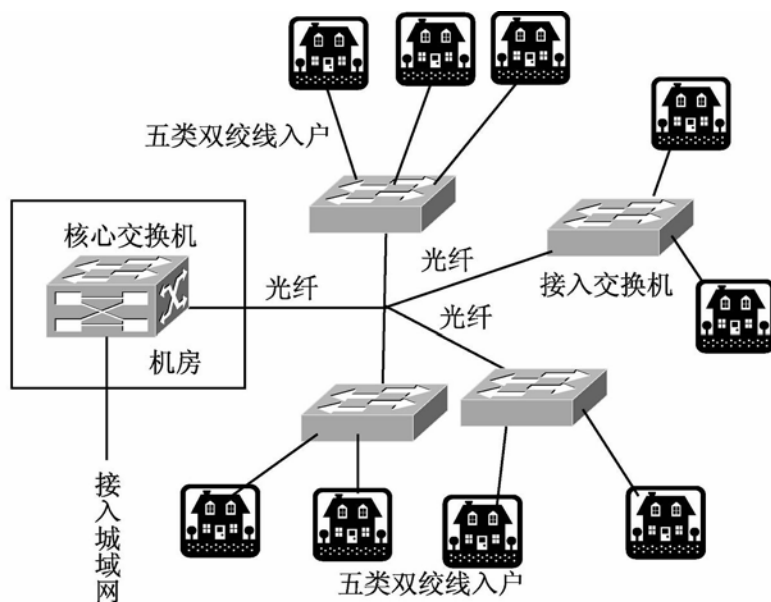


图 3-3 LAN 方式接入示意图

采用 LAN 方式接入可以充分利用园区网局域网的资源优势,为居民提供 10 Mb/s 以上的共享带宽,这比现在拨号上网速度快 180 多倍,并可根据用户的需求升级到 100 Mb/s

以上。以太网技术成熟、成本低、结构简单、稳定性和可扩充性好,便于网络升级,同时可实现实时监控、智能化物业管理、小区/大楼/家庭保安、家庭自动化(如远程遥控家电、可视门铃等)、远程抄表等,可提供智能化、信息化的办公与家居环境,满足不同层次的人们对信息化的需求。根据统计,目前社区主要采用以太网方式接入,主要是因为客户端除网卡外,不需要任何其他设备,局端以太网交换机相对其他交换机价格较低廉并且管理简单。

6. cable modem 接入

cable modem 是近几年开始使用的一种超高速 modem,它利用现成的有线电视(CATV)网进行数据传输,已是比较成熟的一种技术。随着有线电视网的发展壮大和人们生活质量的不断提高,cable modem 通过有线电视网访问 Internet 已成为越来越受业界关注的一种高速接入方式,如图 3-4 所示。

由于有线电视网采用的是模拟传输协议,因此网络需要用一个 modem 来协助完成数字数据的转化。cable modem 与以往的 modem 在原理上都是将数据进行调制后在 cable(电缆)的一个频率范围内传输,接收时进行解调,传输机制与普通 modem 相同;不同之处在于它是通过 CATV 的某个传输频带进行调制解调的。

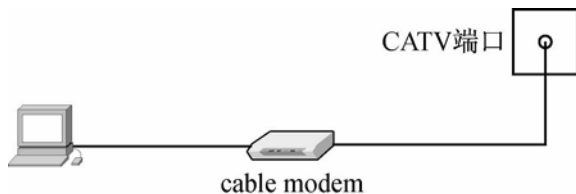


图 3-4 cable modem 接入示意图

cable modem 连接方式可分为两种:对称速率型和非对称速率型。前者的数据上传速率和数据下载速率相同,均为 $0.5 \sim 2 \text{ Mb/s}$;后者的数据上传速率为 $0.5 \sim 10 \text{ Mb/s}$,数据下载速率为 $2 \sim 40 \text{ Mb/s}$ 。

7. PON 接入

PON(passive optical network)是指光配线网络(optical distribution network,ODN)不含有任何电子器件及电子电源,ODN 全部由光分路器(splitter)等无源器件组成,不需要贵重的有源电子设备。PON 的突出优点是消除了户外的有源设备,所有的信号处理功能均在交换机和用户区设备中完成。而且这种接入方式的前期投资小,大部分资金要推迟到用户真正接入时才投入。它的传输距离比有源光纤接入系统的距离短,覆盖的范围较小,但它造价低,无须另设机房,维护容易。因此这种结构可以经济地为居家用户服务。

PON 的复杂性在于信号处理技术。在下行方向上,交换机发出的信号以广播式发给所有的用户。在上行方向上,各 ONU(optical network unit)必须采用某种多址接入协议(如时分多路访问 TDMA 协议)才能完成共享传输通道信息访问。

目前用于宽带接入的 PON 技术主要有 ATM PON 和 Ethernet PON。

8. LMDS 无线接入

LMDS(local multipoint distribution services)是近年来逐渐发展起来的、一种工作于 10 GHz 以上的频段、宽带无线点对多点接入技术,在某些国家(如加拿大、韩国)也称为本地多点通信系统 LMCS(local multipoint communication system)。

在不同国家或地区,电信管理部门分配给 LMDS 的具体工作频段及频带宽度有所不同,其中有 80% 左右的国家将 27.5~29.5 GHz 定为 LMDS 频段。

LMDS 工作在 24~38 GHz 频段,一般在毫米波的波段附近,可用频谱往往达到 1 GHz 以上。由于该技术利用高容量点对多点微波技术,通过毫米波进行传输,它几乎可以提供任何种类的业务,支持双向语音、数据及视频图像业务,能够实现从 64 Kb/s 到 2 Mb/s,甚至高达 155 Mb/s 的用户接入速率,具有很高的可靠性,被称为是一种“无线光纤”技术。图 3-5 是目前可用于社区宽带接入的一种。

在该接入方式中,一个基站可以覆盖直径 20 km 的区域,每个基站可以负载 2.4 万用户,每个终端用户的带宽可达到 25 Mb/s。但是,它的带宽总容量为 600 Mb/s,每个基站下的用户共享带宽,因此如果一个基站负载用户较多,那么每个用户所分到带宽就很小了。故这种技术对于社区用户的接入是不合适的,但它的用户端设备可以捆绑在一起,用于宽带运营商的城域网互连。其具体做法是:在会聚点机房建一个基站,而会聚点机房周边的社区机房可作为基站的用户端,社区机房如果捆绑 4 个用户端,会聚点机房与社区机房的带宽就可以达到 100 Mb/s。采用这种方案的好处是可以使已建好的宽带社区迅速开通运营,缩短建设周期。

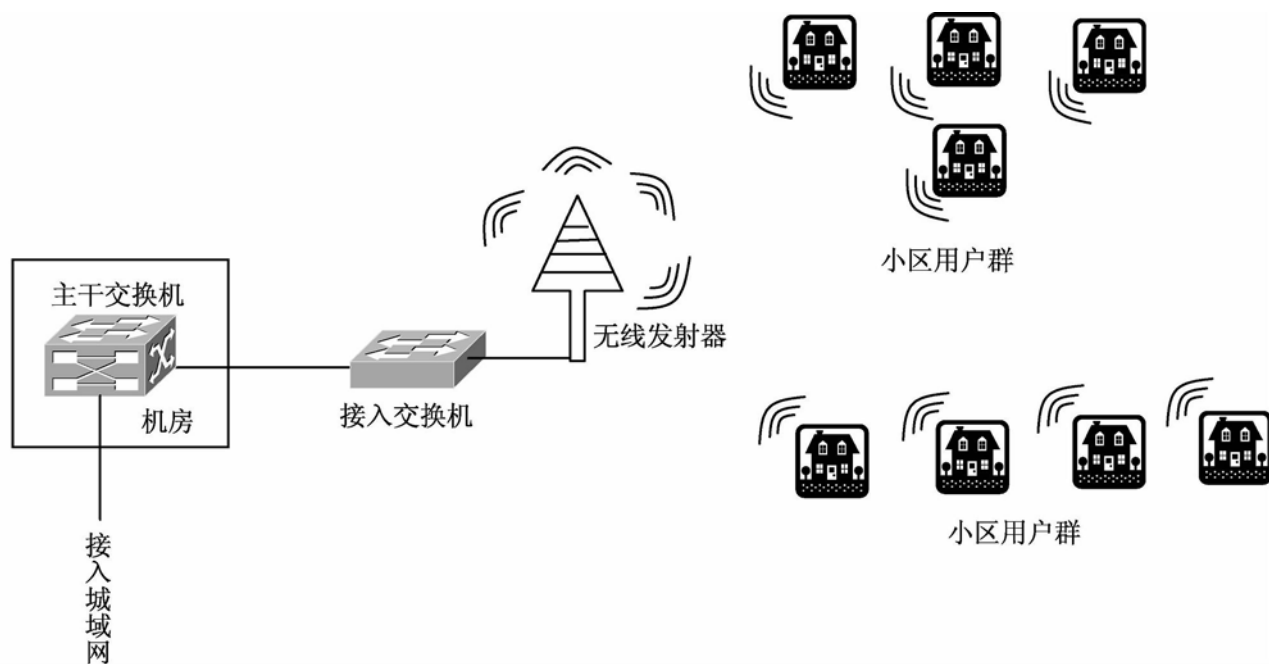


图 3-5 社区宽带接入示意图

3.2 局域网接入 Internet 的方式

在计算机网络组网中,有很多诸如机房、网吧、实验室、多媒体教室、小型办公机构之类的网络,它们具有两个共同的特点:一个 Internet 出口,常见的方式有异步 modem、ISDN、ADSL 拨号或以太网专线,这就要求所有计算机不得不共享 Internet 出口;ISP 分配的合法 IP 地址十分有限,一般只有与 Internet 直接相连的设备才有合法 IP 地址,并且大多数情况下是动态分配的,这意味着局域网内几乎所有设备不得不使用保留 IP 地址。这种小型的办公环境简称为 SOHO (small office and home office)。下面将讲解 SOHO 局域网中的计算机如何共享上网。

对于单台计算机来讲,增加一块调制解调器(拨号方式)或一块网卡(以太网方式),然后

进行简单配置就可以连入 Internet,实现起来非常简单。对于 SOHO 来讲,关键在于局域网中其他没有与 Internet 直接相连的计算机如何共享上网。无论是最简单的 Internet 连接共享,还是较为复杂的 ISA(Internet security and acceleration)、无线宽带路由器,根据原理的不同均可归纳为两种方式:代理(proxy)和网关(gateway)。无论哪种方式,都要求作为代理或网关的设备能够直接访问 Internet。而所谓的代理和网关,是相对其他没有与 Internet 直接相连的计算机而言的。

尽管 SOHO 局域网在外部连接和内部结构上种类繁多,但简化后的模型基本一致,图 3-6 是硬件网关方式访问 Internet 的模型结构,图 3-7 是代理或软件网关方式访问 Internet 的模型结构。代理和网关从原理上均可以利用软硬件实现。如果是拨号方式,如异步 modem、ISDN、ADSL,需要选择相应接口的路由设备和调制解调器;如果是以太网接入,需要换成以太网接口路由设备和以太网网卡。

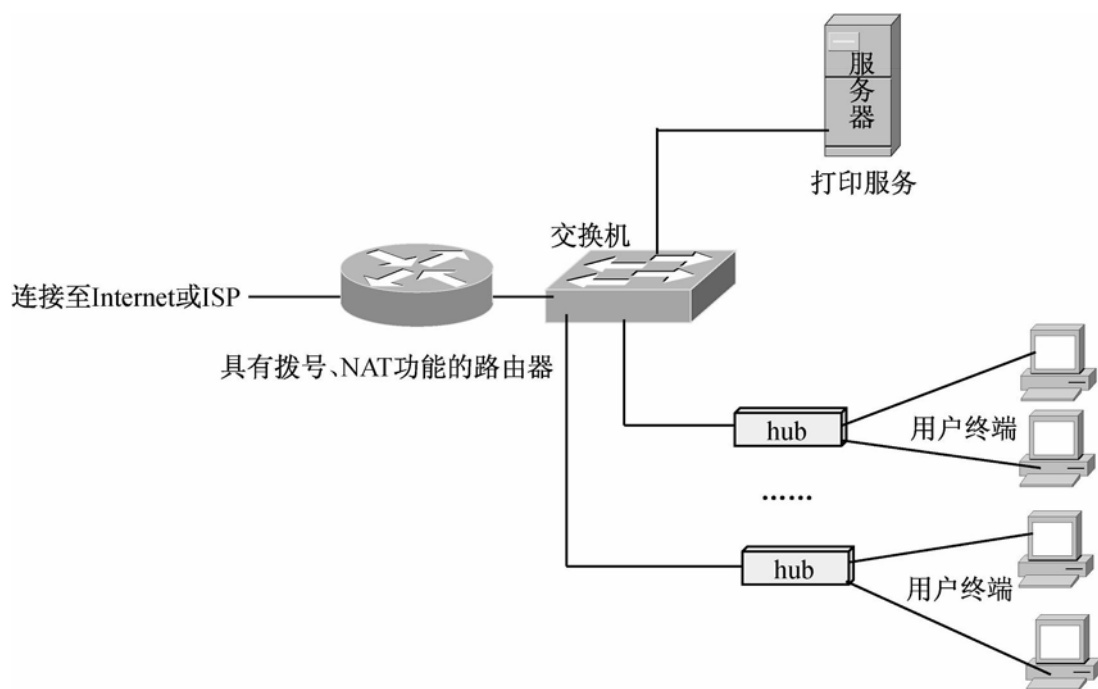


图 3-6 硬件网关方式

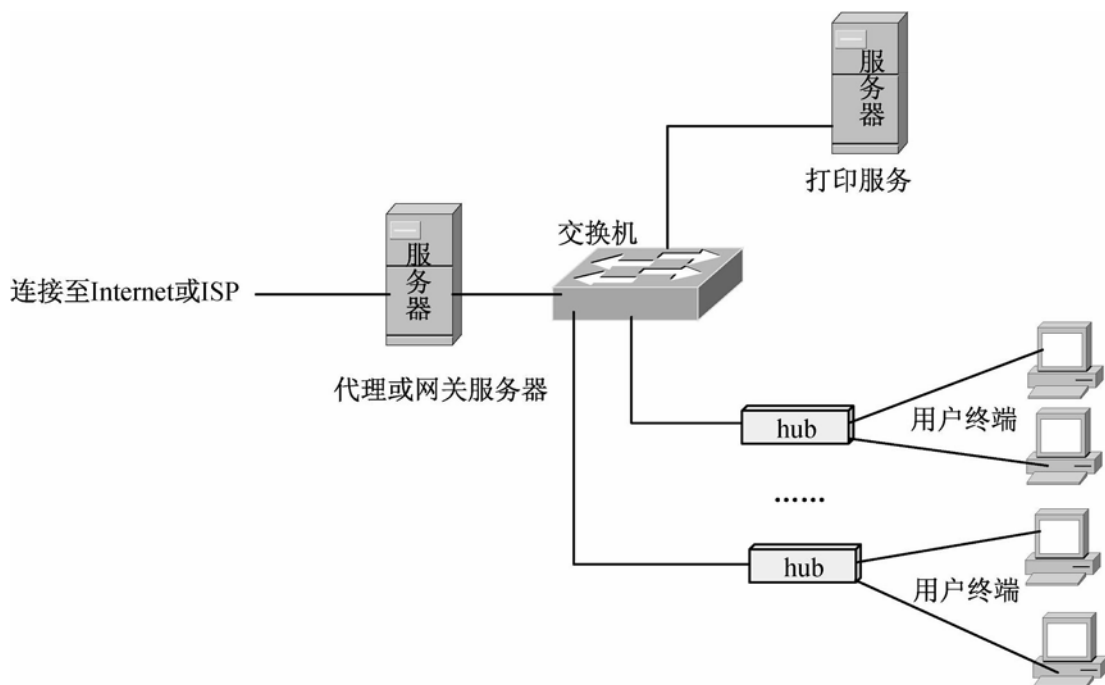


图 3-7 代理或软件网关方式

3.2.1 代理型接入 Internet

代理型接入 Internet 功能一般通过代理软件完成,如 WinGate、CCProxy、ISA 等。

1) 基本工作原理

代理服务器(proxy server)的功能就是代理网络用户去取得网络信息。它是网络信息的中转站。在一般情况下,使用网络浏览器直接去连接其他 Internet 站点取得网络信息时,须送出 request 信号来请求回答,然后对方再把信息以 bit 方式传送回来。代理服务器是介于浏览器和 Web 服务器之间的一台服务器。浏览器不是直接到 Web 服务器去取回信息,而是向代理服务器发出请求,request 信号会先送到代理服务器,由代理服务器来取回浏览器所需要的信息并传送给浏览器。而且,大部分代理服务器都具有缓冲的功能,就如同一个大的 cache(高速缓冲存储器),它有很大的存储空间,不断将新取得的数据存储到本机的内存上。如果浏览器所请求的数据在代理服务器的内存上已经存在而且是最新的,那么它就不重新从 Web 服务器取数据,而直接将内存上的数据传送给用户的浏览器,这样就能显著提高浏览效率。更重要的是,代理服务器是 Internet 链路级网关所提供的一种重要的安全功能,它工作在开放系统互连模型的应用层。

代理服务器的主要功能如下:

(1)设置用户验证和记账功能,可按用户进行记账,没有登记的用户无权通过代理服务器访问 Internet。此外,可对用户的访问时间、访问地点、信息流量进行统计。

(2)对用户进行分级管理,设置不同用户的访问权限。

(3)增加缓冲器,提高访问速度,对经常访问的地址创建缓冲区,大大提高热门站点的访问效率。通常代理服务器都设置一个较大的硬盘缓冲区(可能高达几吉字节或更大),当有外界信息通过时,同时也将其保存到缓冲区中,当其他用户再访问相同的信息时,则直接从缓冲区中取出信息,传给用户,以提高访问速度。

(4)连接 Internet,充当防火墙。因为所有内部网的用户通过代理服务器访问外界时,只映射为一个 IP 地址,所以外界不能直接访问到内部网;同时可以设置 IP 地址过滤,限制内部网对外部的访问权限。

(5)节省 IP 开销。采用代理服务器可以减少对 IP 地址的需求,对于使用局域网方式接入 Internet,如果为局域网内的每一个用户都申请一个 IP 地址,其费用可想而知。但使用代理服务器后,只需代理服务器上有一个合法的 IP 地址,局域网内的其他用户可以使用类似的私有 IP 地址,这样可以节约大量的 IP 地址,降低网络的维护成本。

2) SOCKS 5 透明代理

SOCKS 5 是一种透明的代理协议,能够很好地解决认证、保密以及代理接力等问题。Netscape、IE 等可以直接使用这种代理,还可以使用 SOCKS 5 的客户端软件使那些不直接支持 SOCKS 5 代理的 Internet 软件能够通过代理间接访问 Internet。

该协议所描述的是一种内部主机通过 SOCKS 5 代理来实现一些本来受限制的功能。具体过程如下:

用一台运行 SOCKS 5 的服务器连接内部网和 Internet,内部网主机使用的都是私有的 IP 地址,内部网主机请求访问 Internet 时,首先和 SOCKS 5 服务器建立一个 SOCKS 信道,然后再将请求通过这个信道发送给 SOCKS 服务器,SOCKS 服务器在收到客户请求后,向客户请求的 Internet 主机发出请求,得到响应后,SOCKS 服务器再通过原先建立的 SOCKS 信

道将数据返回给客户。当然在建立 SOCKS 信道的过程中可能有一个用户认证的过程。

SOCKS 和一般的应用层代理服务器是完全不同的。一般的应用层代理服务器工作在应用层,并且针对不同的网络应用提供不同的处理方法,如 HTTP、FTP、SMTP 等。这样,一旦有新的网络应用出现时,应用层代理服务器就不能提供对该应用的代理,因此应用层代理服务器的可扩展性并不好。与应用层代理服务器不同的是,SOCKS 代理服务器旨在提供一种广义的代理服务,它与具体的应用无关,不管出现什么新的应用都能提供代理服务,因为 SOCKS 代理工作在线路层(即应用层和传输层之间)。这和单纯工作在网络层或传输层的 IP 欺骗(或者叫做网络地址转换)又有所不同,因为 SOCKS 不能提供网络层网关服务,如 ICMP 包转发等。

3.2.2 网关型接入 Internet

网关的功能是通过具有路由功能的软硬件实体(简称路由模块)完成的。其工作原理是:当路由模块接收到数据包时,根据目的地址以及路由表来决定数据包的转发。通常该路由模块只有两个接口:一个 WAN 口,连接 Internet;一个 LAN 口,连接局域网集线器或交换机。

网关型接入 Internet 是通过网络地址转换(network address translation, NAT)功能来实现的。NAT 的实现原理就是:在内部专用网络中使用内部地址(不可路由),而当内部结点要与外界网络发生联系时,就在边缘路由器或者防火墙处,将内部地址替换成全局地址——合法地址(可路由),从而在外部公共网上正常使用。因此,NAT 实际上是配合内部地址使用,最终节省对全球合法地址使用的另一种技术。

NAT 的实现方式有 3 种,即静态转换(static NAT)、动态转换(dynamic NAT)和端口多路复用(overload)。

1. 静态转换

静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址,IP 地址对是一对一的,是固定的,即某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换,可以实现外部网络对内部网络中某些特定设备(如服务器)的访问。

静态地址转换的实现原理为:假设内部局域网使用的 IP 地址段为 192.168.0.1~192.168.0.254,路由器局域网端口(即默认网关)的 IP 地址为 192.168.0.1,子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 61.159.62.128~61.159.62.135,路由器在广域网中的 IP 地址为 61.159.62.129,子网掩码为 255.255.255.248,可用于转换的 IP 地址范围为 61.159.62.130~61.159.62.134。要求将内部网络地址 192.168.0.2~192.168.0.6 分别转换为合法 IP 地址 61.159.62.130~61.159.62.134。

第一步,设置外部端口。

```
interface serial 0
ip address 61.159.62.129 255.255.255.248
ip nat outside
```

第二步,设置内部端口。

```
interface ethernet 0
ip address 192.168.0.1 255.255.255.0
ip nat inside
```

第三步,在内部本地与内部合法地址之间建立静态地址转换。

```
ip nat inside source static(内部合法地址)
```

2. 动态转换

动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时,IP 地址对是随机的,所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说,只要指定哪些内部地址可以进行转换,以及用哪些合法地址作为外部地址时,就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时,可以采用动态转换的方式。

动态地址转换的实现原理为:假设内部网络使用的 IP 地址段为 172.16.100.1~172.16.100.254,路由器局域网端口(即默认网关)的 IP 地址为 172.16.100.1,子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 61.159.62.128~61.159.62.191,路由器在广域网中的 IP 地址为 61.159.62.129,子网掩码为 255.255.255.192,可用于转换的 IP 地址范围为 61.159.62.130~61.159.62.190。要求将内部网络地址 172.16.100.1~172.16.100.254 动态转换为合法 IP 地址 61.159.62.130~61.159.62.190。

第一步,设置外部端口。其命令的语法如下:

```
ip nat outside
```

第二步,设置内部端口。其命令的语法如下:

```
ip nat inside
```

第三步,定义合法 IP 地址池。其命令的语法如下:

```
ip nat pool 地址池名称 起始 IP 地址 终止 IP 地址 子网掩码
```

其中,地址池名称可以任意设定。

第四步,定义内部网络中允许访问 Internet 的访问列表。其命令的语法如下:

```
access-list 标号 permit 源地址 通配符
```

其中,标号为 1 至 99 之间的整数。

第五步,实现网络地址转换,在全局设置模式下,将由 access-list 指定的内部本地地址与指定的内部合法地址池进行地址转换。其命令的语法如下:

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名称
```

3. 端口多路复用

端口多路复用是指改变外部数据包的源端口并进行端口转换,即端口地址转换(port address translation,PAT),采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问,从而可以最大限度地节约 IP 地址资源。同时,又可隐藏网络内部的所有主机,有效避免来自 Internet 的攻击。因此,目前网络中应用最多的就是端口多路复用方式。

端口复用动态地址转换的原理为:假设内部网络使用的 IP 地址段为 10.100.100.1~10.100.100.254,路由器局域网端口(即默认网关)的 IP 地址为 10.100.100.1,子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 202.99.160.0~202.99.160.3,路由器广域网中的 IP 地址为 202.99.160.1,子网掩码为 255.255.255.252,可用于转换的 IP 地址为 202.99.160.2。要求将内部网址 10.100.100.1~10.100.100.254 转换为合法 IP 地址 202.99.160.2。

第一步,设置外部端口。

```
interface serial 0
ip address 202.99.160.1 255.255.255.252
in nat outside
```

第二步,设置内部端口。

```
interface ethernet 0
ip address 10.100.100.1 255.255.255.0
ip nat inside
```

第三步,定义合法 IP 地址池。

```
ip nat pool onlyone 202.99.160.2 202.99.160.2 netmask 255.255.255.252
```

指明地址缓冲池的名称为 onlyone,IP 地址范围为 202.99.160.2,子网掩码为 255.255.255.252。由于本例只有一个 IP 地址可用,起始 IP 地址与终止 IP 地址均为 202.99.160.2。如果有多个 IP 地址,则应当分别输入起止的 IP 地址。

第四步,定义内部访问列表。

```
access-list 1 permit 10.100.100.0 0.0.0.255
```

允许访问 Internet 的网段为 10.100.100.0~10.100.100.255,子网掩码为 255.255.255.0。



小提示

在这里子网掩码的顺序跟平常所写的顺序相反,即 0.0.0.255。

第五步,设置复用动态地址转换,在全局设置模式下,设置在内部的本地地址与内部合法 IP 地址间建立复用动态地址转换。其命令语法如下:

```
ip nat inside source list 访问列表号 pool 内部合法地址池名称 overload
```

例如:

```
ip nat inside source list 1 pool onlyone overload
```

以端口复用方式,将访问列表 1 中的私有 IP 地址转换为 onlyone IP 地址池中定义的合法 IP 地址。



请注意

内部 IP 与外部 IP 的区别为当主机 A 访问外网段的主机 B 时,主机 A 的 IP 称为内部 IP (inside address),主机 B 的 IP 称为外部 IP (outside address)。内外部 IP 是相对相互通信的主机而言的,与是否保留 IP 地址没有直接的关系。

3.2.3 代理与网关的比较

无论代理还是网关,有多少台 PC 上网,对外界来说,都只有一个 IP 地址,这个 IP 地址就是代理或网关设备的外接口 IP 地址。因此,如果一些站点限制来自同一 IP 地址的进程数量,将出现部分 PC 无法访问的问题。

代理和网关可以同时使用,假设采用网关方式时局域网中只有一台计算机可以访问国

外站点,这时就可以将该计算机设置成其他计算机的代理服务器。

代理可以部署在网络中的任何位置,对网络拓扑没有任何要求和影响;而网关通常部署在出口位置,对其软件功能和接口均有要求。

1. 原理上的区别

代理是通过软件实现的,是建立在应用层上的一种服务,它负责帮助客户完成相应的 Internet 请求;而网关是一台有硬件路由功能的网络设备或有软件路由功能的计算机,它工作在网络层,负责路由和转发数据包。

2. 配置上的区别

代理和网关在配置上都包含服务器和客户机两部分。

网关的配置非常简单,作为服务器,只需要设置好内外接口的 IP 地址(外接口 IP 地址动态获取时不需要设置)以及默认路由,然后启用 NAT 转换就可以了。客户端只需要将“默认网关”设成网关设备的内接口 IP 地址就可以了。

代理的配置相对复杂一点,软件不同,配置也略有差异,但思路是一样的,客户端必须明确告诉每一个 Internet 客户端软件,如 IE、Outlook 等如何找到代理服务器。例如,要上网浏览页面,就需要在浏览器中选择设置代理服务器的 IP 地址以及端口号,如图 3-8 所示。如果要使用 Outlook 这样的客户端软件,必须安装代理软件的客户端版本。



小提示

如果局域网共享上网采用代理方式,默认网关可有可无,也就是说,与默认网关无关。

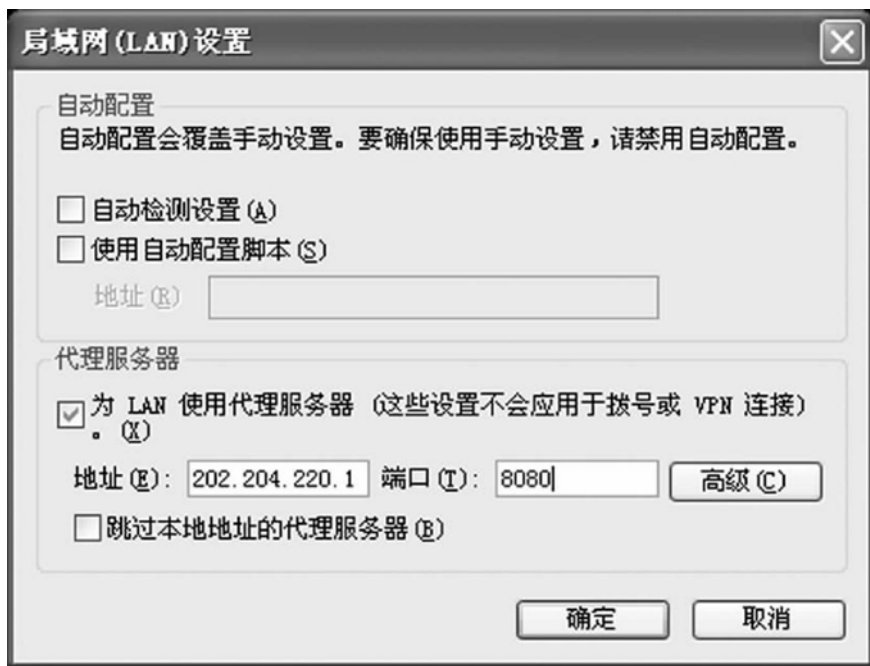


图 3-8 代理设置

3. 软硬件的区别

代理和网关方式的软件实现在网络结构上非常类似,有时使用的软件也相同,唯一的区别在软件的配置上。软件配置通常都需要一台服务器,都要求与内网计算机可以互访,当然还必须能够访问 Internet,并要求安装代理或网关软件。值得注意的是,软件网关是在代理

方式被广泛使用很久以后才出现的,而有时软件也恰好一样,因此,经常被混淆。

代理一般是通过软件方式来实现的;网关一般是通过硬件方式来实现的。网关方式的硬件实现设备很多,只需要一台具有合适接口的路由器就可以,对 SOHO 来说,还要求具有 NAT 功能。

4. 连机上的区别

作为网关的路由模块,原则上须有两个接口分别与内外网相连。而作为代理的服务器,首先保证有一个接口能够访问 Internet,如果内部 PC 通过该接口就可以访问代理服务器,则代理服务器只需要一个接口即可,否则,也至少需要两个接口。

5. 测试上的区别

如果没有安全控制,采用网关方式的内部 PC 可以和拥有合法 IP 的计算机一样 ping 通 Internet 上的主机,因此,测试起来非常简单,ping 通了就配置成功了。而采用代理方式却没有这么简单,内部 PC 只能 ping 通代理服务器,代理服务器之外的计算机是无法 ping 通的,因此,采用代理方式的测试流程一般为:先保证代理服务器能够访问 Internet,其次要求内部 PC 能够 ping 通代理服务器,最后通过安装和配置代理软件使得内部 PC 可以代理上网。

6. 速度上的区别

代理服务器在硬盘上设有 cache,用于缓存用户浏览的页面,在一定时间段内当有用户浏览相同页面时,将直接从 cache 中读取。网关没有 cache 功能,任何时候都是直接访问站点,当用户较多且经常访问同样的站点时,与代理相比,不仅速度慢,而且浪费大量的上网费用。但是,代理服务器只能提高静态页面浏览速度,对动态页面和文件不缓存,当有大量用户使用 FTP 下载文件时,代理服务器显得力不从心。而网关相对要好一些,这是由其工作原理决定的。

7. 控制上的区别

代理和网关的访问控制功能视软件而定,原理上都可以实现地址和协议端口的过滤等,但代理在限制上网时段、用户级管理以及流量监控统计方面显得更为方便一些,这也是代理得以继续使用的原因之一。

8. 安全上的区别

代理和网关方式均在一定程度上提高了 SOHO 局域网的安全等级,但两者存在一定的差异。对 Internet 来讲,代理后面的 PC 是完全透明的,而网关方式没有做到完全透明,只要知道了地址以及端口的映像关系,外网就可以访问内网。因此,代理的安全等级比网关要高。

9. 管理上的区别

网关方式不需要用户安装任何客户端软件,浏览器或 Internet 客户端软件也不需要做特殊设置,只需设好默认网关。而代理相对复杂得多,不仅浏览器需要设置,对于像 Outlook 这样的 Internet 客户端软件,还要安装和配置代理客户端,显然,如果局域网 PC 较多,则维护和培训的工作量会很大。

总之,所有的区别都来源于它们的本质——原理。对于代理来讲,在客户机上只能 ping 通到代理服务器,而 ping 不通外网;而网关方式,不考虑访问控制等其他因素,客户机原则上可以 ping 通任何外网 IP。将客户机的默认网关去掉,IE 中的连接代理加上,如果能访问外网网站,则说明是代理方式;将客户机的默认网关加上,IE 中的连接代理去掉,如果能访

问外网网站,则说明是网关方式。

3.2.4 常用代理软件介绍

目前,代理服务器是网络上的热点问题,尤其是在局域网接入 Internet 过程中,服务器采用共享代理软件,从而可以使客户机上网。而且几乎所有的浏览器、下载软件、信件收发软件都支持代理服务器。下面简要讲述代理服务器的强大功能——代理上网,即使连接代理服务器的其他计算机也能上网。

1. Internet 连接共享

Internet 连接共享(ICS)是 Windows 操作系统内置的服务程序,它让局域网内的多台 PC,通过其中一台已与 Internet 连接的 PC 来连接 Internet,从而达到多台 PC 共享一条 Internet 连接线路上网的目的,并提供防火墙的保护。要使用 ICS,有几点需要注意:

(1)启用 ICS 的计算机必须具有两个接口:一个连接到内部局域网,通常是网卡;一个连接到 Internet,通常是 modem 或 ISDN 接口。

(2)要配置 ICS,必须具有 Administrators 组权限。

(3)ICS 设置完成后,本地将使用动态的地址分配机制,因此不应该将此功能与其他 Windows 2000 Server DC、DNS 服务器、网关服务器、DHCP 服务器或配置为静态 IP 地址的系统一起使用。

(4)在启用 ICS 后,连接到家庭或小型办公室的适配器将获得新的 IP 地址配置。有两种情况:一种是使用系统建议的动态分配的方式,这时启用 ICS 的计算机就充当了一台 DHCP 服务器;另一种是手动设置的方式。

2. WinGate 代理上网

如图 3-9 所示为 WinGate 的服务器主界面。WinGate 是网络代理,通过代理,可以用虚拟的 IP 地址访问 Internet。IP 数据包到达代理服务器被重新打包,然后发出去,回来时,又按照发出的位置自动解包,送回用户机器,就好像用户机器真正连在 Internet 上一样。实际上和 Internet 进行数据交换的是代理服务器,用户所有 IP 包的收发都是通过代理服务器进行的。

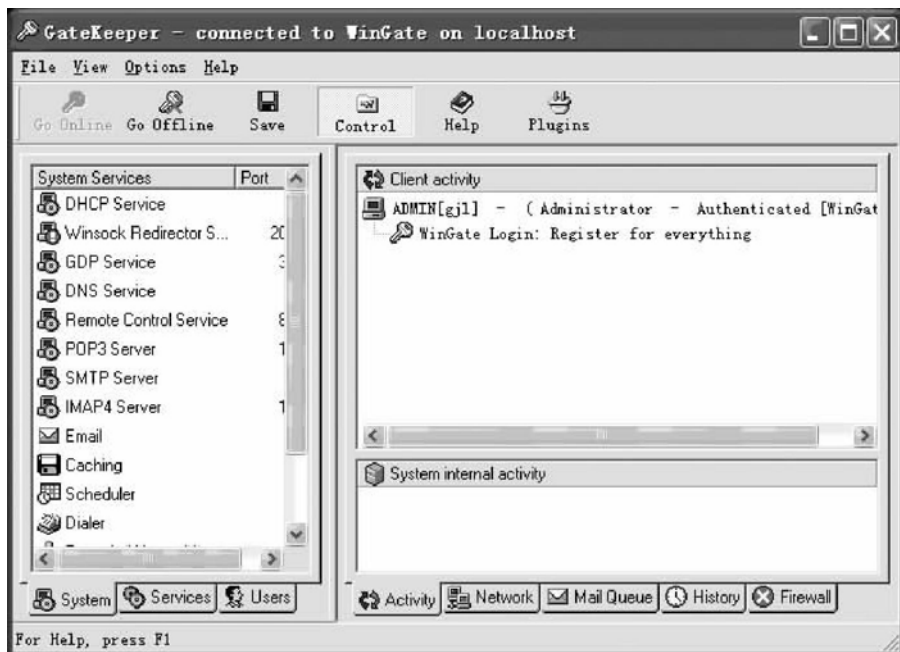


图 3-9 WinGate 的服务器主界面

WinGate 不但支持虚拟的 IP 地址,也支持真实 IP 地址,不过高级设置里可以指定为 Location,那样就可以假定一个用户,然后限制 IP 地址。

WinGate 可提供的代理有 WWW、TELNET、FTP、DNS、News、POP3 等;具有非常灵活、强大的用户管理和计费功能;还支持几乎所有的网络连接类型,如拨号、cable modem、卫星、xDSL、LAN 等。

3. Sygate

Sygate 是业界最为简单易用且功能强大的 Internet 共享软件,它用一条电话线、一个 modem、一个 Internet 账号,就能将整个局域网中的所有 PC 连至 Internet。与其他 Internet 共享软件不同,Sygate 是作为网关与 Internet 进行连接的,而不是作为代理服务器。如图 3-10、图 3-11 所示为 Sygate 服务器端界面和 Sygate 配置界面。Sygate 内置的防火墙、自动响应拨号、自动断线是其独具的三大风格特色。



图 3-10 Sygate 服务器端界面

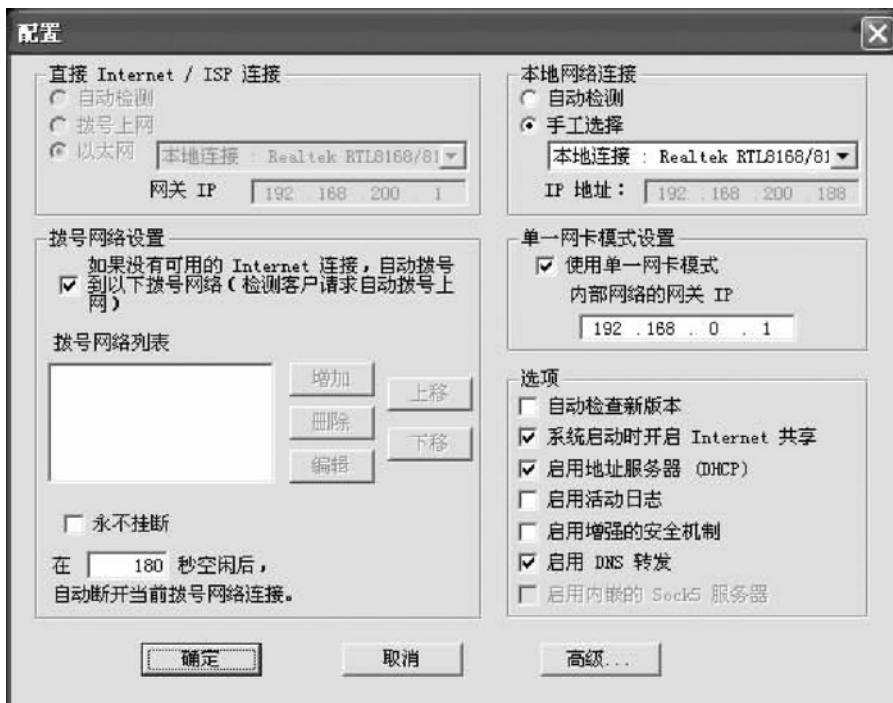


图 3-11 Sygate 配置界面

在线路连接方面, Sygate 可支持 Analog (普通电话拨号)、ISDN、ADSL 和 cable modem。在软件支持环境方面, 所用操作系统必须安装 TCP/IP。与其他 Internet 共享软件相比, Sygate 具有更强更多的优点: 设置简单、使用方便、升级随意、价格便宜。

4. CCProxy 代理上网

CCProxy 是一个非常流行的代理服务器软件。它设置简单、功能强大, 完全支持 Windows 系列操作系统, 支持共享 modem、ISDN、ADSL、DDN 等访问 Internet, 支持 HTTP、FTP、Gopher、SOCKS 4/5、News (NNTP)、RTSP、MMS 等代理协议, 支持浏览器通过 HTTP/Secure/FTP(Web)/Gopher 代理上网。图 3-12 是 CCProxy 的主界面。

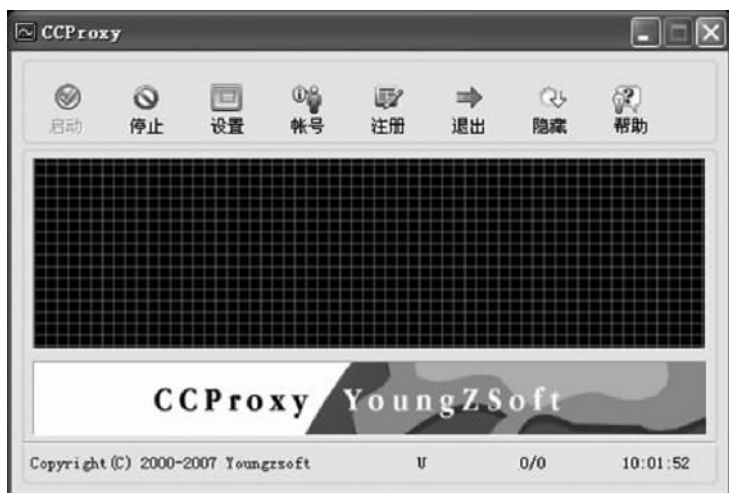


图 3-12 CCProxy 主界面

CCProxy 也支持客户端使用 Outlook、Foxmail 等通用邮件客户端软件收发邮件; 支持 QQ、MSN、联众游戏、股票软件等通过 SOCKS 5 代理上网; 支持 CuteFTP 等软件通过 FTP 代理上网; 支持 RealPlayer 通过 RTST 代理接收视频; 支持 MediaPlayer 通过 MMS 代理接收视频; 支持远程拨号、自动拨号、自动断线功能; 支持二级代理, 可以使代理服务器通过其他代理服务器上网。下面简单介绍下 CCProxy 的主要功能:

(1) 设置功能。在 CCProxy 的主界面上, 单击“设置”按钮就可以进入 CCProxy 的设置界面, 如图 3-13 所示。



图 3-13 CCProxy 设置界面

(2)账号功能。该功能可以针对不同用户定义不同的上网限制。账号管理支持 IP 地址段设置方式和自动扫描账号功能,建立账号更轻松。支持 3 种方式的账号认证方式:IP 地址/MAC 地址/用户名密码;HTTP 和 SOCKS 5 用户验证;内置域名解析功能 DNS。

(3)时间管理功能。该功能可以自由控制不同用户的上网时间。

3.2.5 硬件型接入 Internet

硬件型共享接入 Internet,一般是利用“路由”硬件设备来实现的,该类设备除具有共享上网的功能外,通常还具有 hub 的功能。它通过内置的硬件芯片来完成 Internet 和局域网之间的数据包交换管理,实际上也就是在芯片中固化了共享上网软件。因为硬件工作不依赖于操作系统,所以稳定性好,但是可更新性相对软件较差,并且需要购买;硬件共享上网涉及的设备和技术较复杂、专业,但是更灵活,它不需要后台程序,因此避免了对系统资源的占用。最重要的是,设备稳定性高,避免长时间开启服务器。此外,这类设备还能提供防火墙、FTP 等附加功能。硬件上网方式一般是企业级的用户选用的。下面以一个拥有 200 个信息点的企业为例进行讲解。

现有一公司,内部有 200 个信息点,这些信息点都分布在一栋大楼内。公司通过 ISP 提供的专线访问 Internet(ISP 提供了一个固定的 IP 地址)。现公司局域网内部的计算机想访问 Internet,采用硬件共享方式接入 Internet。本例采用的是一个 TP-LINK TL-R4149 宽带路由器,如图 3-14 所示。其接线方式为:路由器的 WAN 口接 ISP 提供的专线,其余的 4 个 LAN 口接交换机,交换机的各个端口接信息点。这样只要对路由器进行设置后,局域网内的计算机就可以实现连接 Internet 功能了。下面介绍的是路由器的具体的设置方法。



图 3-14 TP-LINK TL-R4149 宽带路由器

1) 设置计算机的 IP 地址

因为 TP-LINK TL-R4149 宽带路由器是在 Web 中进行设置的,要打开 Web 界面,必须先设置本机的 IP 地址。

执行“开始”→“设置”→“网络连接”命令,打开“网络连接状态”对话框,然后双击“本地连接”图标,弹出“本地连接”窗口。单击“属性”按钮,打开“本地连接 属性”对话框,如图 3-15 所示,在“此连接使用下列项目”列表框中选择“Internet 协议(TCP/IP)”选项,单击“属性”按钮,打开“Internet 协议(TCP/IP)属性”对话框。选中“使用下面的 IP 地址”单选按钮,进行如下设置(见图 3-16):

- IP 地址:192.168.1.2~192.168.1.254 可选(注意不要与原网络中的 IP 地址重复)。
- 子网掩码:255.255.255.0。
- 默认网关:192.168.1.1。



图 3-15 “本地连接 属性”对话框

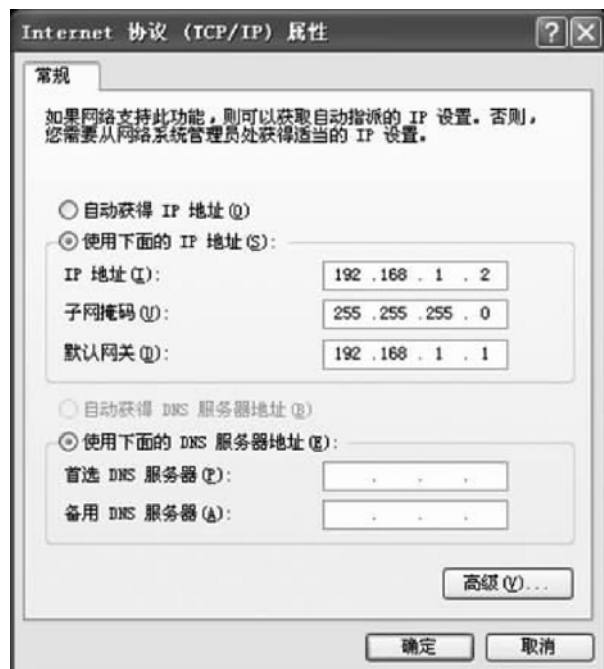


图 3-16 TCP/IP 设置

2) 路由器的设置

在使用路由器之前要进行一些设置工作,这样才可以正常使用路由器。无线路由器的设置工作可以通过“设置向导”来完成。

(1)在浏览器地址栏中输入无线路由器默认的 IP 地址 192.168.1.1,按 Enter 键,进入登录界面。

路由器 TL-R4149 登录界面需输入“用户名”和“密码”,第一次可输入出厂用户名和密码(都是 admin),单击“确定”按钮,即可进入路由器 Web 设置界面,如图 3-17 所示。



图 3-17 路由器设置主界面



路由器的默认 IP 地址可能不相同,可在路由器上的标识或说明书中找到。TP-LINK TL-R4149 宽带路由器的默认 IP 是 192.168.1.1,默认子网掩码为 255.255.255.0,这些值可以根据需要而改变,这里先按照默认值设置。

(2)进入路由器 TL-R4149 Web 设置界面后,单击左边的“设置向导”链接,在打开的“设置向导”中单击“下一步”按钮,选中“以太网宽带,网络服务商提供的固定 IP 地址(静态 IP)”单选按钮,如图 3-18 所示。

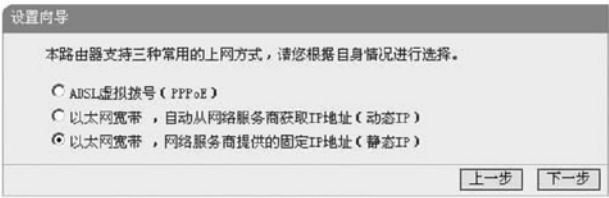


图 3-18 选择上网方式

(3)单击“下一步”按钮,输入“IP 地址”、“子网掩码”、“网关”、“DNS 服务器”和“备用 DNS 服务器”地址,如图 3-19 所示。单击“下一步”按钮。弹出“完成设置”窗口,单击“完成”按钮即可。

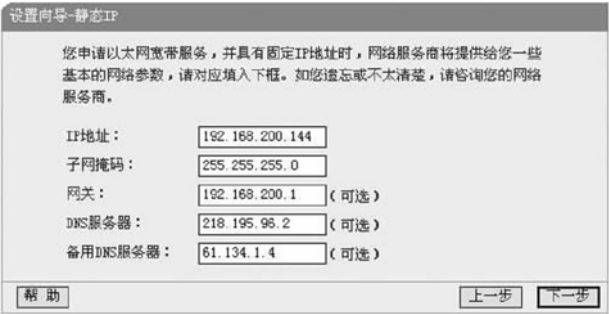


图 3-19 配置静态 IP

(4)弹出“连接状态”信息,如图 3-20 所示。通过这个窗口的信息,可以了解路由器的运行状况。

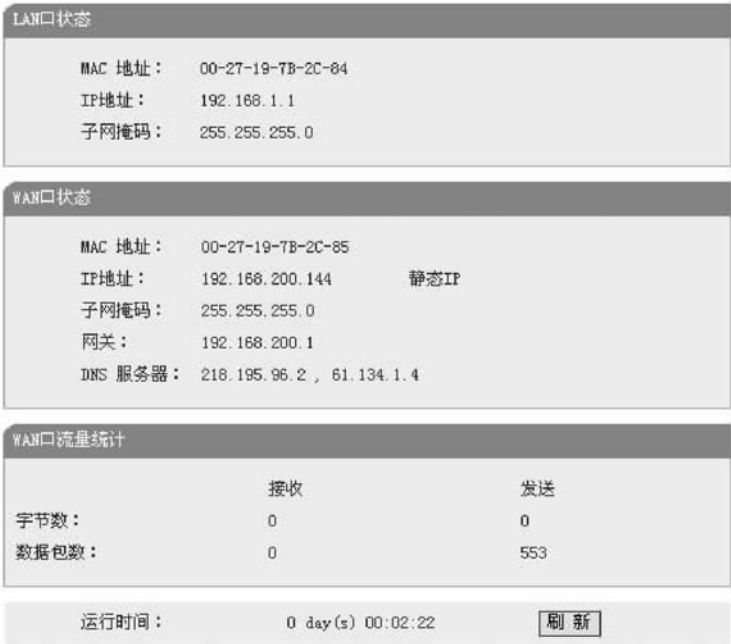


图 3-20 网络连接状态

(5) 路由器 TL-R4149 按照“设置向导”设置完成后,用户还可以根据网络要求进行相应的设置,这些设置包括网络参数、DHCP 服务器、转发规则、安全设置、路由功能、连接数限制以及 IP 与 MAC 绑定等功能。

在客户机上,只要把 IP 地址设置成 192.168.1. x (x 的范围是 2~254),子网掩码设置成 255.255.255.0,网关设置成 192.168.1.1,这样就可以连接 Internet 了。

3.3 远程桌面连接

远程桌面连接组件是从 Windows 2000 Server 开始由微软公司提供的,它在 Windows 2000 Server 中不是默认安装的。该组件一经推出就受到了很多用户的喜欢,所以在 Windows XP 和 Windows 2003 中微软公司对该组件的启用方法进行了改革,通过简单的勾选就可以完成在 Windows XP 和 Windows 2003 下远程桌面连接功能的开启。

1. 远程桌面的功能

若局域网中一台计算机连接到 Internet,同时开启了远程桌面连接功能,就可以在局域网中的另一台计算机上通过远程桌面功能实时地操作这台计算机,安装软件,运行程序,当然也可以畅游 Internet,就好像是直接在该计算机上操作一样。这就是远程桌面的最大功能,而且由于该功能是系统内置的,比其他第三方远程控制工具的使用更方便、更灵活。

2. 启动远程桌面连接的方法

在 Windows 2000 Server、Windows XP 和 Windows 2003 这三个操作系统中,开启远程桌面的方法各不相同,但是基本操作相似。下面以 Windows XP 为例来讲解远程桌面的连接过程。

远程桌面主要包括客户端和服务端。每台装有 Windows XP 的计算机都同时包括客户端和服务端,也就是说本机既可以当成客户端来连接其他装有 Windows XP 的计算机并控制它,也可以当成服务器端,让别的计算机来控制自己。

1) 开启远程桌面连接

Windows XP 安装完成后,就可以架设远程服务器。为了保证计算机内的资料安全,Windows XP 没有登录密码是不能进行远程桌面连接的。所以要开启远程桌面连接,Windows XP 的用户必须有用户名和密码。开启远程桌面连接的方法是在计算机桌面上右击“我的电脑”图标,选择“属性”命令,弹出“系统属性”对话框,如图 3-21 所示。

在该对话框中单击“远程”选项卡,如图 3-22 所示。在“远程桌面”设置中选中“允许用户远程连接到此计算机”复选框,远程服务器就设置好了。如果 Windows XP 系统有多个用户,还可以单击“选择远程用户”按钮进行远程访问用户的选择。



图 3-21 “系统属性”对话框



图 3-22 “远程”选项卡

2) 进行远程桌面连接

执行“开始”→“程序”→“附件”→“通讯”→“远程桌面连接”命令，弹出“远程桌面连接”窗口，如图 3-23 所示。在“计算机”下拉列表框中输入计算机名或 IP 地址，单击“连接”按钮，就可以进行远程连接了。连接成功后，输入要远程访问的计算机的用户名和密码，输入正确后就可以像操作本地计算机一样操作远程计算机了。



图 3-23 “远程桌面连接”窗口

在 Windows 2003 系统上的远程桌面实际上就是终端服务。虽然远程桌面最初在 Windows XP 上就已经存在,但由于 Windows XP 的远程桌面功能只能提供一个用户使用计算机,因此使用率并不高。而 Windows 2003 提供的远程桌面功能则可供多用户同时使用计算机,可以运行程序、保存文件和使用网络资源,在很多方面可以像使用终端一样,并且在管理和配置方面比原来的终端服务更方便。Windows 2003 的远程桌面的设置及连接与 Windows XP 基本相似,这里就不再赘述。

习 题 3

一、选择题

1. 拨号上网的连接速率一般为()。
A. 14.4~56 Kb/s B. 14.4~64 Kb/s C. 1~2 Mb/s D. 2~8 Mb/s
2. ISDN 中 B 信道和 D 信道的基本数据速率为()。
A. 16 Kb/s 和 64 Kb/s B. 64 Kb/s 和 16 Kb/s
C. 16 Kb/s 和 56 Kb/s D. 56 Kb/s 和 16 Kb/s
3. ADSL 是一种非对称的 DSL 技术,它的有效传输距离为()。
A. 1~2 km B. 2~4 km C. 3~5 km D. 5~8 km

二、填空题

1. 按传输媒介分,目前主要的接入技术有光纤接入_____、_____和_____。
2. 代理型接入 Internet 功能一般通过代理软件完成,如_____,_____,_____等。

三、问答题

1. 简述代理服务器的基本工作原理。
2. 简要说明如何使用 WinGate 代理上网。