

上
篇

网络工程部分

项目一

局域网的组建



项目综述

通过对身边所接触网络的了解、观察和调研,掌握局域网的构成、分类、特点,明确网络的重要性和作用;熟悉网络的拓扑结构,掌握局域网相关的基础知识及概念,如协议、IP 地址、常用网络设备、网络配置等;熟练掌握组网工具和仪器的使用。重点在于小型局域网、交换式局域网、虚拟局域网的组建和配置,难点在于交换式局域网及虚拟局域网的设备选型、网络规划设计、系统配置等方面。建议多观察实际的网络系统,多利用网络资源查询相关内容和信息。要尽可能多地进行实操训练和组网练习。表 1-1 为局域网的组建项目综述。

表 1-1 局域网的组建项目综述表

教学内容	任务一 认识局域网 任务二 组建小型局域网 任务三 组建交换式局域网 任务四 组建虚拟局域网	参考学时	8
知识目标	了解局域网的构成和常用设备,掌握局域网的组网方法和步骤		
技能目标	1. 网络设备的认识; 2. 交换式和虚拟局域网的组建技能; 3. 组网工具的使用		
教学重点	局域网的组建方法和步骤		
教学难点	虚拟局域网的组建和交换机的配置		
教学载体与资源	教材、PPT、实训室、规范、图集		
教学方法建议	引导演示,师生共同参与来完成项目		
教学过程	1. 下达任务和要求; 2. 教师带领学生共同分析任务; 3. 分组讨论后完成任务		
考核评价	1. 小组内互相评价; 2. 教师根据任务完成情况和过程进行综合打分评价		



项目准备

(1)完成本项目所需的项目资源清单如表 1-2 所示,按每小组配发。

表 1-2 项目一资源清单表

序号	名称	规格/型号	数量
1	计算机	硬盘空间 200 MB 以上	1 台
2	操作系统	Windows 2000/XP,SP2 以上	1 套
3	Visio 软件	2003 或 2007 版本	1 套
4	Packet Tracer 软件	5.0、6.0 版本	1 套
5	压线钳、双绞线等组网辅料	国产品牌	若干
6	soho 交换机	思科(Cisco)SF90-24	1 台
7	路由器 1	TP-LINK TL-WR941N	1 台
8	交换机 1	思科(Cisco)SF500-24 24 口百兆可堆叠全网管交换机	1 台
9	交换机 2	思科(Cisco)2960	1 台
10	交换机 3	思科(Cisco)SF90-24 24 口非网管型交换机	1 台
11	无线 AP	思科(Cisco)WAP121-E-K9-CN 百兆无线接入点	1 台
12	路由器 2	思科(Cisco)RV110W Wireless-N VPN 防火墙路由器	1 台
13	路由器 3	思科(Cisco)RV042 4 口 VPN 路由器	1 台

(2)预习要点。

- ①集线器的详细说明。
- ②家庭上网的实现调查。
- ③路由器的端口认识。
- ④交换机的端口认识。
- ⑤Visio 软件的使用方法。
- ⑥Packet Tracer 5.0 软件的使用方法。
- ⑦组网工具的用途。
- ⑧测试仪器的性能。

任务一 认识局域网



任务分析及任务目标

通过局域网的组成来认识和掌握局域网常用设备、结构、功能和应用范围。学会用自己的表述方法来描述局域网的组成、特点、拓扑结构和功能。

相关知识链接

一、局域网的概念

局域网(local area network)是在一个局部的地理范围(如一个学校、工厂和机关)内,将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网,简称 LAN。局域网结构示意图如图 1-1 所示。它可以通过数据通信网或专用数据电路与远方的局域网、数据库或处理中心连接,构成一个大范围的信息处理系统。局域网的功能如下。

- (1)资源共享,包括设备共享、访问文件系统和数据库。
- (2)通信,通过网络可以收发邮件、实时通话、传递信息。
- (3)分布式处理,将复杂问题分布到网络中的各台计算机上进行处理。

因此,企业或学校组建局域网可以提高工作效率,为办公人员提供一个很好的自动化办公平台。

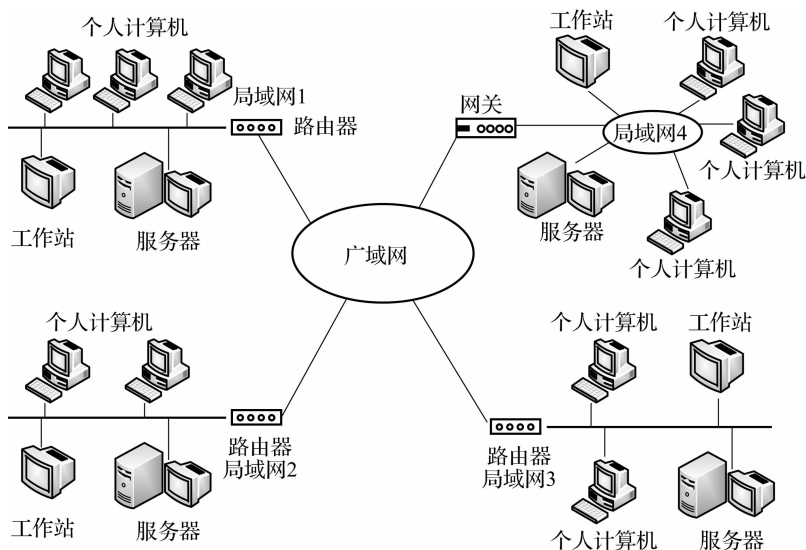


图 1-1 局域网结构示意图

二、局域网的组成

(一) 网络服务器

网络服务器可以分为文件服务器、打印服务器、应用系统服务器和通信服务器等。

1. 文件服务器

在计算机局域网中,以文件数据共享为目标,需要将供多台计算机共享的文件存放于一台计算机中,这台计算机就称为文件服务器,这是一台特殊功能的计算机,其主要目的是向客户机提供文件服务。文件服务器可以是一台能够运行其他应用程序的通用计算机,也可以是一台提供文件服务的专用计算机。



2. 打印服务器

打印服务器提供简单而高效的网络打印解决方案。如图 1-2 所示,通过交换机进行网络连接,打印机在网络中的任何位置都能够很容易地为局域网内所有用户提供打印服务。

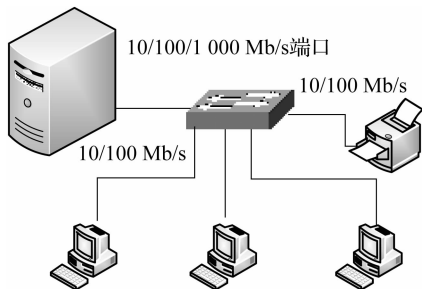


图 1-2 打印服务器

3. 应用系统服务器

应用系统服务器运行客户机/服务器应用程序的服务器端软件,该服务器一般保存着大量信息供用户查询。在执行客户端程序的查询请求后,将查询结果返回客户端。

4. 通信服务器

通信服务器负责处理本网络与其他网络的通信,以及远程用户与本网络的通信。通信服务器根据软件和硬件能力为一个或同时为多个用户提供通信信道。

(二) 客户机

客户机主要运行客户机/服务器应用程序的客户端软件,网络上的每位用户通过客户机与网络联系。由于网络中的客户机能够共享服务器的资源,因此一般情况下其配置比服务器要低一些。从网络架构来看,任何一台计算机都可以作为客户机。

(三) 网络设备

网络设备分为网络接入设备、连接设备、互连设备,如网卡、集线器、交换机、网桥、路由器和网关等。网卡安装在计算机上,如图 1-3 所示,是局域网中连接计算机和传输介质的接口。它不仅能实现与局域网传输介质之间的物理连接和电信号匹配,还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存功能等。



图 1-3 网卡

较为常见的设备还有交换机和路由器,很多人对此都比较熟悉,但对它们的作用、特点和异同并不是特别了解,下面进行简单介绍。

交换机 (switch) 是一种用于电信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。交换机可分为第二层交换机和第三层交换机。第二层交换机同时具备了集线器和网桥的功能。第三层交换机功能更为强大,还具有路径选择功能。

说到电信号交换的历史,应当追溯到电话出现的初期。当电话被发明后,只需要一根足

够长的导线,加上末端的两台电话,就可以使相距很远的两个人实现语音交谈。电话增多后,要使每个拥有电话的人都能相互通信,又不可能在每两台电话机之间都拉上一根线,于是人们设立了电话局,每个电话用户都接一根线到电话局的一个大电路板上。当 A 希望与 B 通话时,就请求电话局的接线员接通 B 的电话。接线员用一根导线,一头插在 A 接到电路板上的孔,另一头插到 B 接到电路板上的孔,这就是接续,相当于临时给 A 和 B 拉了一条电话线,这时双方就可以通话了。当通话完毕后,接线员将电线拆下,这就是拆线。整个过程就是人工交换,它实际上就是一个合上开关和断开开关的过程。因此,把交换译为开关,从技术上讲更容易让人理解。

后来,人们发现可以利用电子技术代替人工交换。电话终端用户只要向电子设备发送一串电信号,电子设备就可以根据预先设定的程序,将请求方和被请求方的电路接通,并且独占此电路,不会与第三方共享,这种交换方式被称为程控交换,而这种设备也就是程控交换机,如图 1-4 所示。



图 1-4 程控交换机

从广义上来看,网络交换机分为两种:广域网交换机和局域网交换机。广域网交换机主要应用于电信领域,提供通信的基础平台。而局域网交换机则应用于局域网络,用于连接终端设备,如 PC 及网络打印机等。从传输介质和传输速度上可分为以太网交换机、快速以太网交换机、千兆以太网交换机、FDDI 交换机、ATM 交换机和令牌环交换机等。从规模应用上又可分为企业级交换机、部门级交换机和工作组交换机等。交换机就是一种在通信系统中完成信息交换功能的设备,它应用在数据链路层。交换机有多个端口,每个端口都具有桥接功能,可以连接一个局域网、一台高性能服务器或工作站。实际上,交换机有时被称为多端口网桥。那么交换机与 HUB 集线器有什么区别吗?集线器就是一种物理层共享设备,HUB 本身不能识别 MAC 地址和 IP 地址,当同一局域网内的 A 主机给 B 主机传输数据时,数据包在以 HUB 为架构的网络上是以广播方式传输的,由每一台终端通过验证数据包的 MAC 地址来确定是否接收。也就是说,在这种工作模式下,同一时刻网络上只能传输一组数据帧的通信,如果发生碰撞,则必须重试。这种方式就是共享网络带宽。交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的物理网段(非 IP 网段),连接在其上的网络设备独自享有全部带宽,无须同其他设备竞争使用。当节点 A 向节点 D 发送数据时,节点 B 可同时向节点 C 发送数据,而且这两个传输都享有网络的全部带宽,都有自己的虚拟连接。假使这里使用的是 10 Mb/s 的以太网交换机,那么该交换机此时的总流量就等于 $2 \times 10 \text{ Mb/s} = 20 \text{ Mb/s}$,而使用 10 Mb/s 的共享式 HUB 时,一个 HUB 的总流量也不会超出 10 Mb/s。总之,交换机是一种基于 MAC 地址识别,能完成封装转发数据帧功能的网络设备。交换机可以“学习”MAC 地址,并将其存放在内部地址表中,通过在数据帧的始发者和目标接收者之间建立临时的交换路径,使数据帧直接由源地址到达目的地址。

路由器(router)是连接因特网中各局域网、广域网的设备,它会根据信道的情况自动选择和设定路由,以最佳路径、按前后顺序发送信号。路由器是互联网络的枢纽。

路由和交换之间的主要区别是,交换发生在 OSI 参考模型的第二层(数据链路层),而路由发生在第三层,即网络层。这一区别决定了路由和交换在移动信息的过程中需使用不同的控制信息,所以两者实现各自功能的方式是不同的。



路由器系统构成了基于 TCP/IP 的 Internet 的主体脉络,也可以说,路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一,它的可靠性则直接影响着网络互联的质量。

网关又叫协议转换器,它的作用是使网络中采用不同高层协议的主机能够相互通信,进而完成分布式应用。网关是传输设备中最复杂的一个,主要用于连接不同体系结构的网络或局域网与主机的连接。

有了硬件,还应该有软件,那就是网络操作系统。它主要由网卡驱动程序、网络协议软件 and 应用程序接口三部分组成。常见的有 Windows NT、UNIX、Netware 和 Linux 四种。

任务实施

(1)参观学校的局域网和机房,了解局域网的硬件组成,一定要对局域网的硬件和线缆有一个全面的认识,让学生画出局域网结构的简图。

(2)查找网络设备的资料,自己列表分析集线器、交换机、路由器的区别。能够正确识别网卡、集线器、交换机、路由器和各类线缆。

(3)做两根网线,直通线和交叉线各一根。掌握 T568A、T568B 的线序标准。学会压线钳、网络测试仪的使用方法。

具体步骤:剪线—剥线—排线—插线—压线—测试网线。

(4)用 Viso 软件绘制局域网结构图。

任务二 组建小型局域网

任务分析及任务目标

学习组建家庭和办公室无线局域网来实现资源共享。通过家庭和办公室组网的实践来熟悉最基本的网络设备和结构,掌握构建局域网的技能、方法,能够根据上网类型确定组网方案,并能绘制简单的网络拓扑图及线路图。

相关知识链接

目前,在人们的家庭和办公室中会有多台设备需要进行网络连接,组成一个小型局域网,通过将家庭、办公室中的所有计算机连接起来,使得所有的资源在局域网内部实现共享,便捷地互相传输数据资料、音视频等文件,能共享网络内光驱;还能共享打印机、扫描仪等。小型局域网除了传统的有线连接外,无线组网成为了很多情况下的首选,因此先了解此方面的相关知识。

无线 AP(access point),即无线接入点,是用于无线网络的无线交换机,也是无线网络的核心。无线 AP 是移动计算机用户进入有线网络的接入点,主要用于宽带家庭、大楼内部及园区内部,覆盖范围为几十米至上百米,目前的主要技术为 802.11 系列。大多数无线 AP 还带有接入点客户端模式(AP client),可以和其他 AP 进行无线连接,延展网络的覆盖范围。无线 AP 是一个包含很广的名称,它不仅包含单纯性无线接入点,也同样是无线路由器(含无线网关、无线网桥)等类设备的统称。在本任务中指的是无线路由器。无线路由器是家庭组建网络的利器,是单纯性无线 AP 和宽带路由器合二为一的扩展型产品,除了具备单

纯性无线 AP 的所有功能外,还支持 DHCP 客户端、VPN、防火墙、WEP 加密等,除了支持局域网用户的网络连接共享外,还可以实现无线网络中的 Internet 连接共享、宽带接入。在使用中可自动连接网络,操作方便,其原因在于内置了虚拟拨号软件,存储用户名和密码实现拨号上网。例如,ADSL 接入时需要拨号,而无线路由器就可以实现这个功能,无须手动拨号或使用服务器。

那么无线路由器和无线 AP 有什么不同?简单地讲,无线 AP 不能直接与 ADSL Modem 相连,必须加一台交换机或集线器。而无线路由器因具备拨号功能,所以可以直接连接 ADSL Modem。可以说,无线路由器就是无线 AP、路由功能和交换机的集合体,支持有线和无线组成同一子网,直接接上 Modem。无线 AP 相当于一个无线交换机,接在有线交换机或路由器上,为跟它连接的无线网卡从路由器那里分得 IP。常见的两种家庭组网方式如图 1-5 及图 1-6 所示。

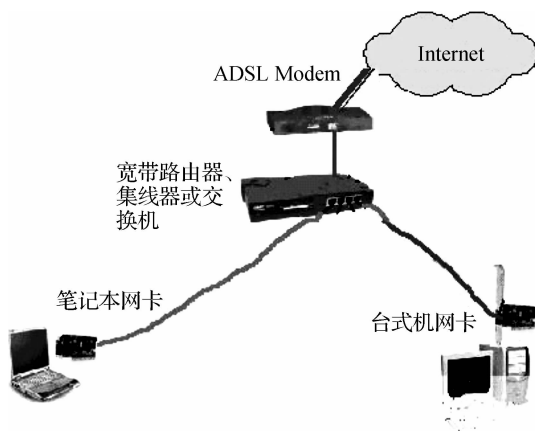


图 1-5 组网方式一

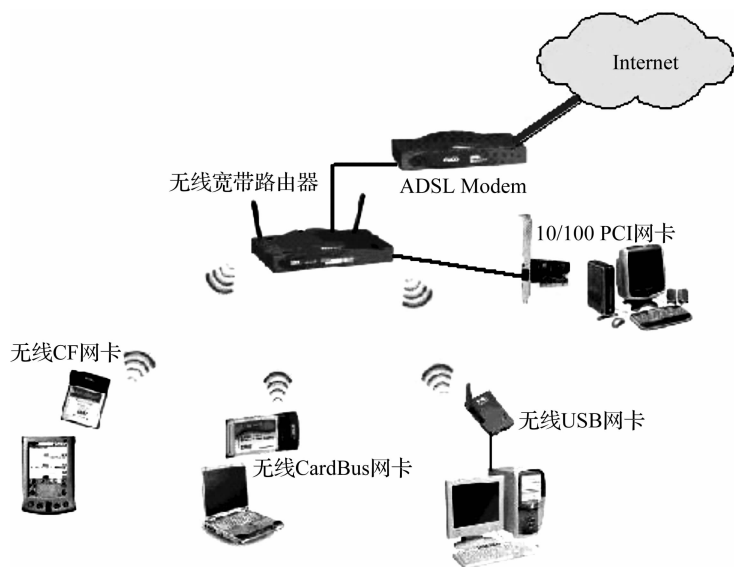


图 1-6 组网方式二



任务实施

现在需要为办公室组建一个小型局域网,此办公室有 4 台台式计算机和其他电子设备(如笔记本、手机、平板电脑等)。要求各设备之间可以相互通信,又可以与外网连接。应具有无线和有线网络两种功能。

一、硬件选择和连接

对于这种小型办公网络而言,集无线 AP、路由器、4 口交换机、防火墙功能于一身的无线路由器无疑是最好选择。当然要考虑具体的性能参数和接口类型、数量等问题。

这里选择 TP-LINK 的 TL-WR941N 路由器,前面板设置有电源、SYS、WLAN、LAN、WAN 指示灯,便于查看工作状态。背面设置了复位键、电源接口、WAN 口以及 4 个 LAN 口,同时还配备能够任意调整方向的三根全向天线,方便用户在不同环境下使用。



图 1-7 TP-LINK TL-WR941N 路由器

TP-LINK 的 TL-WR941N 路由器如图 1-7 所示。

这款无线路由器基于 802.11n(Draft 2.0)标准,无线传输速率最高能达到 300 Mb/s,具有性能稳定、无线覆盖范围广的优点,其性能参数如表 1-3 所示。

表 1-3 TP-LINK TL-WR941N 路由器性能参数表

性能指标	具体性能
网络标准	无线标准:IEEE 802.11n、IEEE 802.11g、IEEE 802.11b; 有线标准:IEEE 802.3、IEEE 802.3u
网络协议	CSMA/CA、CSMA/CD、TCP/IP、DHCP、ICMP、NAT、PPPoE
最高传输速率	300 Mb/s 纠错
频率范围	单频(2.4~2.483 5 GHz)
信道数	1~13
调制方式	DBPSK、DQPSK、CCK、OFDM、16-QAM、64-QAM
网络接口	1 个 10/100 Mb/s WAN 口,4 个 10/100 Mb/s LAN 口

用直通线将四台台式计算机与无线路由器的局域网端口(LAN)连接,再将进入办公室的网线接到无线宽带路由器的 WAN 口上(如果是家庭,那么用直通线把 ADSL Modem 连接到无线宽带路由器的 WAN 口上)。

若需台式机也能无线上网,则需安装无线网卡,而目前有 USB 型无线网卡,安装起来非常方便,在此不进行讲解和操作。

二、软件配置与设置

以 TP-LINK 的 TL-WR941N 为例,进行 Web 配置操作演示。

将设备 LAN 口与计算机相连,在浏览器地址栏中输入 192.168.1.1 并按 Enter 键,在打开的页面中通过输入用户名 admin、密码 admin 便可登录其 Web 配置界面,对用户所需要的路由器配置进行输入调整。界面看起来也很简单、友好,易于操作。

通过 TL-WR941N 自身提供的设置向导,用户就能对路由器进行必要设定,更加方便、快捷地搭建无线网络,如图 1-8 所示。



图 1-8 路由器设置向导

对于初级用户来说,先选择上网方式,然后等待路由器自动检测网络环境,如图 1-9 所示。

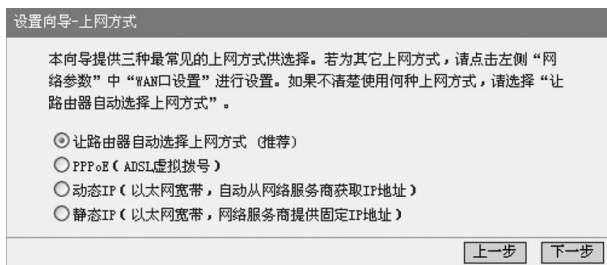


图 1-9 上网方式选择

在无线设置界面中,可根据实际需求,设定无线状态和加密,对于初级用户来说,其他选择默认,只在“无线安全”选项中,选择 WPA-PSK/WPA2-PSK 加密方式,填入密码。之后会看到设置完成的提示,重启路由器即可。接下来,会有重新启动的进度条显示,完成后,就会看到设定好的最终界面了,综合信息如图 1-10 所示。

版本信息		
当前软件版本:	3.10.2_Bui1d_091209_Ra1_51228n	
当前硬件版本:	WR941N v4 00000000	
LAN口状态		
MAC 地址:	00-25-06-27-25-B8	
IP地址:	192.168.1.1	
子网掩码:	255.255.255.0	
无线状态		
无线功能:	启用	
SSID号:	TP-LINK_2725B8	
信道:	自动(当前信道 7)	
模式:	11bgn mixed	
频道带宽:	自动	
最大发送速率:	300Mbps	
MAC 地址:	00-25-06-27-25-B8	
WAN口状态		
MAC 地址:	00-25-06-27-25-B8	
IP地址:	172.31.70.88 静态IP	
子网掩码:	255.255.255.0	
网关:	172.31.70.1	
DNS 服务器:	0.0.0.0, 0.0.0.0	
WAN口流量统计		
	接收	发送
字节数:	0	0
数据包数:	0	0

图 1-10 综合信息显示



图 1-10 显示的综合信息如下。

版本信息:此处显示路由器当前的软硬件版本号。

LAN 口状态:此处显示路由器当前 LAN 口的 MAC 地址、IP 地址和子网掩码。

无线状态:此处显示路由器当前的无线设置状态,包括 SSID 号、频道和频段带宽信息。

WAN 口状态:此处显示路由器当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器地址。

WAN 口流量统计:此处显示当前 WAN 口接收和发送的数据流量信息。

以上为快速设置,是针对初级用户的。还有一些高级配置,如 QSS(即 WPS)安全设置界面,可对该功能进行调节配置,如图 1-11 所示。

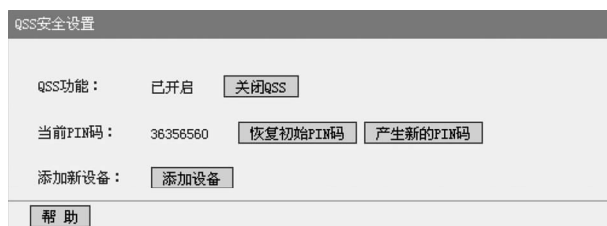


图 1-11 QSS 安全设置界面

在无线设置界面,可对“基本设置”“无线安全设置”“无线 MAC 地址过滤”“无线高级设置”和“主机状态”等项目进行设置。对于高级用户,其中的“无线网络安全设置”和“无线 MAC 地址过滤”都是非常实用的,配置界面如图 1-12、图 1-13 所示。

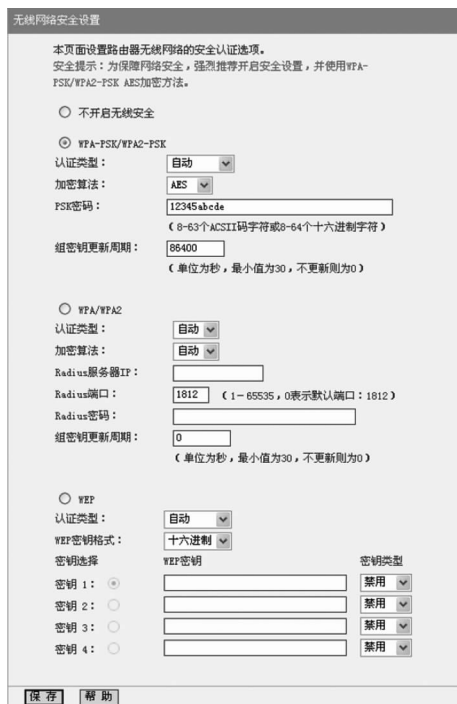


图 1-12 无线网络安全设置

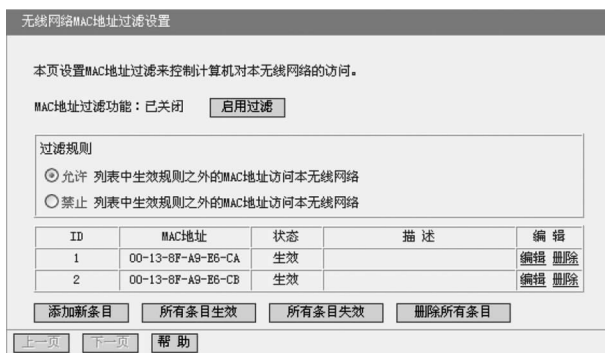


图 1-13 无线网络 MAC 地址过滤

在“安全功能”界面中，还有更为详尽的“安全设置”“高级安全选项”“局域网 WEB 管理”和“远程 WEB 管理”选项。如图 1-14 所示为高级安全选项。

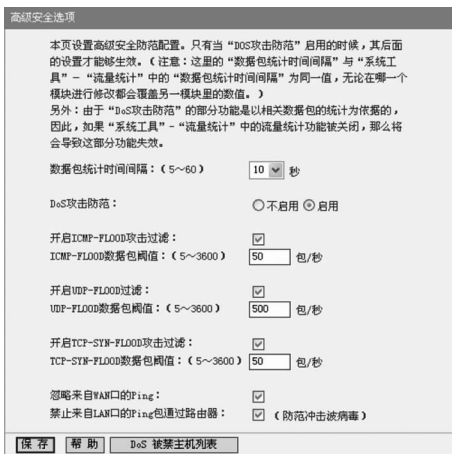


图 1-14 高级安全选项

TL-WR941N 也提供“家长控制设置”“上网控制设置”和“IP 带宽控制设置”功能，可对上网行为进行管理，如图 1-15 所示。

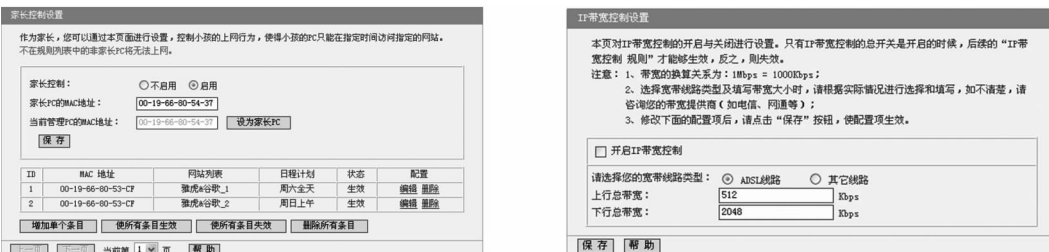


图 1-15 上网行为管理

更有特色的是，在“动态 DNS”设置中，TL-WR941N 还提供“花生壳”功能服务，它可以将计算机作为服务器，在其上建立网站和 FTP 空间。然后，只要去花生壳网站申请一个动态域名，别人就可以在网上通过这个域名访问到计算机上的网站和 FTP 空间了。



详细的设置和应用可以参考相关手册,这些高级设置会充分发挥无线路由器的功能,给用户带来更多的帮助。

三、局域网内的客户端配置

右击计算机桌面上的“网上邻居”图标,在弹出的快捷菜单中选择“属性”命令,在打开的“网络连接”窗口中,右击“本地连接”图标,在弹出的快捷菜单中选择“状态”选项,打开“本地连接状态”对话框,然后对 TCP/IP 协议进行属性设置。单击“属性”按钮,打开“本地连接 属性”对话框,选中“Internet 协议(TCP/IP)”选项,单击“属性”按钮,在打开的对话框中先后选中“自动获得 IP 地址”和“自动获得 DNS 服务器地址”单选按钮。

四、总结并绘制网络连接图和撰写说明书

使用 Visio 软件为建立的网络绘制拓扑结构图,并对组网建立过程撰写说明书。

任务三 组建交换式局域网



任务分析及任务目标

在任务二中,介绍的小型局域网仅仅是办公室和家庭应用范围内的局域网,规模比较小、结构简单、配置容易。但是如果一个企业或学校需要联网的计算机数量很多,上述局域网就不能满足要求了,而且还容易出问题,性能不够稳定,故障频发。所以应该组建更为强大的局域网络,如交换式局域网。



相关链接

用 HUB 连接的局域网会存在以下缺点和问题。

- (1)缺乏管理,容易发生冲突。
- (2)可靠性差,安全问题严重。

使用智能交换机代替 HUB 能提高带宽,独享网络;确保安全,防止外部对内网的攻击,监控和过滤网站信息,监管限制网络中的 P2P 应用。

在组网之前,需要介绍一些有关网络协议、IP 地址、网络拓扑结构的相关基础知识。

一、网络协议

网络协议是为在计算机网络中进行数据交换而建立的规则、标准或约定的集合。例如,网络中一个计算机用户和一个大型主机的操作员进行通信,由于这两个数据终端所用字符集不同,他们所输入的命令彼此不认识。为了能进行通信,规定每个终端都要将各自字符集中的字符先变换为标准字符集中的字符后,才进入网络传送,到达目的终端之后,再变换为该终端字符集的字符。当然,对于不兼容终端,除了需变换字符集字符外,其他特性,如显示格式、行长、行数、屏幕滚动方式等也需进行相应变换。

不同的计算机之间必须使用相同的网络协议才能进行通信。它是网络上所有设备(网络服务器、计算机及交换机、路由器、防火墙等)之间通信规则的集合,它规定了通信时信息必须采用的格式和这些格式的意义。

网络协议分为内部协议和外部协议两大类。其中,内部协议 OSI 是 open systems interconnection 的英文缩写,即开放系统互连。这是由国际标准化组织(ISO)制定的一种数据通信模型。该模型结构分为七层,即物理层、数据链路层、网络层、传输层、会话层、表示层和应用层,如图 1-16 所示。内部协议在组网中很少使用,主要提供给网络开发人员使用,而外部协议是组网时必须面对的。常见的协议有 TCP/IP、IPX/SPX。

为什么需要协议呢?因为实际的计算机世界是复杂的,有各种各样的通信终端,如 PC、工作站,还有各种掌上电脑和智能家电等;通信介质除了最常用的双绞线,还有电话线、电缆、光纤等。需要一个好的标准体系来描述各种网络通信世界,定义操作的规范,解决不同网络互连时所遇到的兼容性问题,只有这样,才能组成协调互通的网络。

加入分层的概念是为了将整个体系的不同组成部分更好地按不同功能级别来划分;同时在层次中引入了服务、接口和协议这三个概念,服务说明某层为上一层提供什么功能,接口说明上层如何使用下一层的服务,而协议定义如何实现本层的服务。每一层的具体作用如表 1-4 所示。



图 1-16 OSI 参考模型

表 1-4 七层结构的作用

结构名称	作用
应用层	面向用户服务
表示层	数据表示
会话层	会话控制
传输层	网络间数据包递交信任监测
网络层	逻辑地址寻址、路由功能
数据链路层	物理地址寻址、拓扑结构、线路存取方法
物理层	电及机械的有关定义

七层的定义和具体职责如下。

(1)物理层。物理层的任务是保证点到点链路在光、电和机械上是可以传送数据流的。它定义了物理链路的电气和机械特性,以及激活、维护和关闭这条链路的各项操作。处理单位是 bit。特征参数包括电压、数据传输率、最大传输距离、物理连接媒体等。物理层定义的标准包括 EIA/TIA RS-232、EIA/TIA、RS-449、V. 35、RJ-45 等。

(2)数据链路层。数据链路层的主要作用是控制网络层与物理层之间的通信。它保证了数据在不可靠的物理线路上进行可靠的传递。它把从网络层接收到的数据分割成特定的可被物理层传输的帧,保证了传输的可靠性。它的主要作用包括物理地址寻址,数据的成帧、流量控制,数据的检错、重发等。它是独立于网络层和物理层的,工作时无须关心计算机是否正在运行软件还是进行其他操作。数据链路层协议的代表包括 SDLC、HDLC、PPP、



STP、帧中继等。代表产品是交换机。

(3)网络层。网络层负责对子网间的数据包进行路由选择,它通过综合考虑发送优先级、网络拥塞程度、服务质量以及可选路由的花费来决定一个网络中两个节点间的最佳路径。另外,它还可以实现拥塞控制、网际互连等功能。对于各种不同的底层技术网络,为了隐藏物理网络细节,引入了逻辑地址这个概念,对各网络中每个网络接口,无论基于何种底层技术,都用逻辑地址来编号;类似地,也引入了包(packet)这个概念,来隐藏不同物理网络数据链路的的不同数据传送模式。通过逻辑信道技术,网络层解决了链路复用的问题,路由和寻径概念的引入和实现,使任意两台数据终端设备的数据接起来。网络层协议的代表包括IP、IPX、RIP、OSPF等。代表产品是路由器。

(4)传输层。网络层关注的是点到点的逐点转递,传输层关注的是端到端的最终效果。各种通信子网在性能上有很大差异,电话交换网、分组交换网、公用数据交换网、局域网等通信子网都可互连,但它们的吞吐量、传输速率、数据延迟等各不相同,传输层要负责隐藏各通信子网的差异,通过差错恢复、流量控制等功能,最终为会话层提供可靠的、无误的数据传输。传输层面对的数据对象主要是与会话层之间的界面端口。传输层是OSI参考模型中最重要的一层,它是两台计算机通过网络进行数据通信时第一个端到端的层次,起缓冲作用。当网络层的服务质量不能满足要求时,它将提高服务,以满足高层的要求;而当网络层服务质量较好时,它只需进行很少的工作。另外,它还要处理端到端的差错控制和流量控制等问题,最终为会话层提供可靠的、无误的数据传输。传输层协议的代表包括TCP、UDP、SPX等。代表产品有三层智能交换机。

(5)会话层。会话层维持面向连接的传输,为会话实体间建立连接;在两个会话用户之间实现有组织的、同步的数据传输;最终释放连接。

(6)表示层。不同计算机体系结构所使用的的数据表示法不同,表示层为异种机通信提供一种公共语言,完成应用层数据所需的任何转换,以便能进行互操作。定义一系列代码和代码转换功能,保证源端数据在目的端同样能被识别,如文本数据的ASCII码、表示图像的GIF或表示动画的MPEG等。

(7)应用层。应用层是最高层,是直接为应用进程提供服务的。其作用是在实现多个系统应用进程相互通信的同时,完成一系列业务处理所需的服务,这些服务按其向应用程序提供的特性分成组,并称为服务元素,有些可为多种应用程序共同使用,有些则为较少的一类应用程序使用。

在数据的实际传输中,发送方将数据送到自己的应用层,加上该层的控制信息后传给表示层;表示层也将数据加上自己的标识后传给会话层;以此类推,每一层都在收到的数据上加上本层的控制信息并传给下一层;最后到达物理层时,数据通过实际的物理媒体传到接收端。接收方则执行与发送方相反的操作,由下往上,将逐层标识去掉,重新还原成最初的数据。由此可见,数据通信双方在对等层必须采用相同的协议,定义同一种数据标识格式,这样才可能保证数据的正确传输。

总之,OSI参考模型有效地解决了不同网络体系互连时所遇到的兼容性问题,它的出现降低了网络的复杂程度,一旦网络发生故障,可迅速定位故障所处层次,便于查找和纠错;通过在各层上定义标准接口,使同属一层的不同网络设备间能实现互操作;它还保证了各层之间的相对独立;高层协议可以放在多种低层协议上运行,提高了网络的效率;因为每次更新

都只需在一个层上进行,不受整体网络的制约,所以它的出现刺激了网络技术革新,它是网络技术发展的原动力。

一些常用的协议如下。

(1) TCP/IP。TCP/IP 是最重要的一个协议,作为互联网的基础协议,没有它就不可能上网,任何与因特网有关的操作都离不开 TCP/IP。但是,TCP/IP 也是配置起来最麻烦的,单机上网还好,而如果要通过局域网访问互联网,就要详细设置 IP 地址、网关、子网掩码、DNS 服务器等参数。

TCP/IP 尽管是目前最流行的网络协议,但在局域网中的通信效率并不高,使用它浏览“网上邻居”中的计算机时,经常会出现不能正常浏览的情况。

(2) IPX/SPX 协议。IPX/SPX 协议本来是 Novell 开发的专用于 NetWare 网络的协议,但是现在大部分可以联机的游戏都支持 IPX/SPX 协议。虽然这些游戏通过 TCP/IP 也能联机,但显然还是通过 IPX/SPX 更方便,因为根本不需要任何设置。除此之外,IPX/SPX 协议在局域网中的用途似乎并不是很大。如果确定不在局域网中联机玩游戏,那么这个协议可有可无。

二、IP 地址

IP 地址(Internet protocol address)是一种给 Internet 上的主机编址的方式,也称为网际协议地址。常见的 IP 地址分为 IPv4 与 IPv6 两大类。

IP 地址被用来给 Internet 上的计算机一个编号。大家日常见到的情况是,每台联网的 PC 上都需要有 IP 地址才能正常通信。如果把 PC 比作一部电话,那么 IP 地址就相当于电话号码,而 Internet 中的路由器就相当于电话局的程控式交换机。IP 地址是给每个连接在 Internet 上的主机分配的一个 32 bit 地址。按照 TCP/IP 规定,IP 地址用二进制来表示,每个 IP 地址长 32 bit,比特换算成字节,就是 4 字节。例如,一个采用二进制形式的 IP 地址是 00001010000000000000000000000001,为了方便人们的使用,IP 地址经常被写成十进制的形式,中间使用符号“.”分开不同的字节,于是,上面的 IP 地址可以表示为 10.0.0.1,还有像 192.168.1.0 等。这种表示法记忆起来显然比 1 和 0 容易得多。

IP 地址就像人们的家庭住址,如果你要写信给一个人,你就要知道他的地址,这样邮递员才能把信送到。计算机就好比邮递员,它必须知道唯一的“家庭地址”,才能不至于把信送错人家。只不过人们的地址是使用文字来表示的,计算机的地址用二进制数字表示。TCP/IP 需要针对不同的网络进行不同的设置,且每个节点一般需要一个 IP 地址、一个子网掩码和一个默认网关。不过,可以通过动态主机配置协议(DHCP)给客户端自动分配一个 IP 地址,避免出错,也简化了 TCP/IP 的设置。因特网上的 IP 地址统一由 ICANN(Internet Corporation for Assigned Names and Numbers,因特网赋名和编号公司)来管理。

为了便于寻址及层次化构造网络,每个 IP 地址包括两个标识码(ID),即网络 ID 和主机 ID。同一个物理网络上的所有主机都使用同一个网络 ID,网络上的一个主机(包括网络上的工作站、服务器和路由器等)都有一个主机 ID 与其对应。NIC 定义了 5 种 IP 地址类型以适合不同容量的网络,即 A~E 类。其中,A、B、C 类由 InternetNIC 在全球范围内统一分配,如表 1-5 所示。D、E 类为特殊地址,作为多播和保留使用。

表 1-5 A、B、C 三类地址详细对照表

网络类别	最大网络数	IP 地址范围	最大主机数	私有 IP 地址范围
A	126(2 ⁷ -2)	1. 0. 0. 0~126. 255. 255. 255	16 777 214	10. 0. 0. 0~10. 255. 255. 255
B	16 383(2 ¹⁴)	128. 0. 0. 0~191. 255. 255. 255	65 534	172. 16. 0. 0~172. 31. 255. 255
C	2 097 151(2 ²¹)	192. 0. 0. 0~223. 255. 255. 255	254	192. 168. 0. 0~192. 168. 255. 255

还有以下一些特殊的 IP 地址。

- (1) IP 地址:127. 0. 0. 1。本地回环(loopback)测试地址。
- (2) 广播地址:255. 255. 255. 255。
- (3) IP 地址 0. 0. 0. 0:代表任何网络。
- (4) 网络号全为 0:代表本网络或本网段。
- (5) 网络号全为 1:代表所有网络。
- (6) 主机位全为 0:代表某个网段的任何主机地址。
- (7) 主机位全为 1:代表该网段的所有主机。

为节约 IP 地址空间,并增加安全性,保留一些 IP 地址段作为私网 IP,不会在公网上出现。处于私有 IP 地址的网络称为内网或私网,与外部公网进行通信必须通过网络地址翻译。

下面是一些私有地址的范围。

- (1) 在 A 类地址中:10. 0. 0. 0~10. 255. 255. 255。
- (2) 在 B 类地址中:172. 16. 0. 0~172. 31. 255. 255。
- (3) 在 C 类地址中:192. 168. 0. 0~192. 168. 255. 255。

三、网络拓扑结构

网络拓扑结构是指用传输媒体互连各种设备的物理布局,就是指用什么方式把网络中的计算机等设备连接起来。拓扑图给出网络服务器、工作站的网络配置和相互间的连接,它的结构主要有总线结构、环型结构、星型结构等,如图 1-17 所示。

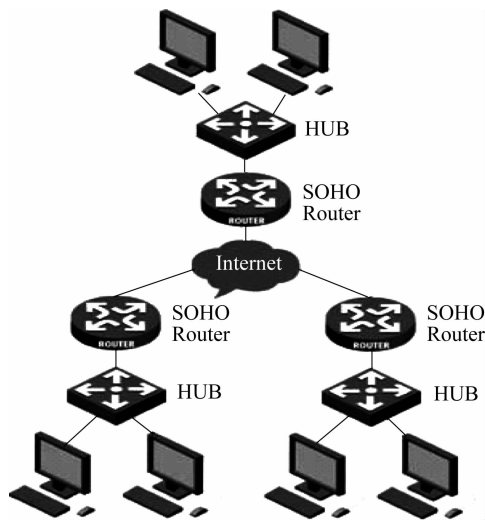


图 1-17 网络拓扑结构

(一) 总线型拓扑结构

总线型拓扑结构的所有设备都直接与一条称为公共总线的传输介质相连,如图 1-18 所示。这种介质一般是同轴电缆(包括粗缆和细缆),不过现在也有采用光缆作为总线型传输介质的,如 ATM 网、Cable Modem 所采用的网络等都属于总线型网络结构。可以用广播方式和点对点方式进行通信。

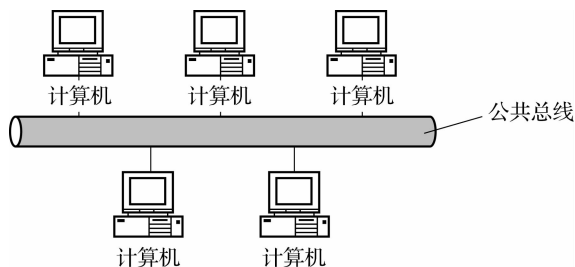


图 1-18 总线型拓扑结构

这种结构具有以下几方面的特点。

(1)组网费用低。这样的结构根本不需要另外的互连设备,直接通过一条总线进行连接,所以组网费用较低。

(2)这种网络各节点是共用总线带宽的,因此在传输速度上会随着接入网络用户量的增多而下降。

(3)网络用户扩展较灵活。需要扩展用户时只需要添加一个接线器即可,但所能连接的用户数量有限。

(4)维护较容易。单个节点(每台计算机或集线器等设备都可以看作一个节点)失效不影响整个网络的正常通信。但是如果总线一断,则整个网络或相应主干网段就断了。

(5)一次仅能有一个端用户发送数据,其他端用户必须等待获得发送权。

(二) 环型拓扑结构

环型拓扑结构的所有设备连接成环,信息通过环进行广播式传送,如图 1-19 所示。这种结构的网络形式主要应用于令牌环网中,在这种网络结构中各设备是直接通过电缆来串联的,最后形成一个闭环,整个网络发送的信息就在这个环中传递,这种网络因此而得名。

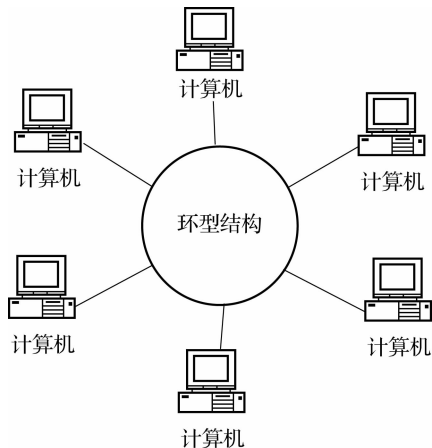


图 1-19 环型拓扑结构



环型拓扑结构的网络主要有以下几个特点。

(1)这种网络结构一般仅适用于 IEEE 802.5 的令牌环网(token ring network),在这种网络中,令牌在环型连接中依次传递。所用的传输介质一般是同轴电缆。

(2)这种网络的实现也非常简单,投资最小。可以从其结构示意图中看出,组成这个网络,除了各工作站就是传输介质,即同轴电缆,以及一些连接器材,没有价格昂贵的节点集中设备,如集线器和交换机等。但也正因为如此,这种网络所能实现的功能最为简单,仅能作为一般的文件服务模式。

(3)传输速度较快。在令牌环网中允许有 16 Mb/s 的传输速率,它比普通的 10 Mb/s 以太网要快许多。当然随着以太网的广泛应用和以太网技术的发展,以太网的速度也得到了极大提高,普遍都能提供 100 Mb/s 的网速,远比 16 Mb/s 要高。

(4)维护困难。从其网络结构可以看到,整个网络各节点间是直接串联的,这样任何一个节点出了故障都会造成整个网络的中断或瘫痪,维护起来非常不方便。另一方面因为同轴电缆所采用的是插针式的接触方式,所以非常容易造成接触不良或网络中断,而且查找故障非常困难。

(5)扩展性能差。它的环型结构决定了其扩展性能远不如星型结构好,如果要添加或移动节点,就必须中断整个网络,在环的两端做好连接器才能连接。

(三)星型拓扑结构

星型拓扑结构是目前在局域网中应用最为普遍的一种,在企业网络中几乎都采用这一方式,如图 1-20 所示。星型网络几乎是以太网专用的,它因网络中的各工作站节点设备通过一个网络集中设备(如集线器或交换机)连接在一起,各节点呈星状分布而得名。这类网络目前用得最多的传输介质是双绞线,如常见的五类线、超五类线等。

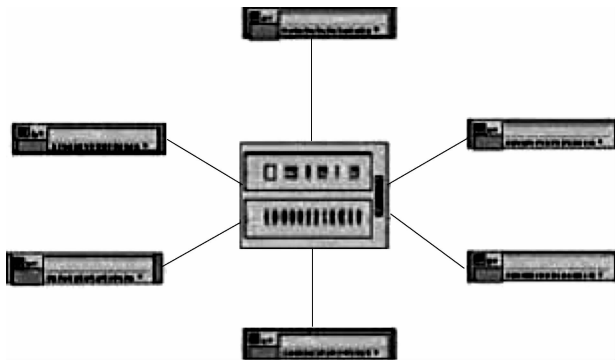


图 1-20 星型拓扑结构

星型拓扑结构的特点如下。

(1)容易实现,可靠性强。它所采用的传输介质一般都是通用的双绞线,这种传输介质相对来说比较便宜。这种拓扑结构主要应用于 IEEE 802.2、IEEE 802.3 标准的以太局域网中。由于每个连接点只连接一个设备,所以当连接点出现故障时只影响相应的设备,不会影响整个网络。

(2)节点扩展、移动方便。节点扩展时只需要从集线器或交换机等集中设备中拉一条线即可,而要移动一个节点只需要把相应节点设备移到新节点即可,而不会像环型网络那样改变一点会造成整体网络的变动。

(3)维护容易。一个节点出现故障不会影响其他节点的连接,可任意拆走故障节点,方便地将该节点从网络中删除。如果是整个网络的通信都不正常,则需考虑是中心节点是否出现了错误。

(4)采用广播信息传送方式。任何一个节点发送信息,在整个网中的节点都可以收到,这在网络方面存在一定隐患,但在局域网中使用影响不大。

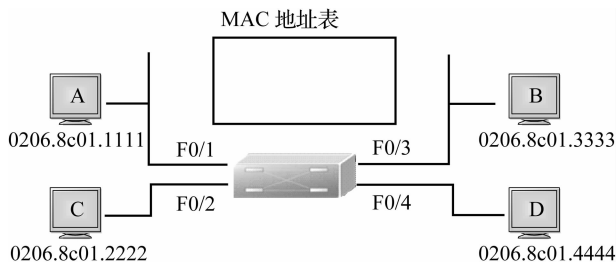
(5)网络传输数据快。这一点可以从1 000 Mb/s~10 Gb/s以太网的接入速度可以看出。

星型拓扑结构是用一个节点作为中心节点,其他节点直接与中心节点相连构成的网络。中心节点可以是文件服务器,也可以是连接设备。常见的中心节点为集线器。星型拓扑结构的网络属于集中控制型网络,整个网络由中心节点执行集中式通行控制管理,各节点间的通信都要通过中心节点。每一个要发送数据的节点都将要发送的数据发送到中心节点,再由中心节点负责将数据送到目的节点。因此,中心节点相当复杂,而各个节点的通信处理负担都很小,只需要满足链路的简单通信要求即可。

总体来说,星型拓扑结构相对简单,便于管理,建网容易,是目前局域网普遍采用的一种拓扑结构。采用星型拓扑结构的局域网,符合综合布线标准,能够满足多种宽带需求。

四、交换机

前面已经介绍了交换机的作用,它可以把一个网段分为多个网段,把冲突限制在一些细分的网段里。同时交换机又可以在不同网段之间进行MAC帧的转发,即连接了各个网段,使各个网段之间可以相互进行访问。通过细分网段,提高了网络带宽,扩大了局域网的范围,所以,它是本任务中的核心设备。交换机的内部都维护着一张MAC地址表,存放在RAM中,初始的MAC地址表是空的,如图1-21所示。之后接收网段上的所有数据帧,利用接收数据帧中的源MAC地址来建立MAC地址表,如图1-22所示。交换机的接口收到数据帧后,查找MAC地址表,如没有相应表项,交换机将该数据帧泛洪到所有其他接口上。如果所有主机都发送过数据帧,就可以建立完整的MAC地址表。如果数据帧的目的MAC地址在MAC地址表中有相应表项,则交换机将该数据帧直接发往相应的接口,如图1-23所示,从而保证其他接口上的主机不会收到无关的数据帧。对于未知单播帧、广播帧执行泛洪操作,如图1-24所示。总之,交换机是工作于OSI参考模型的第二层,即数据链路层的设备,能识别MAC地址,通过解析数据帧中目的主机的MAC地址,将数据帧快速地从源端口转发至目的端口,从而避免与其他端口发生碰撞,提高了网络的交换和传输速率。



刚启动后,交换机的MAC地址表为空

图 1-21 初始阶段

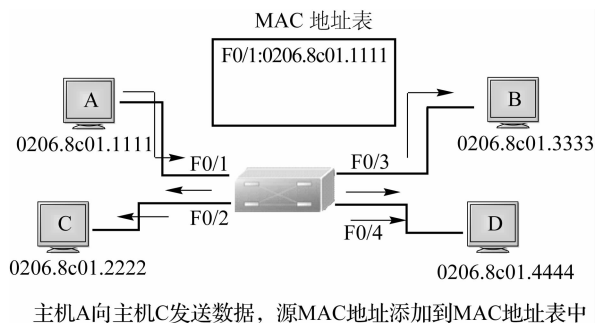


图 1-22 发送数据

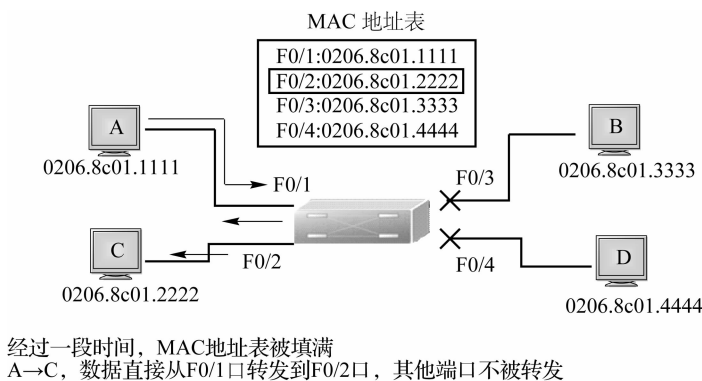


图 1-23 MAC 地址表填满

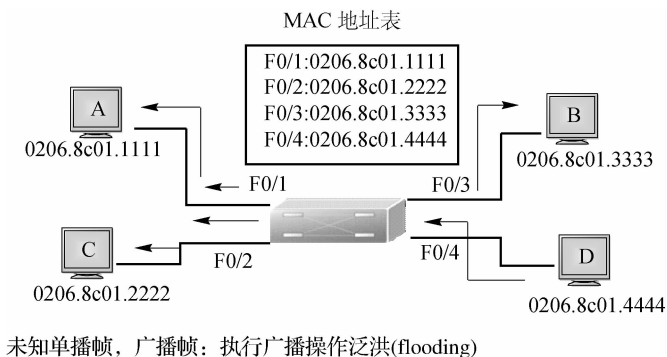


图 1-24 泛洪

而三层交换机是带路由功能的交换机，可工作在 OSI 参考模型的第 3 层，即网络层，也可工作在第 2 层。三层交换机作为三层设备使用时相当于一个多端口的路由器。三层交换机能根据 IP 地址转发数据包。

(1)如图 1-25 所示，交换式局域网中的通信有三种方式：单播、广播和组播。交换机可以实现各客户机单独享受全部带宽，如图 1-26 所示。

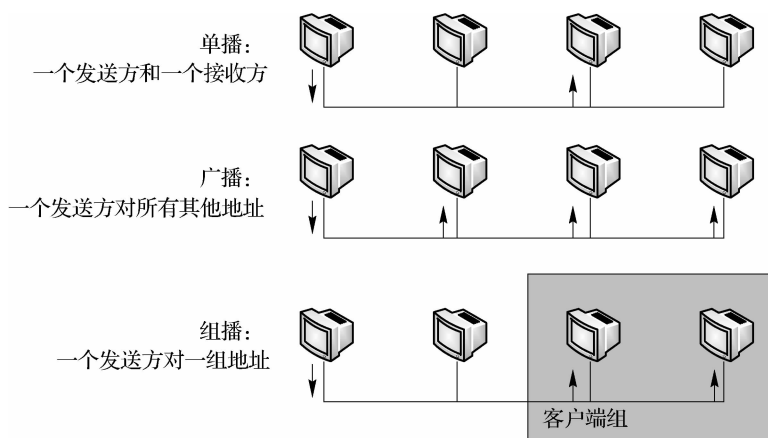


图 1-25 交换式局域网通信的三种方式

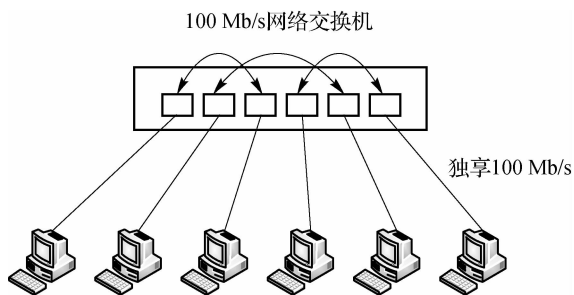


图 1-26 独享带宽

(2)交换机的转发有三种方式:直通式、存储转发式、无碎片直通方式。

①直通式。当输入接口检测到一个数据帧时只检查帧头,根据帧内的目的地址把数据帧发送到相应接口。

②存储转发式。这种方式先将数据帧完整地接收下来,交换机的控制器先缓存输入端口的数据包,然后进行 CRC 校验,滤掉不正确的帧,确认包正确后,取出目的地址,通过内部的地址表确定相应的输出端口,然后把数据包转发到输出端口。再根据目的地址转发到指定端口。

③无碎片直通方式。该方式是介于直通式和存储转发式之间的一种解决方案,它检查数据包的长度是否够 64 字节。如果小于 64 字节,说明该包是碎片(即在信息发送过程中由于冲突而产生的残缺不全的帧),则丢弃该包;如果大于 64 字节,则发送该包;该方式的数据处理速度比存储转发式快,但比直通式慢。

任务实施

现在需要为某单位的一层办公区域建立交换式局域网,以供办公人员使用,如图 1-27 所示。为了将交换式局域网理解透彻,我们可以将标准提高,采用三层结构模式设计,即核心层、汇聚层和接入层,每个层次都有其特定的功能,如图 1-28 所示。在实际情况下可以降低项目难度。

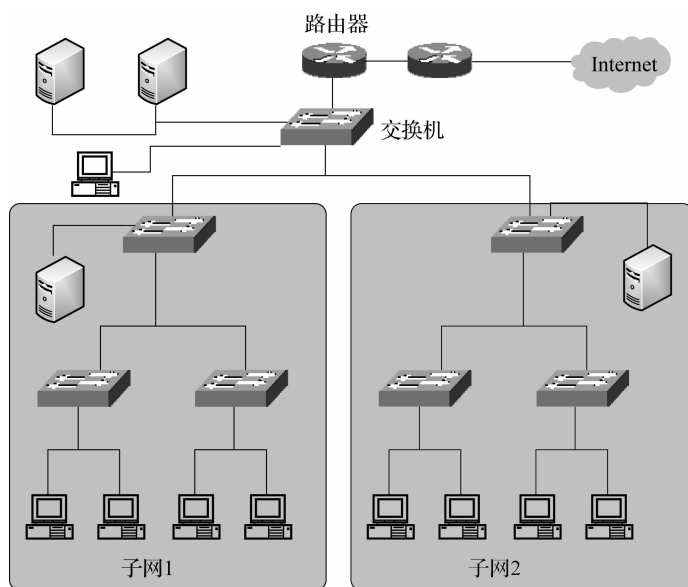


图 1-27 交换式局域网示意图

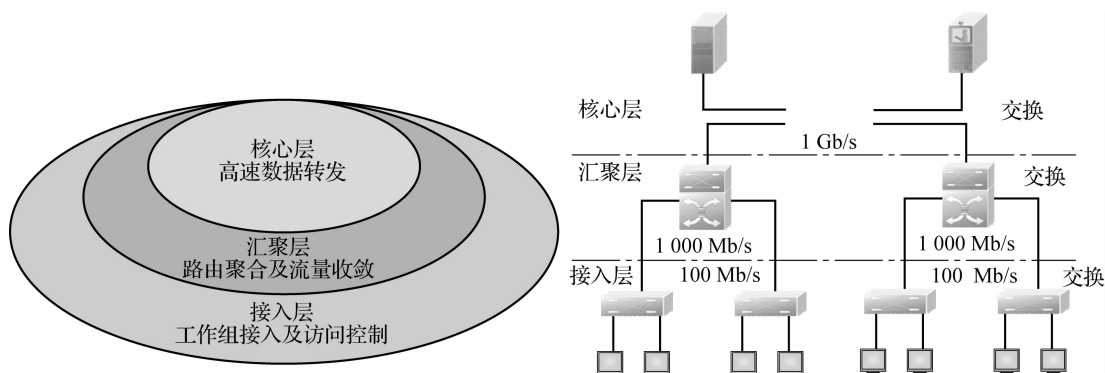


图 1-28 交换式局域网的三层结构

在机房中心放置核心交换机，并根据需要配置相应足够的 100 Mb/s 以太网接口和千兆模块。应该采用模块化机架结构，既可作为局域网高密度千兆网络骨干，又可以作为高密度 10/100 Mb/s 接入交换机。在其高性能和高可靠性的基础上，还能为用户提供丰富的流量控制、优先级访问和服务质量控制、网络安全控制等多种功能手段，及良好的可扩展性，可充分适应现代企业和园区接入网络的商务应用需求。

在汇聚层配置相应交换机，应该通过采用基于硬件的安全转发机制实现宽带接入的安全，在保证宽带接入网的性能和安全的同 时，最大程度简化网络的设计和管理，轻松实现高安全、高性能的宽带接入网。

在终端用户接入层配置楼层交换机，为小区用户提供 10/100 Mb/s 到桌面的带宽。

为了保证每个用户数据通信的安全性，需要将每个客户端连接到每个用户的 PC 上，或者在每个端口下通过二层交换机连接一组可以相互信任的用户群，这样在每个交换机下的客户端口的数据通信都将是安全的，不必担心该端口的数据通信会广播到其他端口而被

窃听。此外,也可利用客户端口的特性来建立多个相对独立的网络,而不用去通过划分 VLAN 来实现。

具体规划图如图 1-29 所示。

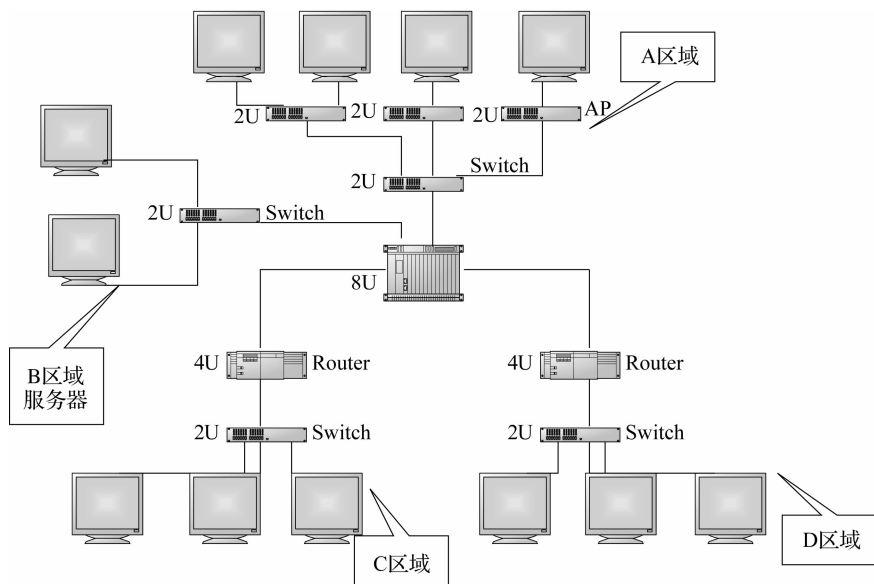


图 1-29 交换式局域网的规划图

具体规划设计和选型如下。

(1) 首先进行设备选型,如在 A 区域选择设置一台核心交换机,连接两台接入层交换机、一台无线 AP,构成了 A 区域的 LAN。

(2) 具体设备的选择要依据厂商的具体产品来进行配置,最好选择同一厂商的产品,并且要依据所需性能进行选择。

(3) 了解具体设备的接口和功能,并进行设备命名及端口描述。

(4) IP 地址规划,可以使用 C 类私有地址。各办公区域选择不同的网段。例如, A 区域使用 192.168.1.0/24 网段, B 区域使用 192.168.2.0/24 网段, C 区域使用 192.168.3.0/24 网段。后面还要进行子网划分。

(5) 路由规划和安全规划。

交换机的启动顺序(以思科交换机为例)如下。

启动加载器是存储在 NVRAM 中的小程序,并且在交换机第一次开启时运行。

步骤 1: PC 或终端已连接到控制台端口,如图 1-30 所示。



图 1-30 计算机与交换机相连

步骤 2: 终端仿真器应用程序(如 HyperTerminal)正在运行且配置正确,如图 1-31 所示。

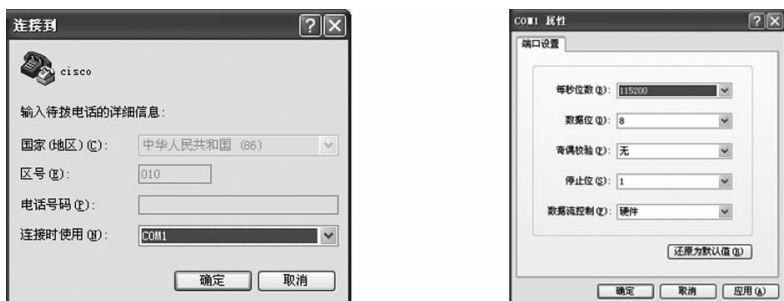


图 1-31 串口配置

步骤 3: 在控制台上查看启动过程,如图 1-32 所示。

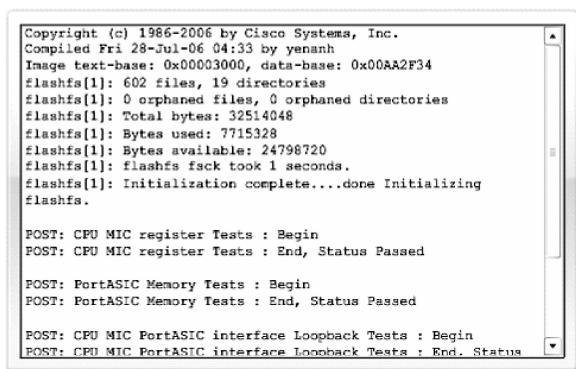


图 1-32 启动过程

步骤 4: 在控制台输入 en,并输入口令,交换机将回送命令提示符。再输入 show mac-address-table,交换机就回送当前存储的端口/MAC 地址映射表。

路由器初次配置过程如下。

(1) 通过 Console 配置口进行配置,用 RJ-45 一端与路由器的配置口相连,DB9 一端与计算机的串口相连。

(2) 选择超级终端建立连接图标,设置串口的属性对话框。

(3) 路由器上电启动,自检过程参考具体手册。

任务四 组建虚拟局域网



任务分析及任务目标

用交换机组建一个虚拟局域网并进行配置。通过组建虚拟局域网了解局域网的概念和目的,掌握其优点和作用。学会使用组建虚拟局域网的相关命令,并能够根据实际需求组建虚拟局域网。

相关知识链接

一、虚拟局域网的概念

虚拟局域网(virtual local area network, VLAN)是一种将局域网设备从逻辑上划分成一个个网段,从而实现虚拟工作组的新兴数据交换技术。这些虚拟工作组中的设备和用户并不受物理网段的限制,可以根据功能、应用等因素将它们组织起来,它们之间的通信就如同在同一网段中一样。同一个 VLAN 的站点可进行广播传输,而不同 VLAN 的站点不能进行广播传输。

二、使用虚拟局域网的目的

VLAN 之所以叫作虚拟局域网,是因为它是在虚拟路由器接口下创建的网段。例如,一个路由器只有一个用于终端连接的端口,这个端口被分配了 192.168.1.1/24 的地址,然而公司的销售部和研发部都要求单独成为一个子网,有单独的服务器。那么可以划分为 192.168.1.0~127/25、192.168.1.128~255/25 两个子网段。但是路由器的物理端口只能分配一个 IP 地址,如何来区分不同网段呢?这就可以通过在这个物理端口下创建两个逻辑接口来实现。例如,逻辑接口 F0/0.1 就分配 IP 地址 192.168.1.1/25,用于销售部,而 F0/0.2 就分配 IP 地址 192.168.1.129/25,用于研发部。这样就等于用一个物理端口实现了两个逻辑接口的功能,将原本只能划分一个网段的情形扩展到了可以划分两个或者更多网段的情形。这些网段因为是在逻辑接口下创建的,所以称之为虚拟局域网。

同样,如果想要每个不同交换机上的端口都分别属于不同的网段,那么有几个网段,就提供几个路由器的接口,此时虽然在路由器的物理端口上能定义这个接口可以连接哪个网段,但是在交换机的层次上,它并不能区分哪个端口属于哪个网段,唯一能够实现区分的方法,就是划分 VLAN,使用 VLAN 就能区分出某个交换机端口的终端是属于哪个网段的。

因此,当一个交换机上的所有端口中有至少一个端口属于不同网段或当路由器的一个物理端口要连接两个或者更多网段的时候,就需要使用 VLAN。

综上所述,VLAN 有以下几个优点。

(1)使网络设备的移动、添加和修改的管理开销减少,增加了网络连接的灵活性。使用 VLAN 技术可以将不同地点、不同网络、不同用户组合在一起,形成一个虚拟的网络环境,降低了管理费用。

(2)可以控制广播活动。LAN 分段可以防止广播风暴波及整个网络。VLAN 可以提供建立防火墙的机制,防止交换网络的过量广播。使用 VLAN 可以将某个交换端口或用户赋予某个特定的 VLAN 组,该 VLAN 组可以在一个交换网中或跨接多个交换机,在一个 VLAN 中的广播不会送到 VLAN 之外。同样,相邻的端口不会收到其他 VLAN 产生的广播。这样可以减少广播流量,释放带宽给用户使用,减少广播的产生。

(3)可提高网络的安全性。含有敏感数据的用户组可与网络的其余部分隔离,从而降低泄露机密信息的可能性。不同 VLAN 内的报文在传输时是相互隔离的,即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信,如果不同 VLAN 要进行通信,则需要通过路由器或三层交换机等三层设备。

三、划分虚拟局域网的方法

划分虚拟局域网的方法有以下几种。

1. 基于端口来划分 VLAN

可以利用交换机的端口来划分 VLAN 成员。被设定的端口都在同一个广播域中。例如,一个交换机的 1、2、6、7、8 端口被定义为虚拟网 A,同一交换机的 3、4、5 端口组成虚拟网 B。这样做允许各端口之间的通信,并允许共享型网络升级。但是,这种划分模式将虚拟局域网限制在了一台交换机上。单交换机端口定义的 VLAN 如图 1-33 所示。

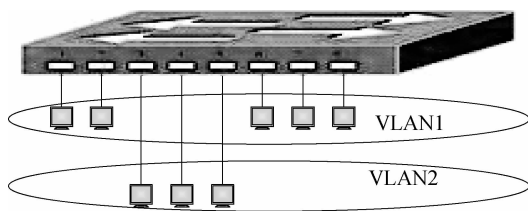


图 1-33 单交换机端口定义的 VLAN

第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN,不同交换机上的若干端口可以组成同一个虚拟网,如图 1-34 所示。

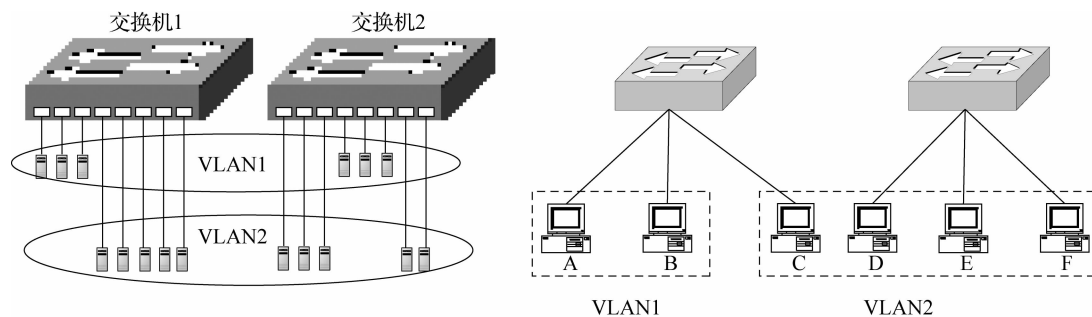


图 1-34 多交换机端口定义的 VLAN

以交换机端口来划分网络成员,其配置过程简单明了。因此,这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

2. 基于 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分的,即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点是,当用户物理位置移动时,即从一个交换机换到其他交换机时,VLAN 不用重新配置,因此,可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。这种方法的缺点是,在初始化时,所有用户都必须进行配置,如果有几百个甚至上千个用户,那么,配置是非常烦琐的。而且这种划分方法也会导致交换机执行效率降低,因为在每个交换机的端口都可能存在很多个 VLAN 组的成员,这样就无法限制广播包了。另外,对于使用笔记本电脑的用户来说,他们的网卡可能经常更换,这样,VLAN 就必须经常配置。

3. 根据网络层划分 VLAN

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的,虽然这种划分方法是根据网络地址,如 IP 地址划分的,但它不是路由,与网络层的路由毫无关系。

这种方法的优点是,如果用户的物理位置改变了,那么也不需要重新配置所属的 VLAN,而且可以根据协议类型来划分 VLAN,这对网络管理者来说很重要。这种方法不需要附加的帧标签来识别 VLAN,这样可以减少网络的通信量。

这种方法的缺点是效率低,因为检查每个数据包的网络层地址是需要处理时间的(相对于前面两种方法),一般的交换机芯片都可以自动检查网络上数据包的以太网帧头,但要让芯片能检查 IP 帧头,则需要更高的技术,同时也更费时。当然,这与各厂商的实现方法有关。

4. 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义,即认为一个组播就是一个 VLAN,这种划分方法将 VLAN 扩大到了广域网,因此具有更大的灵活性,而且也很容易通过路由器进行扩展,当然这种方法不适合局域网,主要原因是效率不高。在 VLAN 中,网络通过广播通知各 IP 节点,若 IP 节点响应,就可以加入该 VLAN 中,与该 VLAN 中的其他 IP 节点通信。

任务实施

一、熟悉并掌握 VLAN 的相关命令(思科交换机)

1. 交换机的基本状态

```
switch: ; ROM 状态,路由器是 rommon>
hostname> ; 用户模式
hostname# ; 特权模式
hostname(config)# ; 全局配置模式
hostname(config-if)# ; 接口状态
hostname(config-if)# ; 配置交换机的 VLAN 参数
```

2. 交换机的口令设置

```
switch>enable ; 进入特权模式
switch#config terminal ; 进入全局配置模式
switch(config)#interface fastethernet 0/1 ; 进入端口配置模式
switch(config)#interface vlan 100 ; 进入 VLAN 配置模式
switch(config)#hostname ; 设置交换机的主机名
switch(config)#enable secret * * * ; 设置特权加密口令
switch(config)#enable password * * * ; 设置特权非加密口令
switch(config)#line console0 ; 进入控制台窗口
switch(config-line)#line vty04 ; 进入虚拟终端
switch(config-line)#login ; 允许登录
```



```
switch(config-line) # password * * ; 设置登录口令  
switch # exit ; 返回命令  
switch(config-if) # end ; 直接返回用户模式
```

3. 帮助信息

```
? ; 显示当前模式下的所有命令  
X? ; 显示以某字母开头的命令  
命令? ; 显示命令的参数
```

4. 常用验证命令

```
show version ; 显示交换机的版本信息  
show running-config ; 显示交换机当前配置信息  
show configure ; 显示交换机配置参数副本信息  
show interface ; 显示端口状态  
show mac-address-table ; 显示 MAC 地址表  
show mac-address-table aging-time ; 显示 MAC 地址表记录的生存时间  
show ip interface ; 显示 VLAN 端口状态  
ping ip ; 可达性测试
```

5. 保存/删除交换机配置信息

```
switch # write memory ; 保存 flash 中的配置信息  
switch # delete flash:config.txt  
switch # delete flash:vlan.dat ; 删除 flash 中的配置信息
```

6. 将一个端口划归 VLAN

```
switch(config) # interface fastethernet 0/1  
switch(config-if) # switchport mode access  
switch(config-if) # switchport access vlan 100
```

7. 将一组端口划归 VLAN

```
switch(config) # interface fastethernet 0/1-12  
switch(config-if) # switchport mode access  
switch(config-if) # switchport access vlan 100
```

8. 设置 VLAN 的 IP 地址

```
switch(config) # interface vlan 100  
switch(config-if) # ip address ip subnetmask
```

二、单交换机划分 VLAN

1. 网络规划

交换机的 IP 地址:10.65.1.10。

交换机的 f0/1-f0/4 vlan2, f0/5-f0/8 vlan3。

2. 建立物理连接

单交换机的物理连接如图 1-35 所示。

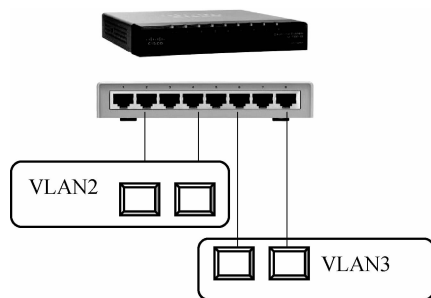


图 1-35 单交换机的物理连接

3. 配置交换机和计算机

首先要用线缆连接交换机,在计算机上使用“超级终端”程序。要对端口进行设置,待交换机进行初始化,进入 `switch>` 模式。当提示 `Would you like to enter the initial configuration dialog? [yes/no]:` 时,输入 `n` 并按 `Enter` 键进入 `switch>` 模式。

交换机配置如下。

```
switch>en
switch# config t
switch(config)# hostname SWB
switch(config)# exit
SWB# vlan database
SWB(vlan)# vlan2
SWB(van)# exit
SWB(config)# int f0/1
SWB(config-if)# switchport access vlan2
.....
SWB(config-if)# int f0/4
SWB(config-if)# switchport access vlan2
SWB(config-if)# int f0/5
SWB(config-if)# switchport access vlan3
.....
SWB(config-if)# int f0/8
SWB(config-if)# switchport access vlan3
```

计算机配置如下。

```
PCA login:root
Password:linux
[root#PCA root]# ifconfig eth0 10.65.1.1 netmask 255.255.0.0
.....
```



4. 网络连通性测试

```
[root#PCA root]#ping 10.65.1.3(通,在vlan2)
[root#PCA root]#ping 10.66.1.3(通,在vlan3)
[root#PCA root]#ping 10.65.1.3(不通,不同VLAN需要路由)
```

三、跨交换机划分 VLAN

1. 网络规划

交换机 A 的 IP 地址:10.65.1.7。
交换机 B 的 IP 地址:10.65.1.8。
交换机 A 的 f0/1-f0/4 vlan2, f0/5-f0/7 vlan3, f0/8 为 trunk。
交换机 B 的 f0/1-f0/4 vlan2, f0/5-f0/7 vlan3, f0/1 为 trunk。
计算机 A 的 IP 地址:10.65.1.1。
计算机 B 的 IP 地址:10.66.1.1。
计算机 C 的 IP 地址:10.65.1.3。
计算机 D 的 IP 地址:10.66.1.3。

2. 建立物理连接

如图 1-36 所示,建立跨交换机的物理连接。

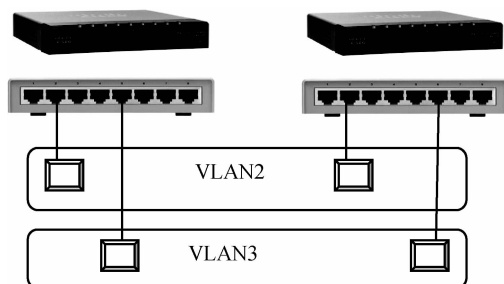


图 1-36 跨交换机的物理连接

3. 配置交换机和计算机

交换机配置如下。

```
switch>en
switch#conf t
switch(config)#hostname SWB
switch(config)#exit
SWB#vlan database
SWB(vlan)#vlan2
SWB(van)#exit
SWB(config)#int f0/1
SWB(config-if)#switchport access vlan2
.....
```



```

SWB(config-if) # int f0/4
SWB(config-if) # switchport access vlan2
SWB(config-if) # int f0/5
SWB(config-if) # switchport access vlan3
.....
SWB(config-if) # int f0/7
SWB(config-if) # switchport access vlan3
SWB(config-if) # int f0/8
SWB(config-if) # switchport mode trunk
SWB(config-if) # switchport trunk allowed vlan 1,2,3
SWB(config-if) # switchport trunk encap dot1q
SWB(config-if) # end
.....

```

计算机配置如下。

```

PCA login:root
Password:linux
[root # PCA root] # ifconfig eth0 10.65.1.1 netmask 255.255.0.0
[root # PCA root] # route add default gw 10.65.1.9
.....

```

4. 网络连通性测试

```

[root # PCA root] # ping 10.65.1.3(通,在vlan2)
[root # PCA root] # ping 10.66.1.3(通,在vlan3)
[root # PCA root] # ping 10.65.1.3(不通,不同VLAN需要路由)

```

四、总结

首先在交换机中创建所需的 VLAN 名和 VLAN ID 号。另外,如果交换机需要与其他交换机相连,那么还需要为交换机上联端口设置 TRUNK(VLAN 中继)。完成上述设置后,就可以将交换机的相应端口加入 VLAN 中。交换机设置 VLAN 的具体操作过程如下所述(以 Cisco 交换机为例)。

步骤 1:在 Windows 操作系统的“开始”→“运行”菜单项中,输入“telnet ×××.×××.×××.×××”(×××.×××.×××.×××为要设置 VLAN 交换机的 IP 地址),登录到交换机上。

步骤 2:在交换机配置界面中输入如下命令。

```

Password:××××
Cisco>enable
Password:×××× ; 添加 VLAN
Cisco#vlan database ; 进入配置 VLAN 模式
Cisco(vlan)#vlan 30 name hello
; 添加一个 VLAN ID 为 30,VLAN 名为 hello 的 VLAN

```



```
VLAN 30 added;
Name:hello
Cisco(vlan) # exit
Cisco# config terminal
Enter configuration commands,one per line. End with CNTL/Z.
; 将 24 端口配置成 trunk
Cisco(config) # interface f0/24
Cisco(config-if) # switchport mode trunk
Cisco(config-if) # switchport trunk allowed vlan all
Cisco(config-if) # exit
; 将 1 端口加到 VLAN 30 中
Cisco(config) # interface f0/1
Cisco(config-if) # switchport mode access
Cisco(config-if) # switchport access vlan 30
Cisco(config-if) # end
Cisco# copy running-config start-config
Destination filename [start-config]?
% Warning:There is a file already existing with this name
Do you want to over write? [confirm]
2023 bytes copied in 2.440 secs (1011 bytes/sec)
至此,就完成了交换机设置 VLAN 的全过程。
```



项目归纳总结

本项目从网络基础知识入手,介绍了网络的结构、种类、作用,应熟练掌握网络的常用设备,如集线器、交换机、路由器等,明确这些设备的作用和使用方法。从家庭的小型局域网开始,着重介绍了局域网的拓扑结构、构成原理、组建方法等。对于小型局域网,要学会设备连接,重点掌握工具的使用方法和基本操作技能,如双绞线的制作、网线测试工具的使用等。在学会掌握小型局域网组建过程的基础上,要继续完成交换式局域网的构成操作练习,加深对交换机、路由器的认识和对网络协议的理解。交换式局域网需要进行一定配置,熟练掌握这些步骤是非常必要的。在设置 VLAN 的过程中,要理解其含义和目的。在配置过程中要结合具体型号的交换机进行,多阅读参考手册会有很大帮助。


知识与能力考核

课程名称:网络与综合布线系统工程技术		授课地点:		
项目一:局域网的组建		授课教师:	授课学时:	
课程性质:理实一体课程		综合评分:		
知识掌握情况评分(35分)				
序号	知识考核点	教师评价	配 分	实际得分
1	掌握网络的基本知识		5	
2	掌握网络设备的性能和参数		10	
3	掌握交换式局域网的概念和作用		5	
4	掌握虚拟局域网的概念和作用		5	
5	掌握 IP 地址的概念		10	
工作任务完成情况评分(65分)				
序号	能力操作考核点	教师评价	配 分	实际得分
1	能够正确使用工具和测试仪器		15	
2	能够制作双绞线		5	
3	能够熟练使用 Visio 软件进行绘图		10	
4	能够熟练使用 Packet Tracer 软件		15	
5	能够正确组建交换式局域网		10	
6	能够正确配置和划分 VLAN		10	
违规扣分(50分)				
序号	违规内容	教师评价	配 分	实际扣分
1	设备、仪器、仪表损坏		10	
2	课上不参与小组工作		15	
3	严重旷课、缺课		15	
4	严重干扰课堂秩序		10	


自测题

1. 上网搜集有关局域网硬件和软件的资料并撰写学习报告。
2. 在家组建一个自己的无线局域网并绘制网络拓扑图。



3. 到网吧进行实地调研,了解网吧的局域网构成并绘制网络拓扑图。
4. 了解组网工具、仪器并学会使用。
5. 对两台计算机进行对等网的连接(制作直通和交叉双绞线)。
6. 什么是网络协议? 交换式局域网的核心设备有哪些?
7. 以太网交换机有何特点? 它与集线器有何区别?
8. 比较共享式局域网和交换式局域网的异同,并撰写报告。
9. 学习局域网 802.3 标准,并撰写报告。
10. 为什么要划分 VLAN? VLAN 的优点是什么?
11. 划分虚拟局域网的方法有哪些?

项目二

连接 Internet



项目综述

当今社会,局域网已经不能满足公司、企业、家庭的需要,越来越多的有用资源出现在全球范围内的网络上,为了共享全球范围内的资源和实现全球计算机通信,必须在彼此之间进行互连,构成更为庞大的网络。当年思科的创始人就是为了实现不同局域网的互连创立了思科(Cisco)公司。各企业都希望能将自己的局域网接入 Internet,因为这是一个更为广阔的虚拟世界。接入 Internet 有很多方式,常用的有 ISDN 接入、FTTX+LAN、ADSL 和代理服务器上几种方式。在接入 Internet 之前,需要进行子网划分,因为在 IPv4 中 IP 地址是有限的,不可能为局域网中的每台机器都分配唯一有效的地址,所以要进行地址划分。另一方面,在掌握交换机配置的基础上,进一步学习、了解路由器的基础知识和配置要点是非常必要的。以上知识和技能需要通过实际操作来学习、巩固和加深。连接 Internet 项目综述表如表 2-1 所示。

表 2-1 连接 Internet 项目综述表

教学内容	任务一 子网划分 任务二 路由器的配置 任务三 如何连接 Internet	参考学时	8
知识目标	掌握子网划分方法和子网掩码的理论,了解熟悉局域网接入 Internet 的几种方法,掌握路由器的配置要点		
技能目标	能够进行子网划分的操作,能够进行路由器基本配置操作,能够利用代理服务器实现上网		
教学重点	网络的组建方法和步骤		
教学难点	子网的划分及子网掩码概念的理解,路由器的典型配置		
教学载体与资源	教材、PPT、实训室、参考手册、网络资源		
教学方法建议	引导演示,师生共同参与完成项目		



续表

教学过程	1. 下达任务和要求； 2. 教师带领学生共同分析任务； 3. 分组讨论
考核评价	1. 小组内互相评价； 2. 教师根据任务完成情况和过程进行综合打分评价

项目准备

(1)完成本项目所需的项目资源清单如表 2-2 所示,按小组配发。

表 2-2 项目二资源清单表

序号	名称	规格/型号	数量
1	计算机	硬盘空间 200 MB 以上	1 台
2	操作系统	Windows 2000/XP,SP2 以上	1 套
3	Visio 软件	2003 或 2007 版本	1 套
4	Packet Tracer 软件	5.0、6.0 版本	1 套
5	压线钳、双绞线等组网辅料	国产品牌	若干
6	代理服务器软件 SyGate、Proxy	最新版本	1 套
7	交换机 1	思科(Cisco)SF500-24 24 口百兆可堆叠全网管交换机	1 台
8	交换机 2	思科(Cisco)2960	1 台
9	交换机 3	思科(Cisco)SF90-24 24 口非网管型交换机	1 台
10	路由器 1	思科(Cisco)RV110W Wireless-N VPN 防火墙路由器	1 台
11	路由器 2	思科(Cisco)RV042 4 口 VPN 路由器	1 台

(2)预习要点。

- ①IP 地址的进一步详细研究和总结。
- ②Internet 上网的几种方式。
- ③路由器的相关知识。
- ④其他网络设备的使用方法。
- ⑤Packet Tracer 6.0 软件的使用。
- ⑥子网划分的优点。

任务一 子网划分

任务分析及任务目标

网络中的任何设备都需要一个 IP 地址,但在目前情况下不可能给每台设备都分配一个有效地址,因此采用地址划分技术,将 IP 地址分成网络号、子网号、主机号三部分。这样既节约了 IP 地址,避免浪费,又可以限定广播的传播,保证了网络的安全。

相关知识链接

一、IP 地址和子网掩码

在前面的项目中,我们介绍了 IP 地址的概念。IP 地址分为网络位和主机位两部分,如图 2-1 所示。A、B、C、D 四类 IP 地址的结构如图 2-2 所示。

网络位		主机位	
172	16	123	208

图 2-1 IP 地址的组成

A类:	0NNNNNNN	Host	Host	Host
	(1~127)			
B类:	10NNNNNNN	Network	Host	Host
	(128~191)			
C类:	110NNNNNN	Network	Network	Host
	(192~223)			
D类:	1110MMMM	多播组	多播组	多播组
	(224~239)			

图 2-2 四类 IP 地址的结构

当然还有一些特殊的 IP 地址,如下所述。

1. 广播地址

主机号各位全是 1 的 IP 地址用于广播,即直接广播地址。直接广播地址可以标识网络上的所有主机。当某台主机需要发送广播时,可以使用直接广播地址向该网络上的所有主机发送报文。

2. 有线广播地址

有线广播地址,即 255.255.255.255,所有位都是 1,主要用于本网的广播。



3.0 地址

主机号各位全为 0 时,表示为本地网络。例如,172.18.0.0 表示 172.18 这个 B 类网络。

4. 回送地址

127.0.0.1 是回送地址,指本地机,一般用来测试。回送地址是本机回送地址(loopback address),即主机 IP 堆栈内部的 IP 地址,主要用于网络软件测试以及本地机进程间通信。所以无论什么程序,一旦使用回送地址发送数据,协议软件立即返回,不会进行任何网络传输。大家经常会在本机上用“ping 127.0.0.1”做回路测试,用来验证本机的 TCP/IP 是否被正确安装。能 ping 通就说明网卡和协议没有问题。其实,使用“ping 127.1”也能得到同样的测试结果,大家可以试一试。因为“ping 127.1”和“ping 127.0.0.1”是一样的,都是在进行回路测试。

在 Internet 的地址结构中,每台主机都会有唯一的一个 Internet 地址,这样就避免了网络上的地址冲突。就好像两家人不可能使用一个收信地址,否则收发信件会造成混乱。所以当 一个局域网需要与 Internet 连接时,一定要向 InternetNIC(Internet 网络信息中心)申请 Internet 合法的 IP 地址。如果只是需要组建局域网,不连接 Internet,那么可以任意使用 A、B、C 类地址。

当然大家也有这样的生活体会:一个院子有很多住户,大家都用一个邮政收信地址,统一收到信后再分发到各户,这就相当于单位内部组网。为了避免各个局域网任意使用网络地址造成 Internet 地址冲突,管理者也进行了具体分配。地址分配按照如表 2-3 所示的私有地址表进行。

表 2-3 私有地址表

A 类	10.0.0.0~10.255.255.255
B 类	172.16.0.0~172.31.255.255
C 类	192.168.0.0~192.168.255.255

了解了 IP 地址的构成,就容易理解什么是子网掩码了。如前所述,IP 地址包含了网络号和主机号,但是如果 不指定,那么知道哪些位是网络号,哪些是主机号呢?这就需要通过子网掩码来实现。

子网掩码由 1 和 0 组成,且 1 和 0 分别连续。子网掩码的长度是 32 位,左边是用二进制数字 1 表示的网络位,1 的数目等于网络位的长度;右边是用二进制数字 0 表示的主机位,0 的数目等于主机位的长度。这样做的目的是让掩码与 IP 地址做“与”运算时用 0“与”掉原主机数,而不改变原网络段数字,而且很容易通过 0 的位数确定子网的主机数。只有通过子网掩码,才能表明一台主机所在的子网与其他子网的关系,使网络正常工作。

子网掩码虽然不是一个地址,但是可以确定一个网络层地址中哪一部分是主机号,哪一部分是网络号。掩码为 1 的部分代表网络号,掩码为 0 的部分代表主机号。子网掩码的作用就是获取主机 IP 的网络地址信息,用于区别主机通信的不同情况,由此选择不同的路由。其中,A 类地址的默认子网掩码为 255.0.0.0;B 类地址的默认子网掩码为 255.255.0.0;C 类地址的默认子网掩码为 255.255.255.0。以上都属于边界子网掩码,很明显,主机位没有借位,使用了整个字节来划分子网。

除了使用上述表示方法之外,还有使用子网掩码中 1 的位数来表示的。在默认情况下,A 类地址为 8 位,B 类地址为 16 位,C 类地址为 24 位。例如,A 类的某个地址为 12. 10. 10. 3/8,这里的最后一个 8 说明该地址的子网掩码为 8 位。子网掩码不能单独存在,必须结合 IP 地址一起使用。用子网掩码判断 IP 地址的网络号与主机号的方法是用 IP 地址与相应的子网掩码进行“与”运算,可以区分出网络号部分和主机号部分。例如,10. 67. 88. 1 是 A 类 IP 地址,所以默认子网掩码为 255. 0. 0. 0,分别转化为二进制进行“与”运算后,得出网络号为 10。再如,202. 31. 153. 3 和 202. 31. 153. 80 为 C 类 IP 地址,默认子网掩码为 255. 255. 255. 0,进行“与”运算后得出两者网络号相同,说明两主机位于同一网络。

二、划分子网的目的和方法

由于目前 IPv4 的地址有限,且只分为五类地址,实际上能用的只有 A、B、C 三类,而且这三类的地址范围都比较大,所以造成 IP 地址浪费比较严重。为了提高 IP 地址的利用率,将 A、B、C 三类地址再利用掩码划分成更细的网段,这样不仅可以充分利用 IP 地址资源,避免造成资源浪费,还可以减少网络阻塞,减少网络的广播。

划分子网是使用主机号字节中某些位作为子网号的一种机制。在没有划分子网时,一个 IP 地址分为两部分,即网络号和主机号,而划分后一个 IP 地址分为 3 部分,即网络号、子网号和主机号,子网号和主机号是由原先 IP 地址的主机地址部分分割成两部分得到的。因此,划分子网的能力依赖于被子网化的 IP 地址类型。IP 地址中主机地址的位数越多,能分得的子网和主机越多。划分子网实际上是把主机地址的一部分拿走用于识别子网。主机位借位说明如图 2-3 所示,当主机位借一位时可分为 2 个网段,借两位时可分为 4 个网段。

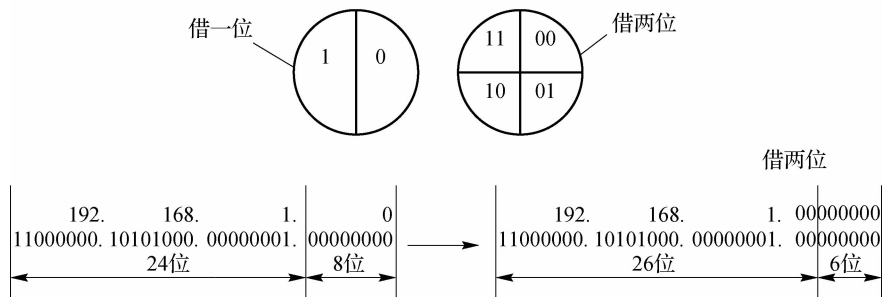


图 2-3 主机位借位说明

如 192. 168. 1. 0 网络借两位时,具体分析如图 2-4 所示,可用的网段是 192. 168. 1. 0、192. 168. 1. 64、192. 168. 1. 128 和 192. 168. 1. 192。

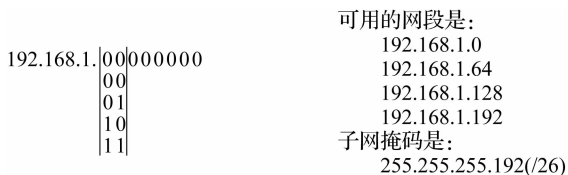


图 2-4 借两位的具体分析



所以每段可用的 IP 地址范围如图 2-5 所示。其中,除去子网号(子网地址)192.168.1.0 和广播地址 192.168.1.63 外,可用的 IP 地址是 192.168.1.1~192.168.1.62,共 2^6-2 个。其实按规定子网号不能全为 0 或 1。所以上面的例子中就不是 4 个网段,而是 2 个网段。全为 0 表示本子网网络,全为 1 的地址用于向子网广播。但是,目前很多设备和操作系统都支持子网号全 0 和全 1,不存在问题,所以子网号全 0 和全 1 也可以使用。

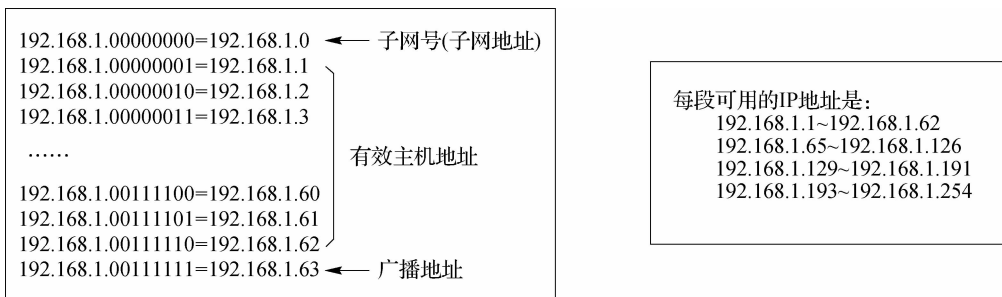


图 2-5 每段可用的 IP 地址范围

任务实施

一、划分子网的步骤

在划分子网时必须为每一个子网分配一个子网号,所以要确定所需要的子网数和每个子网的最大主机数。

划分子网的方法和过程如下。

- (1)确定需要子网的数量,即需要多少子网号,这样就可以标识每个子网。
- (2)确定需要主机号的数量,用来标识每个子网的所有主机。
- (3)确定一个合适的子网掩码。
- (4)确定每个子网的网络地址。
- (5)确定每个子网上主机地址的范围。

二、实例任务

某集团现有两家子公司,每家子公司又有 4 个部门。现分配了一个 192.168.1.0/8(子网掩码是 255.255.255.0)的网段,需要为子公司及子公司的部门分配网段。

1. 分析

根据以上提供的条件,需要划分 2 个子网段,每家子公司的网段中再划分 4 个子网。

2. 步骤

1)划分 2 家子公司的所属网段

有两家子公司,所以 $2^N \geq 2 \geq 2^{N-1}$,则 $N=2$ 。因此网络位需要向主机位借 2 位。这样就可以从 192.168.1.0/8 大网段划出 2 个子网(不包含子网号是 0 和 1 的两个,即子网号只能是 01 和 10)。因此,算上原有的网络号 192.168.1,则规划出的两个子网的网络地址是 192.168.1.64(即 192.168.1.01000000)和 192.168.1.128(即 192.168.1.10000000),子网掩码

都是 255.255.255.192。这样,目前每个子网的主机范围分别是 192.168.1.65~192.168.1.126 和 192.168.1.129~192.168.1.190。

2) 为子公司下的 4 个部门进行网段划分

因为每个子公司有 4 个部门,所以在划分子网的基础上再进行网段划分。因为有 4 个部门,所以 $2^N \geq 4 \geq 2^{N-1}$,则 N 为 2。因此,主机位借 2 位后可划出 4 个子网。例如,192.168.1.64 子网段就可划分为 192.168.1.64/28、192.168.1.80/28、192.168.1.96/28 和 192.168.1.112/28。每个子公司的部门可容纳的主机数是 $2^4 - 2 = 14$ 。

通过以上操作便完成了合理的子网划分。从以上实例操作可以看出,很多情况下需要的子网数量是不同的,需要调整子网的规模大小,避免造成 IP 地址浪费。这种调整方法就属于变长子网划分,即对已划分好的子网进行进一步划分。如此就形成了不同规模的网络。

任务二 路由器的配置

任务分析及任务目标

路由器是连接两个以上不同网络的设备,能将数据打包后通过网络传送至目的地,工作在 OSI 参考模型的网络层。路由器能够实现数据报文的存储、转发和寻径,掌握一定的路由器配置方法非常必要,一般是通过模拟软件 Packet Tracer 来实现。本任务的目标是继续深入掌握路由器的基础知识,学会使用模拟软件,懂得路由器的配置方法,实现多台路由器间静态路由和动态路由协议的配置。

相关知识链接

路由器在前面的任务中已经有所介绍,它是一种非常重要的网络设备,应该具备两个或两个以上的接口,是属于网络层的设备,具备转发、存储、寻径功能。路由器的主要作用是:网络互联和分组数据转发,即路由选择(routing)。作为不同网络之间连接的枢纽,路由器系统构成了基于 TCP/IP 的国际互联网络 Internet 的主体脉络,也可以说,路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一,它的可靠性和稳定性则直接影响网络连接的质量。

1. 路由器的结构及配置途径

路由器的结构如图 2-6 所示,包括内存、CPU、时钟、电源、操作系统,这看上去很像一台计算机。端口包括 RJ-45 端口、控制端口(console port)、扩展口。一般来讲,可以通过两种方式进行路由器的配置。

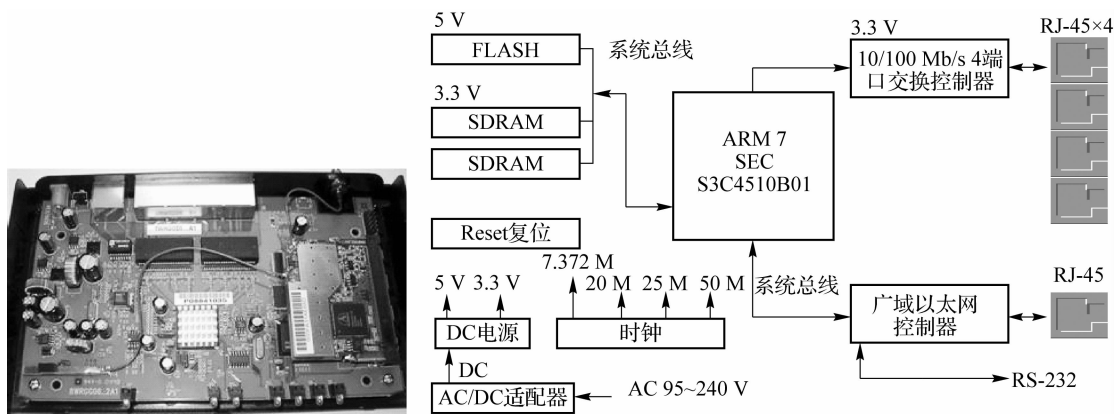


图 2-6 路由器的结构

(1)通过 Console 端口的连接进行配置。通过 Console 端口配置路由器如图 2-7 所示。在配置时使用的 Console 线如图 2-8 所示，一端连接计算机串口，一端连接路由器的 Console 端口。Console 端口与计算机的连接实物图如图 2-9 所示。

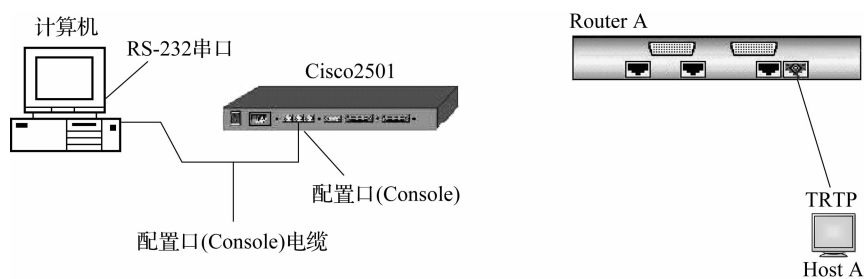


图 2-7 通过 Console 端口配置路由器

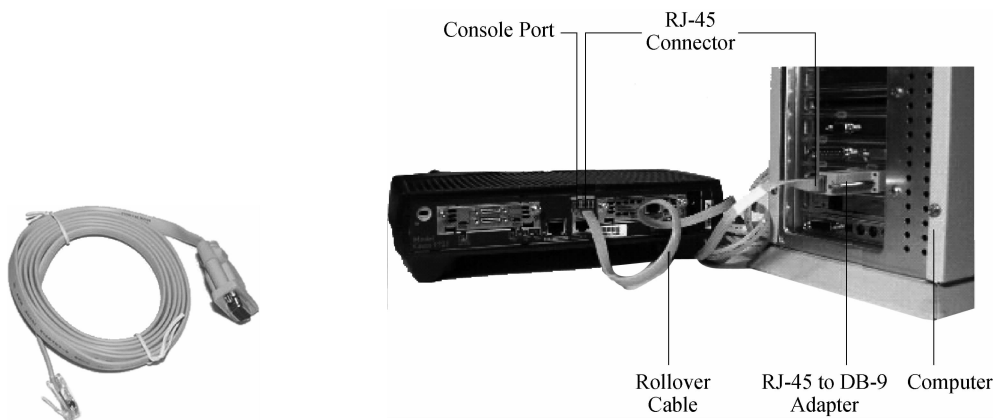


图 2-8 Console 线

图 2-9 Console 端口与计算机的连接实物图

使用 Console 端口与计算机连接后的操作为：在 Windows XP 中，执行“所有程序”→“附件”→“通讯”→“超级终端”命令，打开新建连接的“连接描述”对话框，如图 2-10 所示。设置 COM1 口时单击“还原为默认值”按钮，COM1 设置如图 2-11 所示。



图 2-10 新建连接的连接描述对话框



图 2-11 COM1 设置

通过路由器的 Console 端口管理交换机就属于带外管理,这种方式不会占用交换机的网络接口,特点是线缆特殊,需要近距离配置。第一次必须利用 Console 端口来配置路由器,使其支持 telnet 远程管理。telnet 是指路由器的网络接口,连接到网络中的某台主机。然后利用这台主机进行远程管理和配置,特点是网管可以进行远程控制。另外,还有通过 SNMP 工作站对路由器进行远程管理。路由器在出厂情况下是没有配置支持远程登录的,所以需要事先进行一定设置。

(2)AUX 端口的连接方式。如果用 Modem 之类的拨号设备进行远程访问来对路由器进行配置,就需要采用 AUX 端口。AUX 端口连接如图 2-12 所示,用 AUX 线将路由器和 Modem 进行连接。但并不是所有路由器都有 AUX 端口,所以如果是第一次配置路由器,建议使用 Console 端口配置方式。

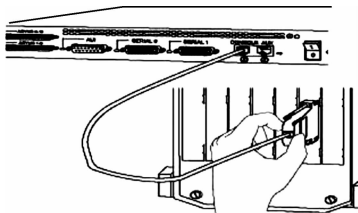


图 2-12 AUX 端口连接



2. 路由器配置命令模式说明

路由器配置中有各种命令模式,每个模式提供不同的功能。

(1)用户模式:只读模式,其中,用户可以浏览关于路由器的一些信息,但是不能进行任何更改(提示符:Router>)。

(2)特权模式:支持调试和测试命令、路由器的详细检查、配置文件的处理以及对配置模式的访问(提示符:Router#)。

(3)全局配置模式:实现强大的单行命令,这些命令执行简单的配置任务[提示符:Router(config)#]。

(4)其他配置模式:提供比较复杂的多行配置[如端口配置子模式,提示符:Router(config-if)#]。

(5)RXBOOT 模式:一种维护模式,只能进行软件升级和手工引导,也可进行路由器的口令恢复(开机 60 s 内按 Ctrl+Break 组合键,提示符:Rommon1>)。

(6)设置对话模式:新路由器开机自动进入的状态,可通过对话方式对路由器进行设置(或使用提示符:Router#setup)。

登录后进入用户模式出现提示符“Router>”,输入 enable 进入特权模式,即“Router>enable”→“Router#”(若要退回用户模式,输入 disable、exit 或 logout 命令即可)。在特权模式下输入“configure terminal”命令,进入全局配置模式,提示符是 Router(config)#(若退出,输入 exit 或 end 命令即可)。从全局配置模式输入 interface 类型编号命令,如“interface fastethernet 0”,进入接口配置模式,提示符是“Router(config-if)#”(若要退回上一级,输入 exit 命令即可)。如果从全局配置模式输入“interface ethernet 0/0.1”,则进入子接口配置模式“Router(config-subif)#”。从全局配置模式,输入 LINE 类型编号命令“Router(config-line)#”,则进入线路配置模式。从全局配置模式输入 Router 类型命令,如“router rip”,则进入路由协议配置模式“Router(config-router)#”。路由器配置模式表如表 2-4 所示。

表 2-4 路由器配置模式表

配置模式	提示符	进入命令
用户模式	Router>	—
特权模式	Router#	enable
全局模式	Router(config)#	configure terminal
线路配置模式	Router(config-line)#	line vty start-number end-number
路由配置模式	Router(config-router)#	router rip
接口配置模式	Router(config-if)#	Interface f 1/1

3. 配置命令介绍

1) 获得帮助

输入“?”,可以列出该命令模式下支持的全部命令列表,可以列出相同字母开头的命令关键字,或者每个命令的参数信息。

Router>? ; 列出用户模式下的所有命令
 Router#? ; 列出特权模式下的所有命令
 Router>t? ; 列出用户模式下所有以 t 开头的命令
 Router# show? ; 列出用户模式下 show 命令后附带的参数
 Router# show fl 用<Tab>键 ; 自动补齐 fl 后的剩余字母
 Router# show configuration ? ; 列出该命令的下一个关联的关键字

2) 支持命令简写

只要输入命令关键字的一部分字符,并且能够识别唯一的命令关键字即可,如“Show startup-config”可写成“Router# show star”。

3) 检查路由器状态的命令

路由器显示组成如图 2-13 所示,路由器显示命令如表 2-5 所示,通过它们,可以检查路由器的各项状态。

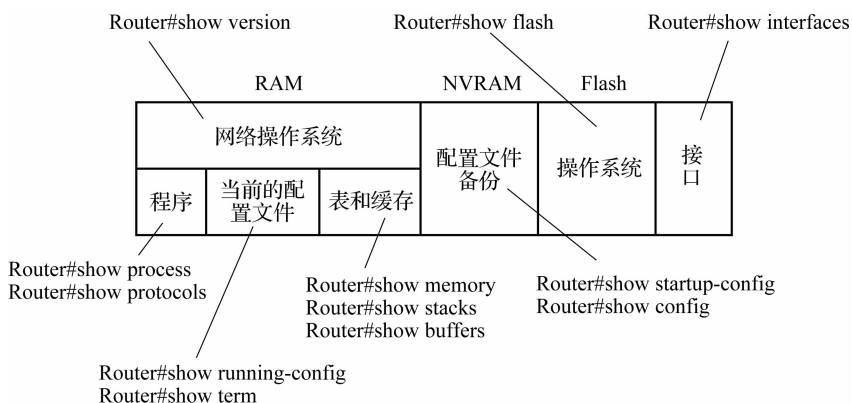


图 2-13 路由器显示组成部分

表 2-5 路由器显示命令表

命 令	含 义
show version	显示系统硬件的配置、软件版本、配置文件的名称和来源以及自举映像
show process	显示处于激活状态的进程的相关信息
show protocols	显示所配置的协议。这条命令显示任何配置的网络层的协议状态
show memory	显示有关路由器内存的统计数字,其中包括内存空闲槽的统计数字
show stacks	监控和中断程序对堆栈的使用
show buffers	显示关于路由器缓冲槽的统计数字
show flash	显示关于快闪存储器内存设备的信息
show running-config	显示激活的配置文件(RAM中)
show startup-config	显示备份的配置文件(NVRAM中)



续表

命 令	含 义
show interfaces	显示在路由器上所配置的所有接口的统计数字
show ip route	显示路由表
show clock	显示时钟

4) 路由器基本设置命令

路由器的一些基本设置命令比较重要,需要记忆掌握,路由器基本设置命令如表 2-6 所示。

表 2-6 路由器基本设置命令

命 令	含 义
configure terminal	全局配置模式
hostname <i>name</i>	设置路由器名
username <i>username</i> password <i>password</i>	设置访问用户及密码
enable password <i>password</i>	设置特权口令
enable secret <i>secret</i>	设置特权密码
interface <i>type slot /number</i>	进入端口设置
ip address <i>address subnet-mask</i>	设置端口 IP 地址
no shutdown	激活端口
line console 0	设置 Console 口
line vty 0 n	设置虚拟终端 vty
password <i>password</i>	设置登录密码
login [<i>local</i>]	启动登录进程
clock set	设置时钟

任务实施

一、常规配置

假设某单位设备机房的路由器进行了初次配置后,管理员希望以后在办公室或其他地方也可以对设备进行远程管理,现在要对路由器进行适当配置,使管理员可以实现这一功能。

将本任务的路由器命名为 RouterB。1 台 PC 通过串口连接到路由器的控制(Console)端口,同时通过网卡连接到路由器的 fastethernet 0 端口,路由器与计算机连接如图 2-14 所示。假设 PC 的 IP 地址为 192.168.0.15,配置路由器的 fastethernet 0 端口的 IP 地址为 192.168.0.16,子网掩码都是 255.255.255.0。

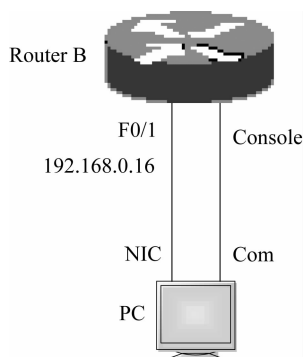


图 2-14 路由器与计算机连接图

在路由器上配置 telnet。

(1) 配置端口地址。

```
Router # configure terminal ; 进入全局配置模式
```

```
Router(config) # hostname RouterB ; 配置路由器名称为 RouterB
```

```
RouterB(config) # interface fastethernet 1/0 ; 进入路由器接口配置模式
```

```
RouterB (config-if) # ip address 192.168.0.16 255.255.255.0
```

```
RouterB (config-if) # no shutdown ; 开启路由器 f 1/0 接口
```

在配置端口地址之后,可以输入下面两条命令来查看路由器接口 fastethernet 1/0 的 IP 地址已经配置和开启的情况。

```
RouterB # show ip interface fastethernet 1/0
```

```
RouterB # show ip interface brief
```

(2) 配置远程登录密码。

```
RouterB(config) # line vty 0 4 ; 进入路由器线路配置模式
```

vty 线路指的是进行 telnet 时使用的线路。这里的“0 4”指的是对第一个 telnet 线路到第五个 telnet 线路进行设置。

```
RouterB(config-line) # login ; 配置远程登录
```

```
RouterB(config-line) # password zjx ; 设置路由器远程登录密码为 zjx
```

```
RouterB(config-line) # end
```

此步设置完后,可以验证通过网线是否从 PC 远程登录到路由器上。

```
C:\>telnet 192.168.0.16 ; 从 PC 登录到路由器上
```

(3) 配置路由器特权模式密码。

```
RouterB(config) # enable secret zjx ; 设置路由器特权模式密码为 zjx
```

或者 RouterB(config) # enable password zjx

(4) 保存在路由器上所进行的配置。

```
RouterB# copy running-config startup-config ; 保存路由器配置
```

或者

```
RouterB# write memory
```

(5) 验证路由器配置已保存。



```
RouterB# show startup-config
```

(6)删除配置文件。

```
RouterB# delete flash:config.text
```

二、Packet Tracer 6.0 软件的使用

1. 软件界面及功能介绍

Packet Tracer 软件是 Cisco 公司提供的—个辅助学习工具,为学习思科网络技术的初学者设计、配置、排除网络故障提供了网络模拟环境。用户可以使用最简单的方式建立网络拓扑,并且可以观察数据包在网络中的详细处理过程,了解网络实时运行情况。最重要的是可以学习 OSI 的配置,掌握故障排查能力。打开 Packet Tracer 6.0 软件进入其初始界面,如图 2-15 所示。

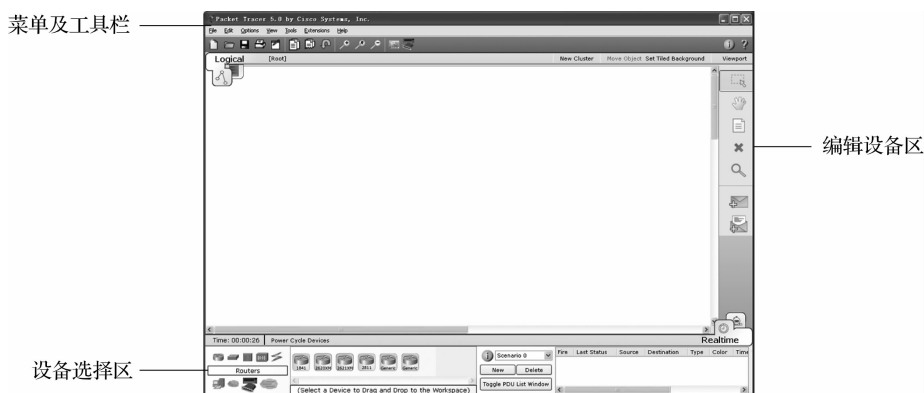


图 2-15 Packet Tracer 6.0 软件的初始界面

Packet Tracer 6.0 软件的界面非常简洁,方便用户使用。初始界面主要分为三个区域:菜单及工具栏、编辑设备区、设备选择区。界面左下角的设备选择区中,包括路由器、交换机、集线器、无线设备、连线、终端设备、广域网仿真、用户自定义设备几个选项。例如,选中 Routers(路由器),右侧出现多款思科的常用路由器供选择,如图 2-16 所示。

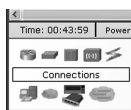


图 2-16 Packet Tracer 6.0 的设备选择区

选择 Connections 后,右侧会出现各种类型的连线,如图 2-17 所示,包括控制线、直通线、交叉线、光纤、电话线等。



图 2-17 连线的种类

菜单栏和工具栏主要提供一些基本的操作,如新建、打开、保存等,与其他软件风格类似。而如果对设备进行编辑,则可以在右边区域进行选择,对设备进行选定、移动、删除、检查等操作。如果记不住图标的作用也没关系,只要把鼠标放在图标上,就可以显示该图标的作用。

2. 常用设备管理配置

1) PC 的管理

PC 的配置比较简单,可以给 PC 任意添加或删除端口,PC 模块选择如图 2-18 所示。所需要配置的内容也比较少,PC 的配置如图 2-19 所示。例如,IP 地址、网关、子网掩码、浏览器等设置,在其中均可根据需要进行设置。

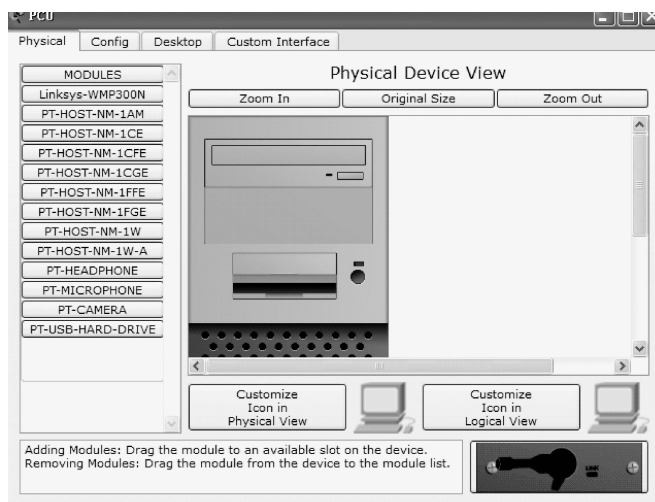


图 2-18 PC 模块选择

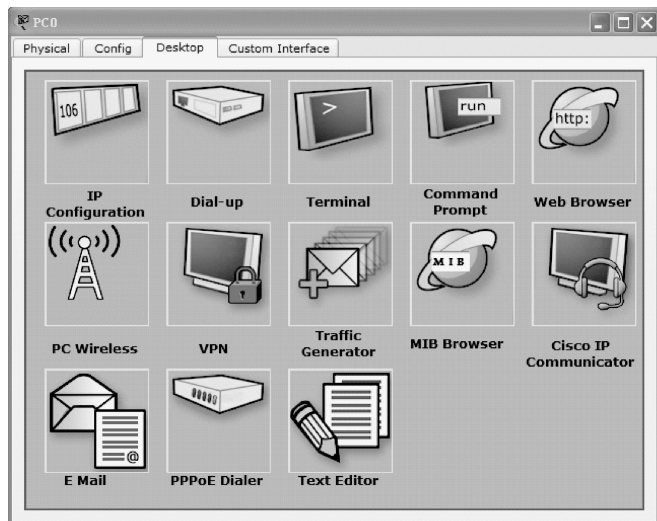


图 2-19 PC 的配置



2)路由器的配置

下面重点介绍路由器的配置。首先选择一款思科的路由器，然后进入其配置界面，如图 2-20 所示。左上角有 3 个标签:Physical、Config、CLI。

在 Physical 里选择 MODULES(模块)，会有许多模块供选择，最常用的是 WIC-1T 和 WIC-2T 两个广域网串口模块。可以添加到右侧的路由器图片的空槽里，前提是要关上电源开关，添加后要打开电源开关，使路由器工作。在 Config 中可以设置路由器的显示名称、主机名称等，而在 CLI(command line interface)中可以通过命令行的方式进行路由器设置。

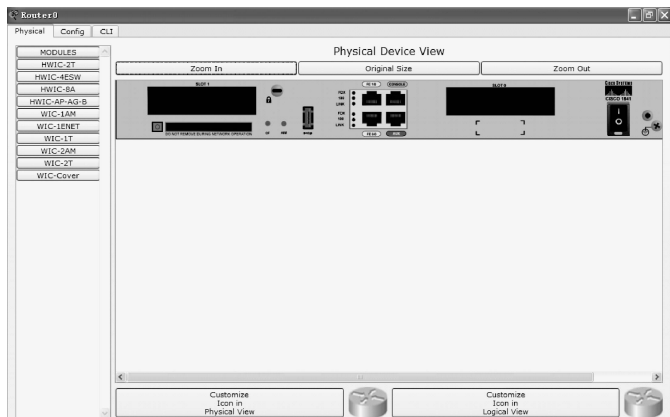


图 2-20 路由器配置界面

3)交换机的基本使用配置方法

(1)模式的选择及命名。在 Config 或 CLI 下都可以进入特权模式 switch #、全局配置模式 switch(config) #、端口配置模式 switch(config-if) #，交换机模式进入及名称命名如图 2-21 所示。

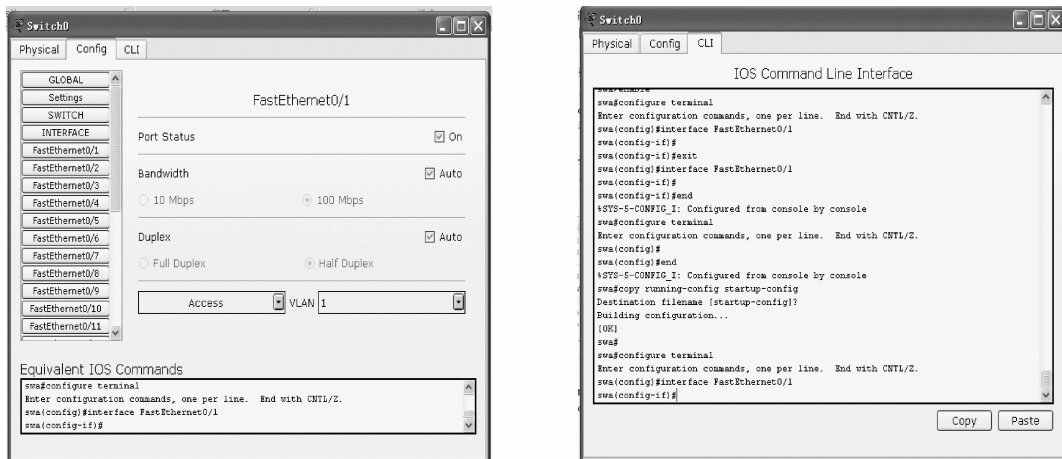


图 2-21 交换机模式进入及名称命名

(2)查看信息。通过 show version、show flash、show mac-address-table 等命令查看各项信息。交换机的信息查询如图 2-22 所示。

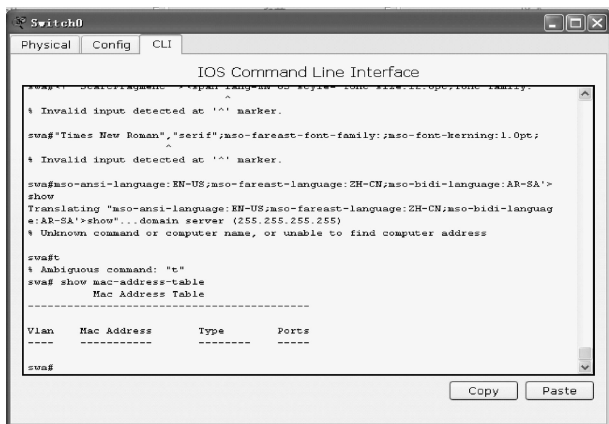


图 2-22 交换机信息查询

(3) 密码设置。可以设置 Console 端口连接设备及 telnet 远程登录所需要的密码，密码设置如图 2-23 所示。

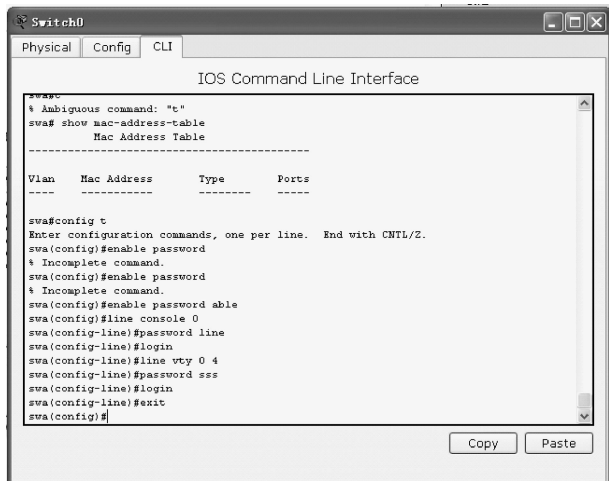


图 2-23 密码设置

3. 单个路由器的配置

利用 Packet Tracer 软件来学习路由器的配置以及 IOS 命令非常方便，从单个路由器的配置入手进行学习掌握。

首先，绘图完成计算机与单个路由器的连接。选择路由器(2811)后添加所需要的模块，模块添加如图 2-24 所示。注意，在添加模块之前要将电源关闭，添加完之后再打开。添加完所需模块后，可以添加一台计算机，然后通过 RS-232 口与路由器的 Console 端口进行连接。路由器与计算机连接如图 2-25 所示。

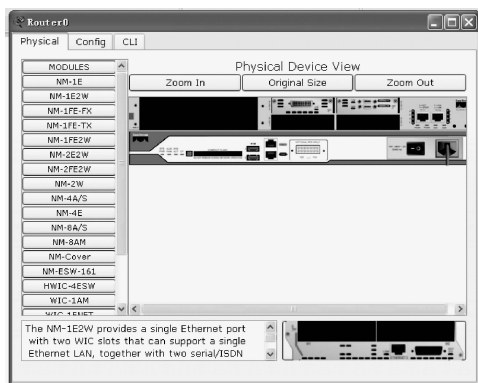


图 2-24 模块添加

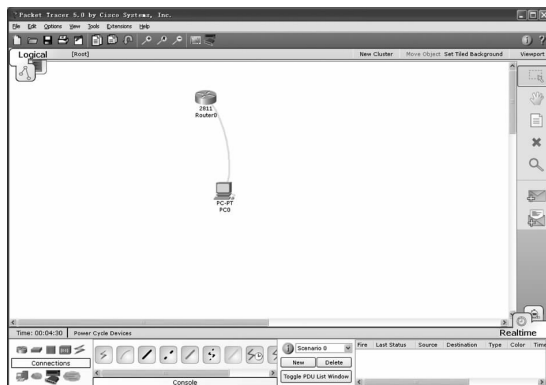


图 2-25 路由器与计算机连接

路由器有多种模式,包括用户模式、特权模式、全局模式、接口配置模式、子接口配置模式、线路配置模式、路由配置模式等。具体命令在前面已进行过介绍,可自行查询输入操作。本操作需更改路由器的名称为 RouterB。另外,还要设置 Console 登录密码,查看路由器接口的 IP 信息等。

4. 静态路由配置

路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径,并将该数据有效地传送到目的站点,所以最佳路径的选择——路由算法是路由器的关键。这项工作是由路由器中的路径表(routing table)完成的,路径表内保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等各种传输路径的相关数据,供路由选择时使用。路径表可以由系统管理员固定设置,也可以由系统动态修改,可以由路由器自动调整,也可以由主机控制。

静态路由是指由用户或管理员手工配置路由信息。当网络的拓扑结构或链路的状态发生变化时,管理员需要手工修改路由表中相关的路由信息。静态路由的信息在默认情况下是私有的,不会传递给其他路由器。当然也可以使之成为共享的。静态路由一般适用于比较简单的网络环境,因为网络管理员比较容易弄清楚网络的拓扑结构,便于设置正确的路由信息。

静态路由除了具有简单、高效、可靠的优点外,还具有很高的网络安全保密性。动态路由需要路由器之间频繁交换各自的路由表,对路由表的分析可以揭示很多信息。因此,出于安全方面的考虑,网络也可以采用静态路由。而且因为静态路由不会产生更新流量,所以不占用网络带宽。

在 Packet Tracer 软件上构建静态路由配置网络拓扑图,两台路由器的静态路由配置拓扑图如图 2-26 所示。

在使用软件配置时,可以在 Config 中设置,也可以在 CLI 中输入命令配置。在 CLI 中的配置过程如下。

先更改两台路由器的名称,分别是 RouterA 和 RouterB。两台路由器通过 serial 0/0/0 口进行连接,路由器与计算机之间通过 fastethernet 口连接。

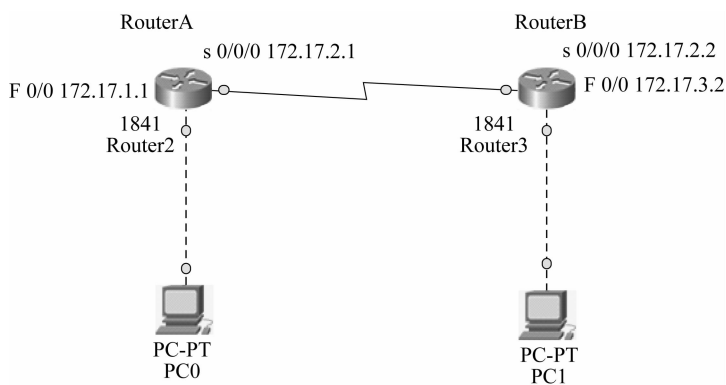


图 2-26 两台路由器的静态路由配置拓扑图

```
RouterA(config) # interface fastethernet0/0
RouterA(config-if) # ip address 172.17.1.1 255.255.255.0
; 设置 RouterA 的 fastethernet 0/0 地址和子网掩码
RouterA(config-if) # no shutdown ; 打开 fastethernet 0/0,此句一定不要丢掉
RouterA(config-if) # exit
RouterA(config) # interface serial0/0/0 ; 设置串口 serial 0/0/0
RouterA(config-if) # ip address 172.17.2.1 255.255.255.0
RouterA(config-if) # clock rate 64000 ; 设置串口的时钟
RouterA(config-if) # no shutdown ; 打开串口,一定不要丢掉此句
根据对 RouterA 的设置,再对 RouterB 进行同样的设置。
```

```
RouterB(config) # interface fastethernet 0/0
RouterB(config-if) # ip address 172.17.3.2 255.255.255.0
RouterB(config-if) # no shutdown
RouterB(config-if) # exit
RouterB(config) # interface serial 0/0/0
RouterB(config-if) # ip address 172.17.2.2 255.255.255.0
RouterB(config-if) # no shutdown
RouterA(config) # ip route 172.17.3.0 255.255.255.0 172.17.2.2
; 在路由器 RouterA 上进行静态路由配置。这句话的意思是: 路由器见到目的网段为
172.17.3.0 的数据包,就将数据包发送到 172.17.2.2 上
RouterB(config) # ip route 172.17.1.0 255.255.255.0 172.17.2.1
; 在路由器 RouterB 上进行静态路由配置
```

通过 config 标签也可以进行设置,过程更容易,但需要认真仔细,尤其是各接口一定要设置为打开状态。设置完后,如果网络是连通的,则各连接点从红色变成绿色,并且可以在虚拟 PC 上测试互通,利用控制台测试互通性,如图 2-27 所示。在 PC0 上的 Command Prompt 下输入 PC> ping 172.17.3.33,或者在 PC1 上的 Command Prompt 下输入 PC> ping 172.17.1.22。

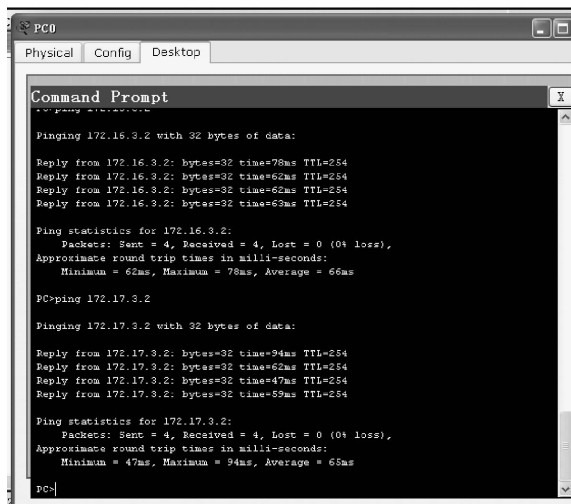


图 2-27 利用控制台测试互通性

5. 两台路由器动态路由配置

动态路由是指利用路由器上运行的动态路由协议,定期与其他路由器交换路由信息,从而根据从其他路由器上学习到的路由信息,自动建立起自己的路由。常用的协议有 RIP 路由信息协议、IGRP 内部网关路由协议、OSPF 开放式最短路径优先协议、IS-IS 中间系统-中间系统协议、EIGRP 增强型内部网关路由协议、BGP 边界网关协议。这些协议可以分成两类,即外部网关协议(EGP)和内部网关协议(IGP)。在自治系统之间交换路由选择信息的互联网络协议是外部网关协议。在自治系统内交换路由选择信息的路由协议是内部网关协议,常用的有 OSPF、RIP、IGRP、EIGRP、IS-IS 等。

这里利用 RIPv2 协议和 OSPF 协议进行动态路由配置。RIP 协议有 v1(有类)、v2(无类)两个版本,一般建议使用 v2 版本。首先在 Packet Tracer 软件上绘制网络连接拓扑图,这里采用上一个拓扑结构图,两台路由器的静态路由配置拓扑图见图 2-26。在 RouterA 的 CLI 上输入的语句如下。

```
RouterA(config)# interface fastethernet 0/0
RouterA(config-if)# ip address 172.17.1.1 255.255.255.0
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# interface serial 0/0/0
RouterA(config-if)# ip address 172.17.2.1 255.255.255.0
RouterA(config-if)# clock rate 64000
RouterA(config-if)# no shutdown
```

此部分与前面静态路由的设置相同,但在 RouterA 上的动态路由配置就不同了。

```
RouterA(config)# router rip
RouterA(config-router)# version 2
RouterA(config-router)# network 172.17.0.0
```


在 RouterB 上的配置依此进行即可,在此不重复操作了。设置完成后可测试互通性。利用 OSPF 进行路由配置的方法为绘制网络拓扑结构图,如图 2-28 所示。命令输入与前面类似,不同之处是在路由配置方面。

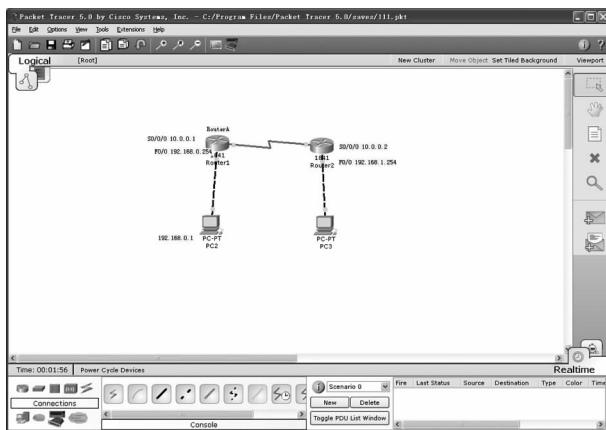


图 2-28 网络拓扑图

RouterA 上的输入命令如下。

```
RouterA(config) # interface fastethernet 0/0
RouterA(config-if) # ip address 192.168.0.254 255.255.255.0
RouterA(config-if) # no shutdown
RouterA(config-if) # exit
RouterA(config) # interface serial 0/0/0
RouterA(config-if) # ip address 10.0.0.1 255.0.0.0 255.0.0.0
RouterA(config-if) # clock rate 72000
RouterA(config-if) # no shutdown
```

RouterB 上的输入命令如下。

```
RouterB(config) # interface fastethernet 0/0
RouterB(config-if) # ip address 192.168.1.254 255.255.255.0
RouterB(config-if) # no shutdown
RouterB(config-if) # exit
RouterB(config) # interface serial 0/0/0
RouterB(config-if) # ip address 10.0.0.2 255.0.0.0
RouterB(config-if) # no shutdown
```

动态路由由 OSPF 配置要在全局模式(config)#下进行。

RouterA 上的命令如下。

```
RouterA (config) # route ospf 10
RouterA (config-router) # network 192.168.0.0 0.0.0.255 area 0
RouterA (config-router) # network 10.0.0.0 0.255.255.255 area 0
RouterA (config-router) # end
RouterA # write
```



PC 的配置如下。

PC0 的 IP 设为 192.168.0.1 255.255.255.0

PC1 的 IP 设为 192.168.1.1 255.255.255.0

任务三 如何连接 Internet



任务分析及任务目标

前面介绍了局域网的组建过程以及交换机、路由器等设备的配置方法,然而一个组织中如果仅仅有局域网肯定是不够的。无论是对商业的需要,还是对信息资源的渴求及广度交流的愿望,都促使人们在更大范围内相互连接形成全球性的网络——因特网(Internet)。如何将家庭的计算机和企事业单位的局域网接入 Internet 是我们重点研究的内容。在接入后如何使局域网内的终端都能共享 Internet? 这就需要代理服务器技术。



相关知识链接

接入 Internet 的方式非常多,技术的进步使上网方式变得越来越简单、越来越快速。虽然很多以前的上网方式早已不再使用,但是能够了解、回忆一下那些曾经的 Internet 接入方式,会让读者对目前的网络有一个更清楚的认识和感受。下面就来简单了解一下那些曾经和目前正在使用的 Internet 接入方式。

1. 拨号上网

20 世纪 90 年代,上网需要 Modem(调制解调器)和电话线支持。输入某个 ISP 服务商的账号和密码就能上网,不用到电信部门办理。但速度非常慢,理论上只有 56 kb/s;按小时收费,没有包月;线路不稳定,容易掉线;上网时还占用电话线路,如有人打电话会听到忙音。这种方式很快就不再使用了。

2. ISDN

ISDN(综合业务数字网)也曾经短暂地存在过一段时间,速度比拨号上网快,可以实现电话、传真、数据在同一线路上的传输,所以一对电话线可以连接几个不同的终端,如电话机、计算机、传真机等,俗称为一线通。但 ISDN 的速度依然不是很理想,满足不了日益发展的网络需要,所以它也很快退出了家庭上网的市场。

3. ADSL

ADSL(asymmetric digital subscriber line,不对称数字用户线路)是目前广泛使用的上网方式。很多家庭都依赖于这种方式上网。它以普通电话线为传输介质,实现了上下行不同的传输速率。因为上行和下行带宽不对称,因此称为不对称数字用户线路。它采用频分复用技术把普通的电话线分成了电话、上行和下行 3 个相对独立的信道,从而避免了干扰。也就是说,即使一边打电话一边上网,也不会发生上网速率和通话质量下降的情况,这在拨号上网方式中是不可能的。在用户端,需要使用一个 ADSL 终端来连接电话线路。由于 ADSL 使用高频信号,电话线中还有低频的电话音频信号,所以在两端还都要使用 ADSL 信号分离器将 ADSL 数据信号和普通音频电话信号分离开来,避免打电话时出现噪声干扰。

ADSL 通常提供 3 种网络登录方式:桥接、PPPoA(PPPoVerATM,基于 ATM 的端对端协议)、PPPoE(PPPoVerEthernet,基于以太网的端对端协议)。桥接直接提供静态 IP,而后两种通常不提供静态 IP,是动态地给用户分配网络地址。所以在家里用 ADSL 上网,每次的 IP 地址都是不同的。

ADSL 比较成熟,其带宽较大、连接简单、投资较小,所以发展很快。但从技术角度看,ADSL 对宽带业务来说也只能是一种过渡性方法。当然,局域网也可以通过 ADSL 实现上网,ADSL 上网方式如图 2-29 所示。

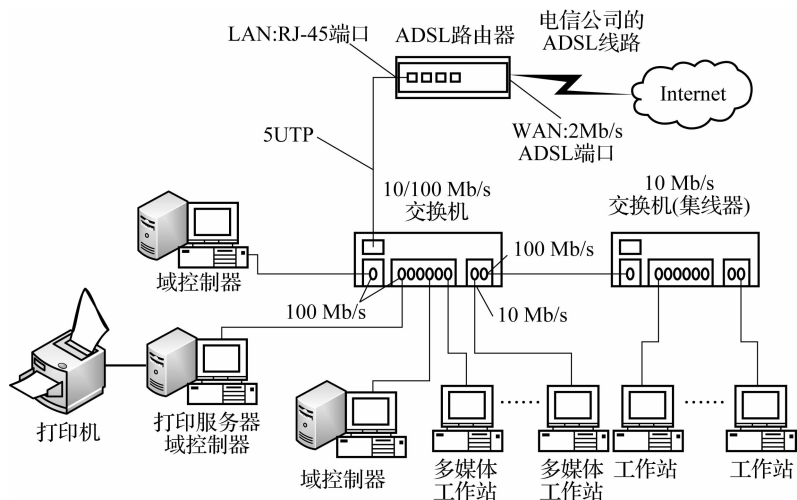


图 2-29 ADSL 的上网方式

4. DDN 专线

DDN(digital data network,数字数据网)是利用光纤、微波、卫星等数字传输通道和数字交叉复用节点组成的数据传输网。它具有传输质量好、速率高、网络时延小等特点,适合于计算机主机之间、局域网之间、计算机主机与远程终端之间的大容量、多媒体、中高速通信的需要,是我国的中高速信息“国道”。组成 DDN 的基本单位是节点,节点间通过光纤连接,构成网状的拓扑结构,用户的终端设备通过数据终端单元(DTI)与就近的节点机相连。DDN 的主要作用是向用户提供永久性和半永久性连接的数字数据传输信道,既可用于计算机之间的通信,也可用于传送数字化传真、数字话音、数字图像信号或其他数字化信号。永久性连接的数字数据传输信道是指用户间建立固定连接、传输速率不变的独占带宽电路。半永久性连接的数字数据传输信道对用户来说是非交换性的,但用户可提出申请,由网络管理人员对其提出的传输速率、传输数据的目的地和传输路由进行修改。网络经营者向广大用户提供了灵活方便的数字电路出租业务,供各行业构成自己的专用网。DDN 在民航、银行联网等专业行业有着广泛的应用,非常适合于业务量大、实时性强的用户。

5. FTTx+LAN

FTTx+LAN 技术是一种利用光纤加超 5 类网络线方式实现宽带接入的方案,可以实现千兆光纤到小区(大楼)中心交换机,再用百兆光纤或超 5 类网络线连接中心交换机和楼道交换机,楼道内采用综合布线。用户上网速率可达 10 Mb/s,网络可扩展性很强,投资规



模比较小。现在还有光纤到办公室、光纤到户(FTTH)、光纤到桌面等多种接入方式满足不同用户的需求。因 FTTx 接入方式成本较高,就我国目前的综合国情而言,将 FTTx 与 LAN 结合,可以大大降低接入成本,同时可以提供高达 100 Mb/s 的用户端接入带宽,是目前及将来比较理想的 Internet 接入方式。所以光纤到小区(FTTC)、光纤到大楼(FTTB)的应用方式更为常见。

例如,光纤接到大楼中的一个路由器或交换机上,然后楼中的所有用户也都接到交换机上,这样所有用户就都能连接到 Internet。FTTx+LAN 的接入方式将逐渐取代 ADSL 接入方式。在很多大城市的居民小区已经进行了宽带改造,实现了光纤到小区,甚至光纤到楼层。

随着网速的提升,远程医疗、远程教学、视频点播等应用会越来越广泛。而原来的有线电视提供商也发现了这方面的商机,近几年也大力推广 Cable Modem 接入上网方式,即有线宽带上网。其实际的速度与 ADSL 相近,但稳定性和安全性不足。

任务实施

一、FTTC+LAN 或 FTTB+LAN 实现局域网接入 Internet

将电信部门的光纤接到大楼或小区的进线间,在进线间安装有配置 1 000 Mb/s 光纤模块的交换机,也可以使用光纤收发器加普通交换机的方式。FTTx+LAN 接入方式如图 2-30 所示。光纤收发器是将光信号转换为电信号的设备,如图 2-31 所示。

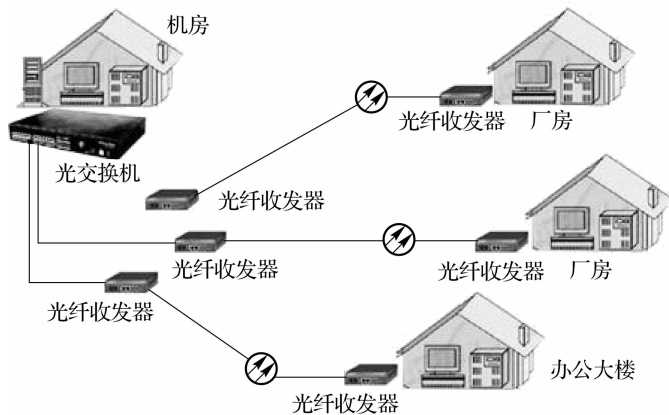


图 2-30 FTTx+LAN 接入方式



图 2-31 光纤收发器

将光纤插入光纤收发器的光纤口,再用一根双绞线(6类或超5类)连接光纤收发器与交换机。如果局域网规模比较大,就不能使用上面的方法,而应该采用光纤收发器与企业级路由器及交换机连接上网的方式,光纤路由器的上网方式如图 2-32 所示。这种方式是用户自己拥有一台具备 NAT 功能的企业级路由器。

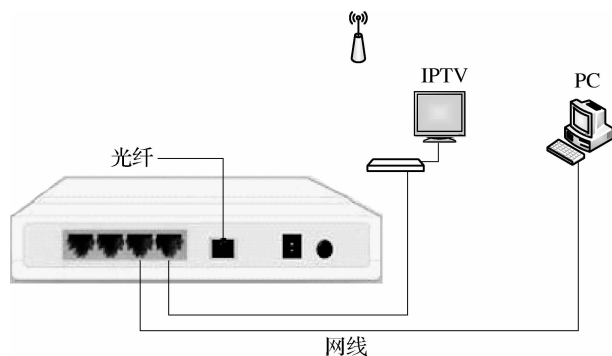


图 2-32 光纤路由器的上网方式

二、利用 ADSL+LAN 实现局域网接入 Internet

前面已经介绍了家庭无线局域网的组建方式,在此就不过多讲解和实际操作了。多 PC 通过路由器共享 ADSL 上网如图 2-33 所示,为了避免 ADSL Modem 自带的的路由功能无法实现,可以采用 ADSL Modem+宽带路由器+交换机的上网方式。

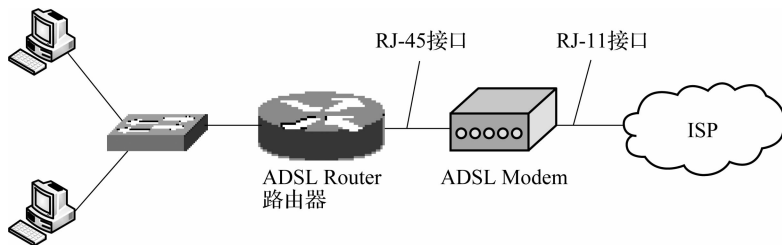


图 2-33 多 PC 通过路由器共享 ADSL 上网

三、代理服务器上网

1. 代理服务器上网简介

代理服务器不是接入技术而是一种技术功能。代理服务器(proxy server)是网上提供转接功能的服务器,一般情况下,在使用网络浏览器直接连接 Internet 站点获得网络信息时,是连接到目的站点服务器,然后再由目的站点服务器把信息传送回来。代理服务器是介于客户端和 Web 服务器之间的另一台服务器,有了它之后,PC 不是直接到 Web 服务器去取回网页,而是向代理服务器发出请求,信号会先送到代理服务器,由代理服务器取回 PC 所需要的信息并传送到 PC,代理服务器上网如图 2-34 所示。

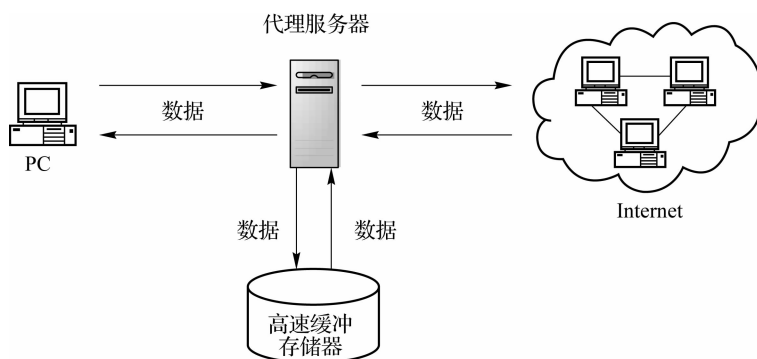


图 2-34 代理服务器上

例如,用户想访问的目的网站是甲,由于某种原因不能访问到网站甲或者不想直接访问网站甲,此时就可以使用代理服务器,在实际访问网站时,PC 会自动先访问代理服务器,然后代理服务器将用户转接到目标网站。代理服务器有什么作用呢? 首先它可以提高访问速度。因为通常代理服务器都设置了一个较大的缓冲区,可以存储一定信息。其他用户再访问相同信息时,可以直接从缓冲区中取出信息传给用户,提高了访问速度。其次可以隐藏真实身份。上网者也可以通过代理服务器隐藏自己的真实地址信息,防止被攻击。另外还具有突破某些网站访问限制的作用。

2. 使用局域网代理服务器软件(Sygate)

1)项目所需设备准备

- 装有 Windows XP 操作系统的 PC 3 台。
- 代理服务器 1 台(双网卡)。
- 交换机 1 台。
- ADSL Modem 1 台。
- 直通线 5 根。
- 代理软件 Sygate Home Network 4.5 中文版 1 套。

2)网络拓扑结构图

代理服务器上网的网络拓扑结构图如图 2-35 所示。

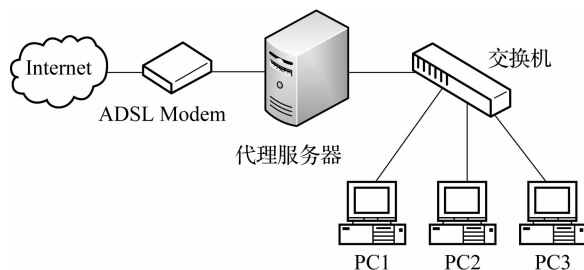


图 2-35 代理服务器上网的网络拓扑结构图

3)硬件连接

- (1)用直通双绞线将 PC1、PC2、PC3 和代理服务器的网卡 1 连接到交换机上。

(2)用直通双绞线连接 ADSL Modem 的 Ethernet 端口和代理服务器的网卡 2。

(3)打开 ADSL Modem 和交换机的电源,如果 ADSL Modem 上的 LAN-Link 指示灯亮,表明 ADSL Modem 与代理服务器连接成功;如果交换机相应的 LAN 端口指示灯亮,表明计算机和代理服务器与交换机连接成功。

(4)代理服务器接入 Internet。在代理服务器中,建立并进行虚拟拨号,接入 Internet。也可通过其他方法接入 Internet。

(5)安装完 Sygate 后进行 Sygate 服务器的配置。

①进入 Sygate 管理主窗口。执行“开始”→“所有程序”→Sygate Home Network→“Sygate 管理器”命令,进入 Sygate 管理主窗口,如图 2-36 所示。

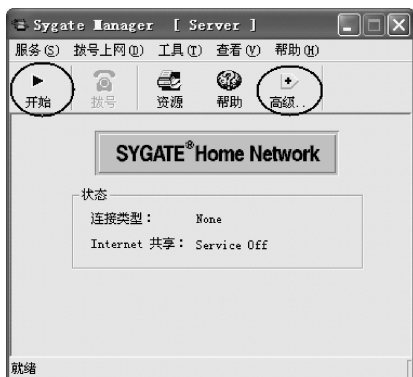


图 2-36 Sygate 管理主窗口

②单击工具栏中的“开始”按钮,启动 Sygate 代理服务。单击“高级”按钮,打开 Sygate 高级特性管理窗口。“状态”区域显示“连接类型: High-Speed Connection Internet 共享: Online”,窗口右下角的指示灯显示绿色,“网络流量信息”区域显示信息传输状况,“INTERNET接口状态”区域显示线路、用户、连接 Internet 网卡情况。显示信息如图 2-37 所示。

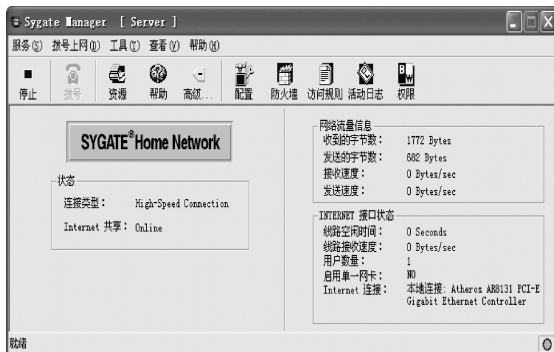


图 2-37 显示信息

③有时由于某种原因,需要暂停 Sygate 代理服务,暂停服务的方法是:在 Sygate 高级特性管理窗口中,单击工具栏左边的“停止”按钮或执行“服务”→“停止”菜单命令,弹出提示框,询问是否暂停 Sygate 服务,单击“是”按钮。此时“状态”区域显示“连接类型: None

Internet共享:Service Off”,同时窗口右下角的指示灯变为红色。

④配置网卡。如果 Sygate 代理服务器只有两块网卡,在安装 Sygate 时会自动配置。在 Sygate 的高级特性管理窗口中,单击“配置”按钮,打开“配置”对话框,如图 2-38 所示。配置完毕后,单击“确定”按钮,重新启动服务使配置生效。

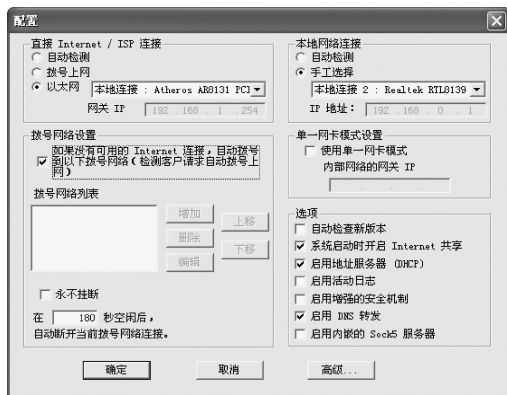


图 2-38 配置单一网卡的 Sygate

⑤自动启动 Sygate 服务。在“配置”对话框中,选中“系统启动时开启 Internet 共享”复选框,单击“高级”按钮,弹出“高级设置”对话框,如图 2-39 所示。

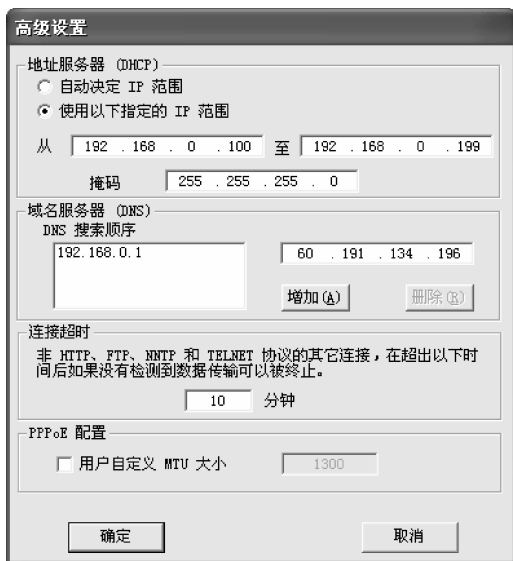


图 2-39 高级设置

⑥管理 Sygate 的黑名单。黑名单,即不允许这些用户在指定的时间访问指定的站点,而其他用户则无此限制,这里的指定时间和指定站点可以是全部时间和全部站点。下面将以禁止 IP 地址为 192.168.0.100 的用户在每周一的 9:00~周三的 9:00 期间上网为例进行说明,黑名单管理如图 2-40 所示。



图 2-40 黑名单管理

⑦管理 Sygate 的白名单。白名单,即在 Sygate 代理服务器中,允许这些用户在指定的时间访问指定的站点,这里的指定时间和指定站点可以是全部时间和全部站点。Sygate 的白名单与黑名单类似,它们是相互对应的,但黑名单的优先级要高些,例如,在白名单中允许的设置,只要在黑名单中禁止,则 Sygate 将采用黑名单中的设置。

⑧Sygate 客户端的设置。一般不必在 workstation 安装 Sygate 的客户端软件,安装只是为了增加诊断和特殊管理功能。客户端设置比较简单。最简单的办法是将“TCP/IP 属性”设置为“自动获得 IP 地址”。如果进行手工配置,客户端的 IP 地址和代理服务器连接局域网网卡的 IP 地址要在同一网段,网关指向代理服务器连接局域网网卡的 IP 地址,DNS 服务器配置为 Internet 上的 DNS 服务器或代理服务器连接局域网网卡的 IP 地址。

⑨用 ping 命令或访问网页的方式,测试 PC1、PC2、PC3 客户机是否可以访问 Internet。

项目归纳总结

本项目以实现局域网接入 Internet 为目的,对子网划分、路由器的配置和使用、局域网接入广域网的方式等内容进行了详细的介绍和任务实施。通过对子网划分的练习应该明确子网划分的目的和意义,熟练掌握子网划分的方法。重点在于会根据子网数来划分子网,也能够通过主机数来划分子网。路由器的配置是本项目的重点。应该掌握包括路由器在内的网络设备的基本操作和配置命令,掌握不同网络协议在设备接口的配置加载。重点掌握静态路由配置、动态路由配置的方法。熟练掌握 Packet Tracer 软件的使用,尤其是交换机、路由器、PC 的设置方法和过程。学会拓扑结构的构建和命令语言的编写。应当掌握常见的局域网接入 Internet 的方式,尤其是 FTTx+LAN 方式。



知识与能力考核

课程名称:网络与综合布线系统工程技术		授课地点:		
项目二:连接 Internet		授课教师:	授课学时:	
课程性质:理实一体课程		综合评分:		
知识掌握情况评分(35分)				
序号	知识考核点	教师评价	配 分	实际得分
1	掌握子网划分的目的和意义		5	
2	掌握子网划分的方法和计算过程		10	
3	掌握路由器的静态路由配置方法		10	
4	掌握路由器的动态路由配置方法		5	
5	掌握局域网接入 Internet 的方法		5	
工作任务完成情况评分(65分)				
序号	能力操作考核点	教师评价	配 分	实际得分
1	能够正确计算和确定子网划分方案		15	
2	能够正确配置静态路由		15	
3	能够熟练使用 Packet Tracer 软件		25	
4	能够正确配置动态路由		5	
5	能够正确实现局域网接入 Internet		5	
违规扣分(50分)				
序号	违规内容	教师评价	配 分	实际扣分
1	设备、仪器、仪表损坏		10	
2	课上不参与小组工作		15	
3	严重旷课、缺课		15	
4	严重干扰课堂秩序		10	



自测题

1. 子网划分的目的和意义是什么?
2. 什么是子网掩码? 子网掩码的作用是什么?
3. 简述子网划分的步骤和计算方法。

4. 详细说明 A、B、C 三类网络 IP 的地址范围。
5. 学习 IPv6 相关技术,并撰写报告。
6. 简述路由器的启动过程。
7. 路由器有几种模式? 分别是什么? 如何进入这几种模式?
8. 简述路由器的工作原理。
9. 练习使用 Packet Tracer 软件,并进行路由器的静态路由配置。
10. 局域网接入 Internet 有几种方式? 画图并进行详细说明。

项目三

网络的测试与诊断

项目综述

一个局域网已经组建完成,并且已经连接到了 Internet 上,接下来的工作就是让这个网络起作用,让它发挥应有的功能。计算机之间形成网络,涉及了硬件、软件的很多内容,因此难免会出现问题和故障,这就需要利用合理的方法和手段进行分析和诊断。同时为了保障网络的正常运行,需要进行一些必要的设置,在这方面也需要进行测试。当一个构建良好的网络能够正常运行,后期的各项服务功能就需要更加完善,应用领域就需要不断扩大。在因特网上有各种各样的信息和服务,而这些信息和服务分布在各种服务器上。例如,门户网站、电子商务、视频点播等,都需要建立特定功能的服务器,并以网站形式呈现。也经常采用服务器托管或租用服务器空间的方法来建立网站,因此对于网络的应用尤其是服务器应用的相关知识、技术应该有一定的了解和掌握。当然,网络技术领域涉及的知识非常多,不是短时间内就能掌握的,需要在日常的操作维护中不断积累和提高。网络的测试与诊断项目综述表如表 3-1 所示。

表 3-1 网络的测试与诊断项目综述表

教学内容	任务一 使用网络命令行工具进行测试诊断 任务二 服务器的认识与构建 任务三 网络的安全防范	参考学时	6
知识目标	掌握网络命令行工具的使用方法,了解有关服务器的相关知识和构建方法,掌握网络的安全防范手段和相关知识		
技能目标	能够使用命令行工具对网络进行测试和诊断,能够构建特定功能的服务器,能够使用相应的技术手段进行网络安全管理和防范		
教学重点	利用网络命令行工具进行网络的测试和诊断		
教学难点	理解和熟练掌握网络命令行工具、特定服务器的构建方法和过程		
教学载体与资源	教材、PPT、实训室、参考手册、网络资源		

续表

教学方法建议	引导演示,师生共同参与项目的完成
教学过程	1. 下达任务和要求; 2. 教师带领学生共同分析任务; 3. 分组讨论

项目准备

(1)完成本项目所需的项目资源清单如表 3-2 所示,按每小组配发。

表 3-2 项目三资源清单表

序号	名称	规格/型号	数量
1	计算机	硬盘空间 200 MB 以上	1 台
2	操作系统	Windows 2000/XP,SP2 以上	1 套
3	Serv-U 软件	10.3 版本	1 套
4	Winmail、U-Mail Server 软件	最新版本	1 套
5	Apache 软件	2.2 版本	1 套
6	FoxMail 软件	6.5 版本	1 套
7	IIS 软件	最新版本	1 套

(2)预习要点。

- ①常用的网络命令行工具种类和作用。
- ②微软 IIS 的安装。
- ③Serv-U 软件的安装。
- ④U-Mail Server 和 Apache 等软件的安装与使用。
- ⑤网络服务器的概念、种类及作用。
- ⑥网络安全防范的方法和措施。

任务一 使用网络命令行工具进行测试诊断

任务分析及任务目标

网络的连通情况和是否正常需要用合适的工具来进行测试和诊断。常用的工具是一些命令行工具,要掌握网络命令的格式以及它们的功能,能够熟练使用命令行工具进行网络的测试和诊断。

相关知识链接

网络的管理是长期的工作,能否让网络发挥应有的作用和实现最初的目的,后期维护、故障诊断、测试都是重要的工作任务。常用的网络管理命令有 ipconfig、ping、arp、tracert、netstat、nslookup、pathping、route 等。



1. ipconfig 命令

该命令用于显示、更新和释放网络地址设置,包括 IP 地址、子网掩码、网关地址和 DNS 服务器设置。如果计算机和所在局域网使用了动态主机配置协议(DHCP),那么 ipconfig 命令可以让用户了解自己的计算机是否成功租用到了一个 IP 地址,并且可以进一步了解它目前分配到的是什么地址。知道机器当前的 IP 地址、子网掩码和默认网关等有利于测试和分析故障。

ipconfig 命令带上/all 参数,即 ipconfig /all 会显示所有网络配置信息。

ipconfig /renew ; 重新申请 IP 地址
ipconfig /release ; 释放 IP 地址
ipconfig /flushdns ; 清空 DNS 解析的缓存

2. ping 命令

Ping 命令比较常用,用于确定本地主机是否能与另一台主机交换(发送与接收)数据包。根据返回的信息,可以推断 TCP/IP 参数是否设置正确以及运行是否正常。另外,能够与另一台主机进行几次数据包交换并不能说明 TCP/IP 配置是正确的,必须执行大量本地主机与远程主机的数据包交换,才能确定 TCP/IP 的正确性。

Ping 是一个测试程序,如果 ping 运行正确,大体上就可以排除网络访问层、网卡、Modem 的输入/输出线路、电缆和路由器等存在的故障,从而缩小了问题的范围。按照默认设置,运行的 ping 命令会发送 4 个 ICMP(网间控制报文协议)回送请求,每个为 32 字节数据,如果正常,应能得到 4 个回送应答。Ping 能够以毫秒为单位显示从发送回送请求到返回回送应答之间的时间量。如果应答时间短,表示数据报不必通过太多的路由器或网络连接速度比较快。Ping 还能显示 TTL(time to live, 存在时间)值,可以根据 TTL 值推算一下数据包已经通过了多少个路由器,即源地点的 TTL 起始值减去返回时的 TTL 值。例如,返回 TTL 值为 119,那么可以推算数据报离开源地址的 TTL 起始值为 128,而源地点到目标地点要通过 9 个路由器网段(128-119);如果返回的 TTL 值为 246,则 TTL 起始值为 256,源地点到目标地点要通过 9 个路由器网段。

Windows 下 ping 命令的格式如下。

```
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [-j -Host list] | [-k Host-list] [-w timeout] 目的主机/IP 地址
```

- -t:有此参数时,当 ping 一个主机时,系统就不停运行这个命令,直到按下 Ctrl+C 组合键。
- -a:解析主机的 NETBIOS 主机名,如果想知道所 ping 的计算机名,则要加上这个参数,一般是在运行 ping 命令后的第一行就显示出来。
- -n count:定义用来测试所发出的测试包的个数,默认值为 4。通过这个命令可以自己定义发送的个数,对衡量网速很有帮助。例如,想测试发送 20 个数据包返回的平均时间、最快时间和最慢时间,就可以通过执行带有这个参数的命令获知。
- -l length:定义所发送缓冲区的数据包的大小,默认的情况下,Windows 的 ping 发送的数据包大小为 32 字节,也可以自己定义,但最大只能发送 65 500 字节,超过这个数时,对方就很可能因接收的数据包太大而死机,所以微软公司为了解决这一安全漏洞

限制了 ping 数据包的大小。

- -f: 在数据包中发送“不要分段”标志, 一般所发送的数据包都会通过路由分段再发送给对方, 加上此参数后路由就不会再进行分段处理。
- -i ttl: 指定 TTL 值在对方系统中停留的时间, 此参数同样帮助检查网络运转情况。
- -v tos: 将“服务类型”字段设置为 tos 指定的值。
- -r count: 在“记录路由”字段中记录传出和返回数据包的路由。一般情况下发送的数据包是通过一个个路由才到达对方的, 但到底经过了哪些路由呢? 通过此参数就可以设定探测经过的路由的个数, 但是限制为 9 个, 即只能跟踪到 9 个路由。
- -s count: 指定由 count 设定的跃点数的时间戳, 此参数与 -r count 类似, 只是它不记录数据包返回所经过的路由。
- -j Host-list: 利用 computer-list 指定计算机列表路由数据包。连续计算机可以被中间网关分隔 IP, 允许的最大数量为 9。
- -k Host-list: 利用 computer-list 指定计算机列表路由数据包。连续计算机不能被中间网关分隔 IP 允许的最大数量为 9。
- -w timeout: 指定超时间隔, 单位为毫秒。

3. arp 命令

ARP(地址转换协议)是一个重要的 TCP/IP, 用于确定对应 IP 地址的网卡物理地址。arp 命令能够查看本地或另一台计算机 ARP 高速缓存中的当前内容。arp 表项的内容就是计算机的逻辑地址(IP 地址)和硬件地址(网卡的 MAC 地址)的对应关系表。此外, 使用 arp 命令也可以用人工方式输入静态的网卡物理/IP 地址对, 有助于减少网络上的信息量。

Arp 命令有以下 3 种使用形式。

(1) 显示高速缓存区 cache 中的 ARP 表内容, 其命令格式为 arp/a。

(2) 添加 ARP 静态表项, 命令格式为 arp-s inet-addr ether-addr。其作用是在 ARP 缓存中添加新项, 将 IP 地址 inet-addr 和物理地址 ether-addr 相关联。

(3) 删除 ARP 表项, 命令格式是 arp-d inet-addr。其作用是删除由 inet-addr 指定的项。

4. tracert 命令

如果网络连通有问题, 可用 tracert 检查到达的目标 IP 地址的路径并记录结果。Tracert 命令的使用很简单, 只需要在 tracert 后面加一个 IP 地址或 URL 即可, tracert 一般用来检测故障的位置, 可以用 tracert IP 确定在哪个环节上出了问题。如果有网络连通性问题, 可以使用 tracert 命令检查到达的目标 IP 地址的路径并记录结果。Tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器, 以及每个跃点所需的时间。如果数据包不能传递到目标位置, tracert 命令将显示成功转发数据包的最后一个路由器。当数据包从某计算机经过多个网关传送到目的地时, tracert 命令可以用来跟踪数据报使用的路由(路径)。如果配置使用的是 DNS, 那么常常会从所产生的应答中得到城市、地址和常见通信公司的名字。Tracert 是一个运行比较慢的命令(指定的目标地址比较远), 每个路由器大约需要给它 15 秒的时间。

Tracert 命令格式如下。

```
tracert [-d][-h maximum_hops][-j host_list][-w timeout] 目标名称
```



- -d: 不解析远程计算机的名字。
- -h maximum_hops: 指定搜索到目标地址的最大跃点数。
- -j host_list: 按照计算机列表中的地址释放源路由。
- -w timeout: 指定超时时间间隔, 程序默认的时间单位是毫秒。

5. netstat 命令

Netstat 命令用于显示与 IP、TCP、UDP 和 ICMP 相关的统计数据, 一般用于检验本机各端口的网络连接情况。可以让用户得知当前有哪些网络连接正在运行。它用来检测网络上的连接情况, 告知用户所有连接及详细的端口, 可以使用该命令实现实时监控, 很清楚地观察网络上所有进程和用户连接。有时计算机接收到的数据包会导致出错数据删除或故障, 这是因为 TCP/IP 可以容许这些类型的错误, 并能够自动重发数据包。但如果累计的出错情况数目占相当大的比例, 或者数目正迅速增加, 那么就on应该使用 netstat 命令检查一下原因。

Netstat 命令的格式如下。

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

- -a: 用来显示在本地机上的外部连接, 它也显示远程所连接的系统, 本地和远程系统连接时使用和开放的端口, 以及本地和远程系统连接的状态。这个参数通常用于获得本地系统开放的端口, 用它还可以自己检查系统上有没有被安装木马, 如果在机器上运行 netstat 命令后发现诸如 port 12345 (tcp) netbus、port 31337 (udp) back orifice 之类的信息, 则机器上很可能感染了木马。
- -e: 显示静态以太网统计, 该参数可以与 -s 选项结合使用。
- -n: 这个参数基本上是 -a 参数的数字形式, 它是用数字的形式显示地址和端口, 通常用于检查自己的 ip 时使用。
- -s: 显示机器默认情况下每个协议的配置统计, 默认情况下包括 TCP、IP、UDP、ICMP 等协议。
- -p protocol: protocol 用来显示特定的协议配置信息, 它的格式为 netstat -p××××, ×××× 可以是 udp、ip、icmp 或 tcp, 如果要显示机器上的 TCP 配置情况, 则可以用 netstat -p tcp。
- -r: 用来显示路由分配表。
- interval: 每隔 interval 秒重复显示所选协议的配置情况, 直到按 Ctrl+C 组合键中断。

6. nslookup 命令

Nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。该命令可以返回正在使用的 DNS 服务器名称和 IP 地址。如果 nslookup 命令后面跟域名参数, 则可以完成正向搜索, 会返回域名对应的 IP 地址。如果 nslookup 后面带 IP 地址参数, 则可以反向搜索, 会返回 IP 地址对应的机器域名。

7. pathping 命令

Pathping 命令是一个路由跟踪工具。它将 ping 和 tracertrt 命令的功能和这两个工具所不提供的其他信息结合起来。Pathping 命令定期将数据包发送到通往最终目标的路径上的每个路由器, 然后基于从每个跃点返回的数据包来计算结果。由于该命令显示数据包在任何给定路由器或链接上丢失的程度, 因此可以很容易地确定可能导致网络问题的路由器或链接。

8. route 命令

大多数主机一般都驻留在连接一台路由器的网段上。由于只有一台路由器,因此不存在使用哪一台路由器将数据包发到远程计算机上去的问题,该路由器的 IP 地址可作为该网段上所有计算机的默认网关来输入。

但是,当网络上拥有两个或多个路由器时,就不一定只想依赖默认网关了。实际上可能想让某些远程 IP 地址通过某个特定的路由器来传递,而其他远程 IP 则通过另一个路由器来传递。

在这种情况下,需要相应的路由信息,这些信息存储在路由表中,每个主机和每个路由器都配有自己独一无二的路由表。大多数路由器使用专门的路由协议来交换和动态更新路由器之间的路由表。但在有些情况下,必须人工将项目添加到路由器和主机上的路由表中。Route 就是用来显示、人工添加和修改路由表项的。

Route 命令的格式如下。

```
route[-f] [-p] [command [destination] [mask netmask] [gateway] [metric]
[if interface]
```

- -f:用于清除路由表。清除所有不是主路由(子网掩码为 255.255.255.255 的路由)、环回网络路由(目标为 127.0.0.0,子网掩码为 255.255.255.0 的路由)或多播路由(目标为 224.0.0.0,子网掩码为 240.0.0.0 的路由)的路由表。如果它与 add、change 或 delete 命令结合使用,表会在运行命令之前清除。
- -p:用于永久保留某条路由。与 add 命令共同使用时,指定路由被添加到注册表并在启动 TCP/IP 时初始化 IP 路由表。默认情况下,启动 TCP/IP 时不会保存添加的路由。与 print 命令一起使用时,则显示永久路由列表。所有其他命令都忽略此参数。永久路由存储在注册表中的位置是 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes。
- command:主要有 print(打印)、add(添加)、delete(删除)、change(修改)4 个命令。
- destination:代表所要达到的目标 IP 地址,指定路由的网络目标地址。目标地址可以是一个 IP 网络地址(其中网络地址的主机地址位设置为 0),对于主机路由是 IP 地址,对于默认路由是 0.0.0.0。
- mask netmask:子网掩码的关键字。netmask 代表具体的子网掩码,如果不加说明,默认是 255.255.255.255(单机 IP 地址),因此输入掩码时要特别小心,要确认添加的是某个 IP 地址还是 IP 网段。如果代表全部出口子网掩码,则可用 0.0.0.0。
- gateway:代表出口网关。指定超过由网络目标和子网掩码定义的可达到的地址集的前一个或下一个跃点 IP 地址。对于本地连接的子网路由,网关地址是分配给连接子网接口的 IP 地址。对于要经过一个或多个路由器才可用到的远程路由,网关地址是一个分配给相邻路由器的、可直接达到的 IP 地址。
- metric:为路由指定所需跃点数的整数值(范围是 1~9 999),它用来在路由表的多个路由中选择与转发包中的目标地址最为匹配的路由。所选的路由具有最少的跃点数。跃点数能够反映跃点的数量、路径的速度、路径可靠性、路径吞吐量以及管理属性。



- if interface: 指定目标可以到达的接口的接口索引。使用 route print 命令可以显示接口及其对应接口索引的列表。对于接口索引可以使用十进制或十六进制值。对于十六进制值,要在十六进制数的前面加上 0x。忽略 if 参数时,接口由网关地址确定。

任务实施

1. 进入控制台

在 Windows 操作系统中执行“开始”→“运行”命令,弹出“运行”对话框,在“打开”文本框中输入 cmd 并单击“确定”按钮,打开控制台程序窗口,如图 3-1 所示。



图 3-1 进入控制台程序

2. ipconfig 命令测试

输入 ipconfig/all 命令并按 Enter 键,将会得到网络配置的详细信息,如图 3-2 所示。

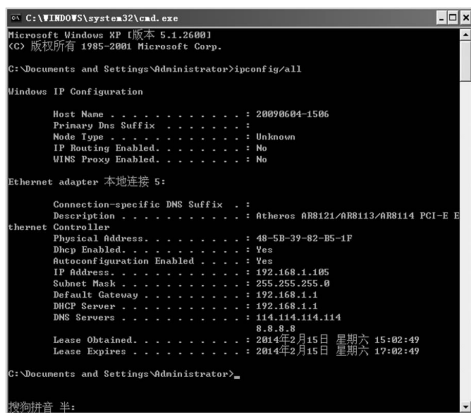


图 3-2 显示所有网络配置信息

3. arp 命令测试

在控制台程序中输入 arp/a 并按 Enter 键,则会显示高速缓存的 arp 表项内容,输入 arp -a 并按 Enter 键将显示本机的 arp 映射表,如图 3-3 所示。可以用 arp -s 命令向 ARP 高速缓存中人工输入一个静态项目,该项目在计算机引导过程中将保持有效状态,或者在出现错误时,人工配置的物理地址将自动更新该项目。输入 arp -d 命令并按 Enter 键能够人工删除一个静态项目。

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>arp/a

Interface: 192.168.1.105 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1           b0-48-7a-2e-7f-44    dynamic

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.105 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1           b0-48-7a-2e-7f-44    dynamic

C:\Documents and Settings\Administrator>_

```

图 3-3 显示 arp 表项

4. ping 命令测试

在控制台程序中输入 ping www.sohu.com 并按 Enter 键,可以观察测试本机到 sohu 主页是否连通,如图 3-4 所示。

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping www.sohu.com

Pinging fbjuni.a.sohu.com [61.135.132.59] with 32 bytes of data:

Reply from 61.135.132.59: bytes=32 time=25ms TTL=58
Reply from 61.135.132.59: bytes=32 time=24ms TTL=58
Reply from 61.135.132.59: bytes=32 time=22ms TTL=58
Reply from 61.135.132.59: bytes=32 time=24ms TTL=58

Ping statistics for 61.135.132.59:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 25ms, Average = 23ms

C:\Documents and Settings\Administrator>_

```

图 3-4 测试连通性

利用命令 ping -t www.sohu.com 可以连续测试,如图 3-5 所示。

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping -t www.sohu.com

Pinging fbjuni.a.sohu.com [61.135.181.167] with 32 bytes of data:

Reply from 61.135.181.167: bytes=32 time=25ms TTL=58
Reply from 61.135.181.167: bytes=32 time=25ms TTL=58
Reply from 61.135.181.167: bytes=32 time=23ms TTL=58
Reply from 61.135.181.167: bytes=32 time=22ms TTL=58
Reply from 61.135.181.167: bytes=32 time=24ms TTL=58
Reply from 61.135.181.167: bytes=32 time=23ms TTL=58
Reply from 61.135.181.167: bytes=32 time=25ms TTL=58
Reply from 61.135.181.167: bytes=32 time=24ms TTL=58
Reply from 61.135.181.167: bytes=32 time=24ms TTL=58

Ping statistics for 61.135.181.167:
    Packets: Sent = 9, Received = 9, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 25ms, Average = 23ms
Control-C
^C
C:\Documents and Settings\Administrator>_

```

图 3-5 连续测试连通性



5. netstat 命令测试

在控制台程序中输入 netstat -a 命令并按 Enter 键,则会显示出目前所有本地端口和远程端口的连接状态,包括 TCP 和 UDP,如图 3-6 所示。

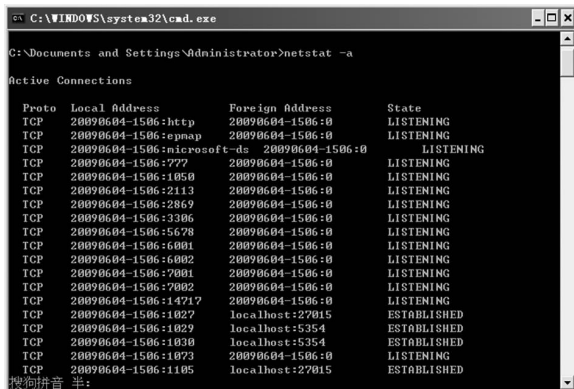


图 3-6 显示联网状态

6. tracert 命令测试

在控制台中输入 tracert www.sohu.com 命令并按 Enter 键,则会出现如图 3-7 所示的界面。输出共有五列,第一列是描述沿该路径的序号。第二、第三、第四列是第一、第二、第三次返回的时间。第五列是路由器的名字及其输入端口的 IP 地址。如果从任何给定的路由器接收到的报文少于三条,则会在该路由器号码后面加一个星号。

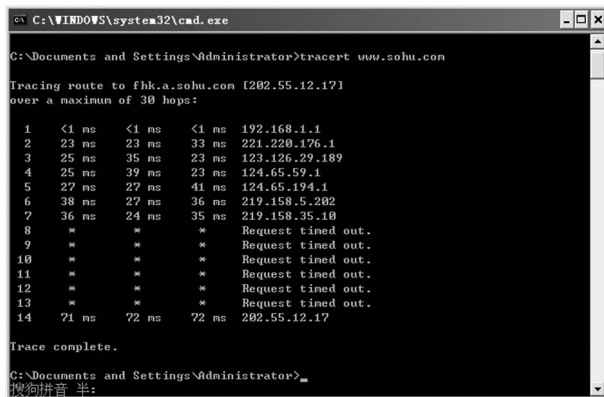


图 3-7 路径测试

7. nslookup 命令测试

在控制台中输入命令 nslookup 并按 Enter 键后,会出现如图 3-8 所示的界面,返回正在使用的 DNS 服务器的名称和 IP 地址。

```

C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup
Default Server: dnspai-public-dns.dnspai.com
Address: 123.125.81.6

> =

```

图 3-8 查询 DNS 服务器的地址和名称

如果输入 nslookup www.baidu.com 命令,则会完成正向搜索,返回域名对应的 IP 地址,如图 3-9 所示。

```

C:\WINDOWS\system32\cmd.exe - nslookup
> nslookup www.baidu.com
Server: www.a.shifen.com
Addresses: 61.135.169.105, 61.135.169.125
Aliases: www.baidu.com

DNS request timed out.
timeout was 2 seconds.
*** Request to www.baidu.com timed-out
>

```

图 3-9 正向搜索

8. pathping 命令测试

在控制台中输入命令 pathping -n 58.132.132.105 并按 Enter 键,会显示数据包在任何给定路由器或链接上丢失的程度,如图 3-10 所示。

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>pathping -n 58.132.132.105

Tracing route to 58.132.132.105 over a maximum of 30 hops:

 0 192.168.1.105
 1 192.168.1.1
 2 221.220.176.1
 3 123.126.29.157
 4 61.148.6.117
 5 61.148.158.46
 6 61.148.158.74
 7 202.106.51.42
 8 211.153.4.49
 9 * * * * * 211.153.4.10
10 211.153.10.2
11 211.153.12.74
12 211.153.12.78
13 * * * * *

Computing statistics for 325 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 0ms 0/100 = 0% 0/100 = 0% 192.168.1.105
1 0ms 0/100 = 0% 0/100 = 0% 192.168.1.1
2 129ms 0/100 = 0% 0/100 = 0% 221.220.176.1
3 130ms 1/100 = 1% 1/100 = 1% 123.126.29.157
4 --- 100/100 =100% 100/100 =100% 61.148.6.117
5 --- 100/100 =100% 100/100 =100% 61.148.158.46
6 --- 100/100 =100% 100/100 =100% 61.148.158.74
7 118ms 2/100 = 2% 2/100 = 2% 202.106.51.42
8 122ms 0/100 = 0% 0/100 = 0% 211.153.4.49
9 135ms 0/100 = 0% 0/100 = 0% 211.153.4.10

```

图 3-10 pathping 命令的使用



9. route 命令测试

在控制台中输入 route print 命令并按 Enter 键,会显示路由表,如图 3-11 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...48 5b 39 82 05 1f ..... Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Cont
roller - 数据包计划程序微型端口
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1     192.168.1.105    20
127.0.0.0                  255.0.0.0        127.0.0.1       127.0.0.1        1
169.254.0.0                255.255.0.0     192.168.1.105  192.168.1.105    20
192.168.1.0                255.255.255.0   192.168.1.105  192.168.1.105    20
192.168.1.105              255.255.255.255 127.0.0.1       127.0.0.1        20
192.168.1.255              255.255.255.255 192.168.1.105  192.168.1.105    20
224.0.0.0                  240.0.0.0        192.168.1.105  192.168.1.105    20
255.255.255.255           255.255.255.255 192.168.1.105  192.168.1.105    1
Default Gateway:          192.168.1.1
=====
Persistent Routes:
None
C:\Documents and Settings\Administrator>_
搜狗拼音 半:
```

图 3-11 显示路由表

任务二 服务器的认识与构建

任务分析及任务目标

将局域网接入 Internet,可以使用户充分享受因特网带来的好处。Internet 也在不断发展和完善,应用领域越来越广泛,除了通过因特网浏览和检索信息,还有一些其他服务提供给用户,这些服务都在各种各样的服务器上。因此,了解和简单构建服务器也是非常必要的。通过本任务,应该了解或掌握 FTP 服务器、邮件服务器、Web 服务器的构建过程。

相关知识链接

一、FTP 服务器

FTP 的全称是 file transfer protocol(文件传输协议),是用来在两台计算机之间传输文件的协议。支持 FTP 的服务器就是 FTP 服务器。用户联网的目的之一就是实现信息共享,文件传输是信息共享中非常重要的一个内容。

但是 Internet 的构成是非常复杂的,有 PC、工作站、MAC、大型机等。这些计算机可能运行不同的操作系统,为了使各种操作系统之间能够进行文件交流,需要建立统一的文件传输协议,即 FTP。不同的操作系统有不同的 FTP 应用程序,而人们都遵守同一种协议,这样文件就可以互传。

FTP 也属于客户机/服务器系统。客户机连到服务器需要提供账号和密码,或是允许在匿名的 FTP 服务器上通过匿名访问。用户通过一个支持 FTP 协议的客户机程序,连接到在远程主机上的 FTP 服务器程序。用户通过客户机程序向服务器程序发出命令,服务器程序执行用户所发出的命令,并将执行的结果返回到客户机。例如,用户发出一条命令,要求服务器向用户传送某个文件的一份拷贝,服务器会响应这条命令,将指定文件送至用户的机

器上。客户机程序代表用户接收这个文件,将其存放在用户的某个目录中。

在 FTP 的使用中存在下载和上传两个操作过程。下载文件就是从远程主机复制文件到自己的计算机上,上传文件就是将文件从自己的计算机中复制至远程主机上。使用 FTP 时必须先登录,在远程主机上获得相应的权限后,才能上传或下载文件,因此必须有用户的 ID 和密码,否则便无法传送文件。这种情况是有弊端的,因为不可能要求每个用户在每台主机上都拥有账号。匿名 FTP 就是为了解决这个问题而产生的。

匿名 FTP 是指用户可以连接到远程主机上,并从其上下载文件,而无须成为其注册用户。系统管理员建立了一个特殊的用户 ID,名为 anonymous。Internet 上的任何人在任何地方都可使用该用户 ID。通过 FTP 程序连接匿名 FTP 主机就变得简单了,在要求提供用户标识 ID 时输入 anonymous 即可,而密码可以是任意字符串。

当然,匿名 FTP 不适用于所有 Internet 主机,需要 Internet 主机提供这项服务才行。

二、邮件服务器

电子邮件是因特网上重要的应用之一,是人们之间保持联系互通的重要手段。电子邮件非常快速,可以远隔万里而瞬时寄到。同时易于分发,可以将一封邮件同时发送给多个收信人。另外成本低廉,有很多免费的邮箱供大家使用,邮箱的容量也在增大。与传统信件相比,电子邮件可以包含图像、声音甚至视频数据。很多企业已经完全使用电子邮件代替传统信函来满足办公需要,极大提高了办公效率。

邮件服务器是电子邮件系统的核心。每个收发信人都有一个位于某个邮件服务器上的邮箱。电子邮件通过发信人的邮件服务器转到收信人的邮件服务器,然后投递到收信人的邮箱中,图 3-12 所示是电子邮件的运行原理。

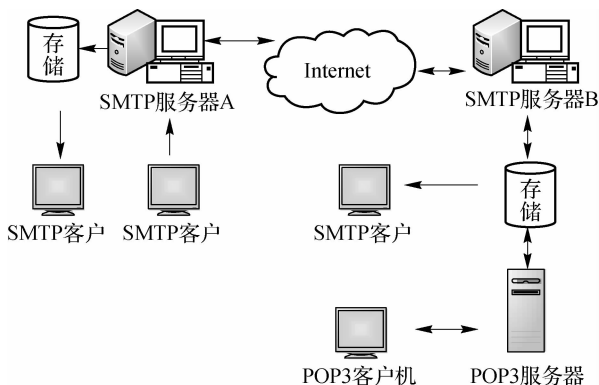


图 3-12 电子邮件的运行原理

目前,电子邮件也在逐渐被新的技术形式所取代,如微信、腾讯 QQ 等,而企业内部也被办公自动化系统所涵盖,但学会建立邮件服务器还是有必要的。

三、Web 服务器

Web 服务器也称为 WWW(world wide web)服务器,主要提供网上信息浏览服务。WWW 是 Internet 的多媒体信息查询工具,是目前发展最快和应用最广泛的服务,是它造就了 Internet 的迅速发展。

Web 服务器是指网站服务器,即用于存放网站数据的服务器。一个网站上所有的文字、图片等统称为数据,这些数据是需要有后台服务器支撑的。当用户访问网站时,其实是通过网络向服务器发送了一个请求,服务器再将用户请求的页面反馈到用户,这时用户才可以看到网站的界面。而 Web 服务器就是这个在后台提供数据服务的服务器。简单来说,Web 服务器是提供网页给别人看的服务器。例如,如果想访问搜狐网,就要访问搜狐网的 Web 服务器。Web 服务器是具有独立 IP 地址的计算机,可以向客户机提供 WWW、E-mail 和 FTP 等各种 Internet 服务。Web 服务器使用 HTTP(超文本传送协议)与客户机浏览器进行信息交流,所以人们常把它们称为 HTTP 服务器。最常用的 Web 服务器是 Apache 和微软公司的 Internet 信息服务器(Internet information server, IIS)。

IIS 是允许在公共 Intranet 或 Internet 上发布信息的 Web 服务器。它是最流行的 Web 服务器之一,很多网站都是建立在 IIS 平台上的。IIS 提供了一个图形界面的管理工具,称为 Internet 服务管理器,可用于监视配置和控制 Internet 服务。

IIS 是一种 Web 服务组件,包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器,分别用于网页浏览、文件传输、新闻服务和邮件发送。它使得在因特网或局域网上发布信息变得容易。它提供 ISAPI(Intranet server API)作为扩展 Web 服务器功能的编程接口,同时还提供一个 Internet 数据库连接器,可以实现对数据库的查询和更新。通过 IIS,开发人员可以开发动态的、富有魅力的 Web 站点。

Apache 是世界上用得最多的 Web 服务器,市场占有率高达 60%左右。它源于 NCSAhttpd 服务器。世界上很多著名的网站都是建立在 Apache 平台上的,Apache 的成功之处主要在于源代码开放、支持跨平台应用(可以运行在几乎所有 UNIX、Windows 和 Linux 系统平台上)以及可移植性等方面。

任务实施

一、使用 Serv-U 软件构建 FTP 服务器

下载 Serv-U 10.3 执行文件并安装,安装成功后开始配置,管理控制台如图 3-13 所示。单击“新建域”按钮,打开如图 3-14 所示的域向导步骤 1。



图 3-13 Serv-U 10.3 管理控制台



图 3-14 域向导步骤 1

设好名称和说明后单击“下一步”按钮，会打开步骤 2 界面，如图 3-15 所示。选中第一个复选框，这里的参数保持默认 FTP 端口为 21，也可以改为其他不冲突的端口（出于安全方面考虑），单击“下一步”按钮，打开如图 3-16 所示的步骤 3 界面，选择现有的 IP 地址后，单击“下一步”按钮。

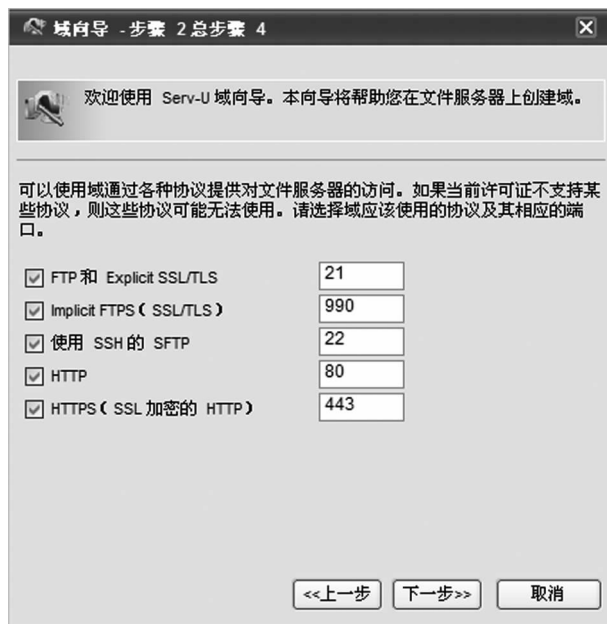


图 3-15 域向导步骤 2



图 3-16 域向导步骤 3

在打开的如图 3-17 所示的步骤 4 界面中选择默认的密码加密模式即可。单击“完成”按钮,域创建完成。

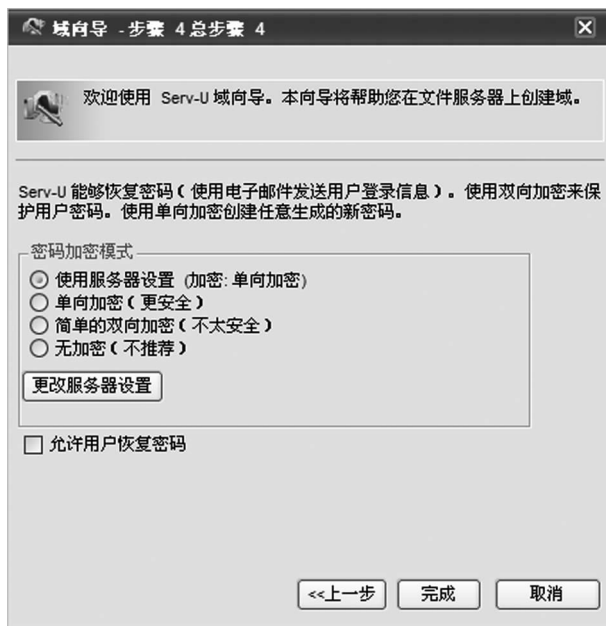


图 3-17 域向导步骤 4

完成了域的创建,下面要去访问 FTP 服务器,就需要创建用户,管理员也可以在此时创建,使用向导创建用户方便维护和管理,用户向导步骤 1 如图 3-18 所示。登录 ID 是作为访

问 FTP 的用户身份的,为访问者所持有。域管理员有修改的权限,可以对其权限进行修改和限制。填好 ID 后,单击“下一步”按钮,打开如图 3-19 所示的步骤 2 界面。

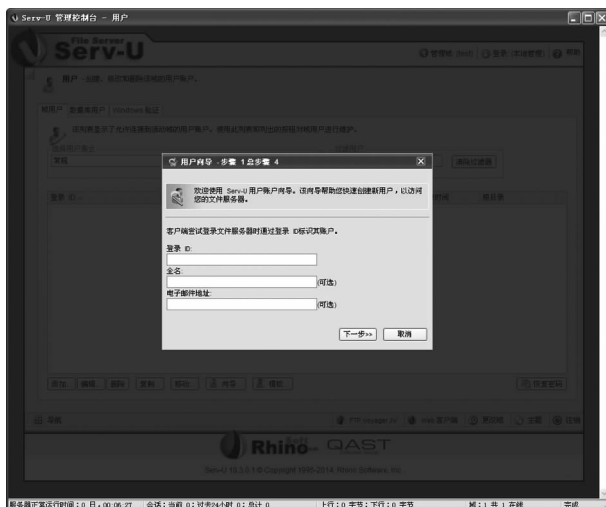


图 3-18 用户向导步骤 1



图 3-19 用户向导步骤 2

默认密码为一串随机密码,记忆起来很不方便,但是安全性较高。也可以设置个性密码,但在实际应用中要注意安全。填好后单击“下一步”按钮,打开如图 3-20 所示的步骤 3 界面。选择根目录,也就是用户登录以后停留的物理目录位置例如,这里在 C 盘下建立了目录 FTP。选择完成后单击“下一步”按钮,打开如图 3-21 所示的步骤 4 界面,可以对用户的访问权限进行设定,有只读访问和完全访问两种权限。只读访问权限是指用户不能修改目录下的文件信息,只能以只读的方式访问。如果用户要下载、上传或修改目录下的文件,就将其权限设置为完全访问。单击“完成”按钮,用户创建完成。



图 3-20 用户向导步骤 3

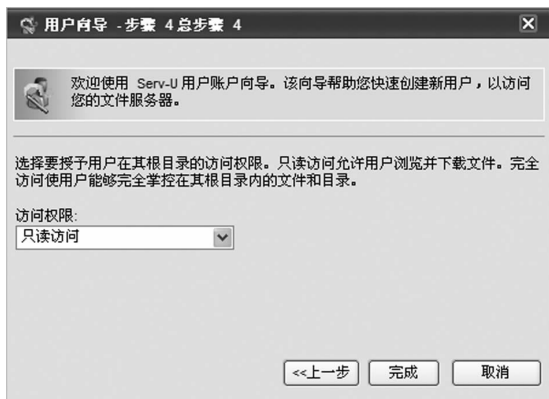


图 3-21 用户向导步骤 4

FTP 服务器创建好之后,用户可以通过三种方式访问,即客户端软件、浏览器和命令行。其中,通过浏览器访问方式比较简单。

在浏览器地址栏中输入 FTP 服务器的地址并按 Enter 键后会出现登录界面,输入登录 ID 和密码后单击“登录”按钮即能进入,如图 3-22 所示。



图 3-22 登录界面

二、邮件服务器的构建

架设邮件服务器的工具有很多,如 Exchange 2007、Winmail、U-Mail Server 等。这里介绍 U-Mail Server 软件。

可以到其公司网站 <http://www.comingchina.com/> 下载软件或了解更多产品介绍。U-Mail Server 是一款安全、易用、全功能的邮件服务器软件,内嵌卡巴斯基杀毒引擎,基于行为识别的反垃圾过滤引擎,纯 Web 端的便捷管理,全自动化的自我管理,在安装系统之前,还必须选定操作系统平台。例如,U-Mail for Windows 可以安装在 Windows 2000、Windows 2003、Windows 2008 操作系统上(建议打全所有操作系统补丁)。

该软件的安装过程与一般软件类似,下面只给出一些要注意的步骤,如安装组件、安装目录以及设置管理员的登录密码等。

1. U-Mail Server 软件的安装

(1)开始安装,检测安装环境,这里用简体中文演示,如图 3-23 所示。



图 3-23 检测安装环境

(2)安装向导界面如图 3-24 所示。



图 3-24 安装向导界面

(3)授权协议界面如图 3-25 所示。

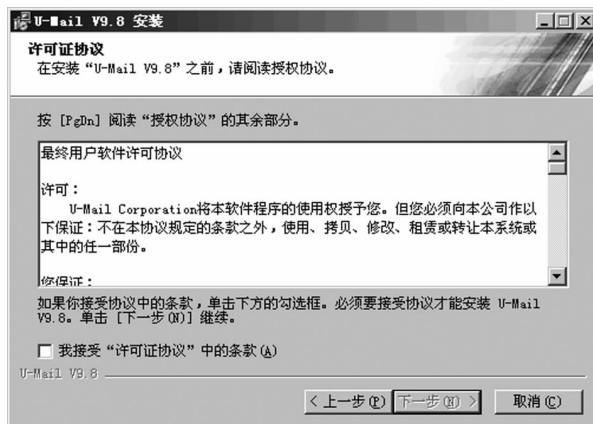


图 3-25 授权协议界面

(4)选择安装组件,如图 3-26 所示。



图 3-26 选择安装组件

(5)选定安装位置,如图 3-27 所示。

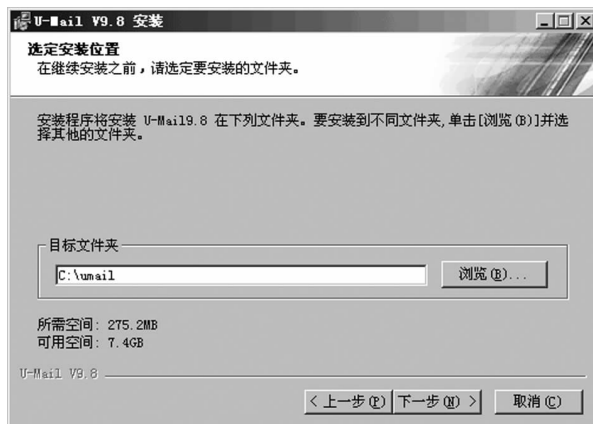


图 3-27 选定安装位置

(6) 邮件系统主域名设置,如图 3-28 所示。

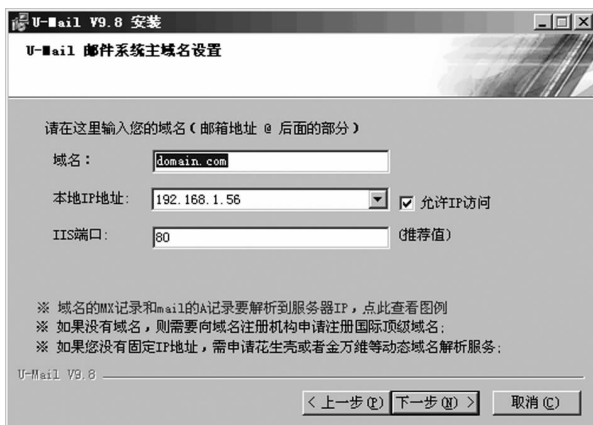


图 3-28 主域名设置

(7) 邮件系统管理账号设置,如图 3-29 所示。

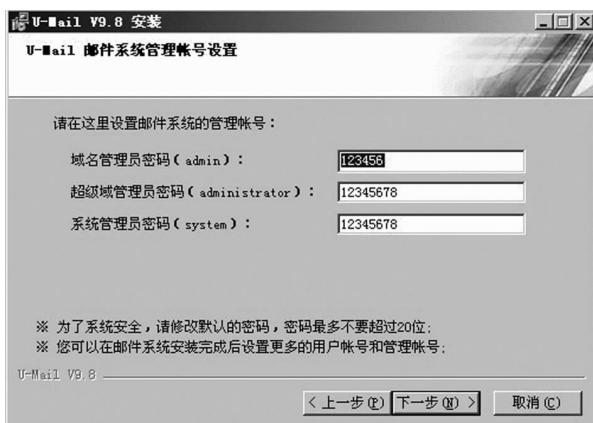


图 3-29 管理账号的设置

(8) 开始安装,如图 3-30 所示。



图 3-30 安装界面



(9)安装成功(需重启服务器),如图 3-31 所示。

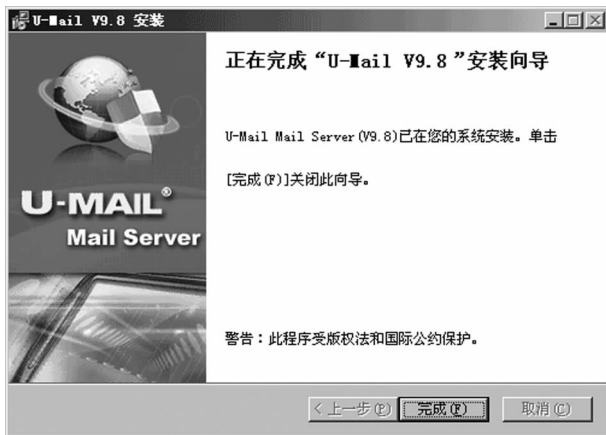


图 3-31 安装完成

U-Mail Server 安装完成后就可以进行收发信测试了。可以使用常用的邮件客户端软件,如 Outlook Express、FoxMail 来测试。

2. 客户端软件测试

下面以 Outlook Express 为例,讲述如何设置邮件客户端软件。

(1)增加邮件账号。执行“工具”→“账号”菜单命令,弹出如图 3-32 所示的对话框,单击“添加”按钮,选择“邮件”选项。

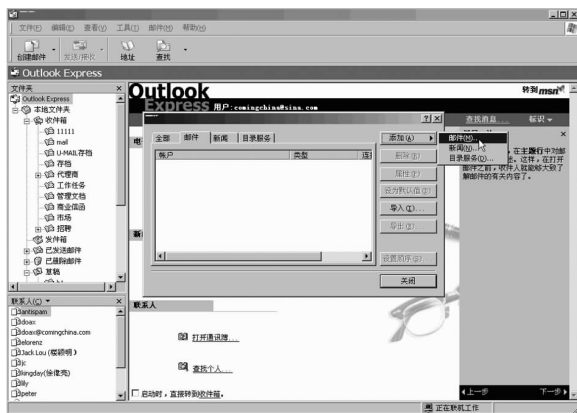


图 3-32 添加邮件账号

(2)设置发件人名字。进入 Internet 连接向导,在“显示名”文本框中填入名称,如图 3-33所示。单击“下一步”按钮。



图 3-33 填写用户名

(3)填写邮件地址,如图 3-34 所示,在“电子邮件地址”文本框中填写在邮件系统中增加的用户电子邮件地址。



图 3-34 填写电子邮件地址

(4)填写邮件服务器。接收邮件服务器选为 POP3,在“接收邮件 (POP3、IMAP 或 HTTP)服务器”的文本框中填入邮件服务器的主机名或 IP 地址,而在“发送邮件服务器 (SMTP)”中填入邮件服务器的主机名或 IP 地址,如图 3-35 所示。

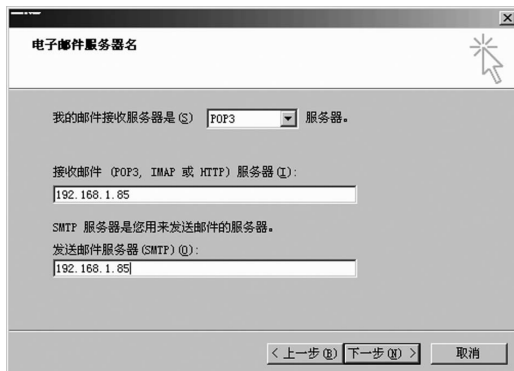


图 3-35 填写电子邮件服务器



(5)填写账户名和密码。输入邮件系统中的用户账户名和密码,如图 3-26 所示。然后单击“下一步”按钮。

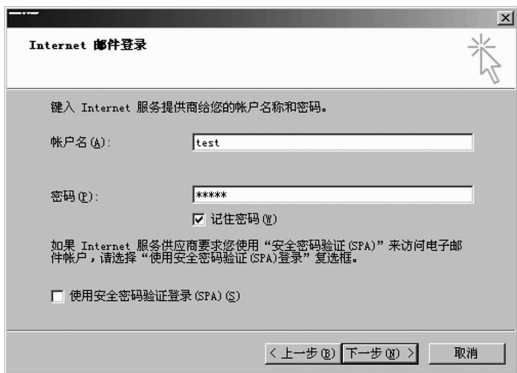


图 3-36 填写账户名及密码

(6)添加账户完成,如图 3-37 所示。

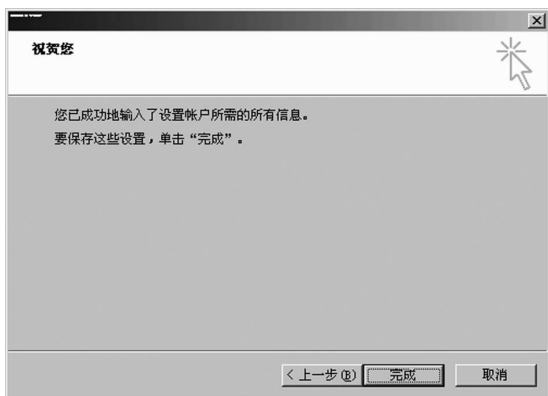


图 3-37 账户添加完成

(7)修改账户属性。要修改用户设置,执行“工具”→“账户”菜单命令,在弹出的对话框中选择要设定的账户,单击“属性”按钮,在弹出的对话框中可以修改账户属性,如图 3-38 所示。



图 3-38 修改账户属性

(8)在“用户信息”栏中可以修改用户资料,如图 3-39 所示。



图 3-39 修改用户资料

(9)修改账户信息。如果邮件系统的 SMTP 服务激活了发送认证功能,则必须选中“我的服务器要求身份验证”复选框,如图 3-40 所示。

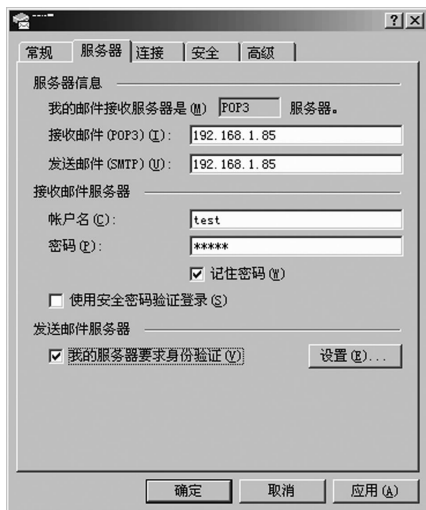


图 3-40 修改账户信息

(10)设置认证方式。在上面的步骤中,如果选中“我的服务器要求身份验证”复选框,则可以单击右边的“设置”按钮,在打开的对话框中设置认证方式。一般采用“使用与接收邮件服务器相同的设置”,如图 3-41 所示。

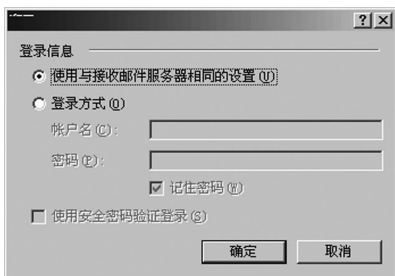


图 3-41 设置认证方式

(11)设置账户的高级属性。如果用户希望在收信之后,不删除服务器上的邮件,可以在“高级”选项卡中选中“在服务器上保留邮件副本”复选框,如图 3-42 所示。

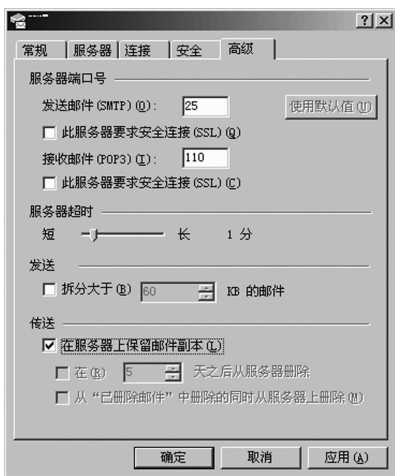


图 3-42 设置账户的高级属性

(12)收发邮件测试。写邮件分别发送到本域用户和外域用户,然后接收邮件,也可以用 Webmail 测试。U-Mail Server 系统支持 Webmail 收发邮件,安装完成后用浏览器进行测试即可。登录地址是 <http://mail.yourdomain.com/>。

(13)登录 Webmail,如图 3-43 所示。



图 3-43 登录 Webmail

U-Mail Server 主要的组件有服务器核心和管理工具两部分。服务器核心主要完成 SMTP、POP3、ADMIN、HTTP 等服务功能；管理工具主要负责设置邮件系统，如设置系统参数、管理用户、管理域等。U-Mail Server 是高度自动化的邮件服务器系统，反垃圾和反病毒都是自动升级的，所有操作都是纯网页操作，非常便捷。

三、Web 服务器的构建

Windows XP 在默认情况下是不安装 IIS 组件的，需要手工安装，安装步骤如下。

(1) 插入 Windows XP 的安装光盘，在控制面板中打开“添加或删除程序”窗口。

(2) 在窗口左边选择“添加/删除 Windows 组件”选项。

(3) 系统会启动 Windows 组件向导，选中“Internet 信息服务(IIS)”复选框，如图 3-44 所示，单击“下一步”按钮。

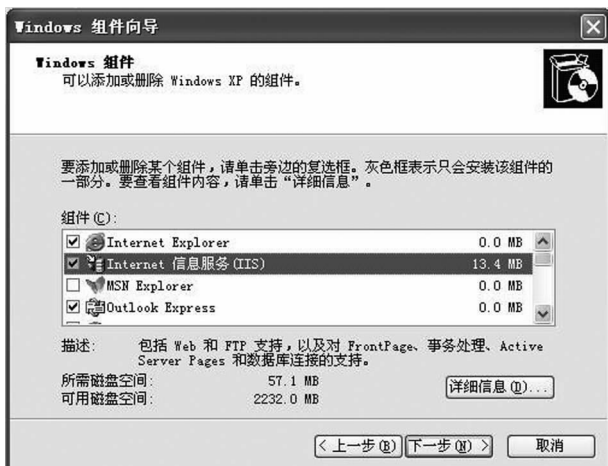


图 3-44 安装向导

(4) 系统安装成功，会自动在系统盘新建网站目录。执行“控制面板”→“性能和维护”→“管理工具”→“Internet 信息服务”命令，打开“Internet 信息服务”窗口，如图 3-45 所示。



图 3-45 Internet 信息服务

(5) 可以重新命名一个 Web 站点，右击图 3-45 中的“默认网站”，在弹出的快捷菜单中选择“重命名”命令即可，若选择“属性”命令，则打开如图 3-46 所示的对话框。在“IP 地址”文本框中输入 127.0.0.1，其他设置可参考有关资料。



图 3-46 属性设置

(6)先做好网页,然后可以启动 Web 站点测试。在浏览器中输入 `http://127.0.0.1` 并按 Enter 键,就可以浏览自己制作的网页了。

任务三 网络的安全防范

任务分析及任务目标

随着 Internet 的发展和用户的迅速增加,网络安全风险变得更加严重和复杂。原来只是由个体计算机安全事故所引起的损害可能传播到其他系统,引起大范围损失。在本任务中要了解网络安全的概念,掌握一定的防护措施,能够使用相关工具提高网络系统的安全性。

相关知识链接

一、网络安全的概念

网络安全就是网络上的信息安全,它涉及的领域很广,网络系统的硬件、软件及其系统中的数据要受到保护,避免遭到破坏、更改、泄露,要保障系统可靠、正常运行。它包括网络运行系统安全、网络系统信息安全、信息传播安全、网络信息内容安全等方面。对网络安全进行防范应注意以下几个方面。

(1)网络上的信息不应该泄露给非授权用户。世界上的很多国家都发生过政府部门重要的保密信息被盗取的事件,造成巨大的损失。所以防止攻击和信息盗取是目前面临的主要网络安全工作。

(2)数据未经授权不能被改变。信息在存储或传输过程中保持不被修改、不被破坏和不会丢失的特性。很多网站都发生过被篡改和更换信息的事件,对社会产生了负面影响。

(3)对信息的传播及内容具有控制能力。

二、维护网络安全的措施

维护网络安全的工具有 VIEID、数字证书、数字签名和基于本地或云端的杀毒软件等,还有具体的法律支持。构建网络安全系统,要进行认证、加密、监听、分析、记录等工作,会增加一定成本。但是在网络上运行关键业务时,网络安全是首先要解决的问题。例如,证券、银行、军队部门等的网络安全等,在网络安全上的投入不应计较成本。

安全防范不是某一方面的措施,而是一个体系的建立,多种方式共同作用的结果。主要体现在以下方面。

(1)访问控制。通过对特定网段、服务建立访问控制体系,将绝大多数攻击阻止在到达某攻击目标之前或某一范围内,如 VLAN 技术。

(2)检查安全漏洞。通过对安全漏洞的周期性检查,即使攻击可到达攻击目标,也可使绝大多数攻击无效。

(3)攻击监控。通过对特定网段、服务建立攻击监控体系,可实时检测出绝大多数攻击,并采取相应行动,如断开网络连接、记录攻击过程、跟踪攻击源等。

(4)加密通信。主动的加密通信可使攻击者不能了解、修改敏感信息。在此方面很多商业网站、电子商务行业都进行了各种各样的防护措施。

(5)认证。良好的认证体系可防止攻击者假冒合法用户。

(6)备份和恢复。良好的备份和恢复机制可在攻击造成损失时,尽快地恢复数据和系统服务。这是最后的也是最重要的保险。

(7)多层防御。攻击者在突破第一道防线后,可以延缓或阻断其到达攻击目标。

(8)隐藏内部信息。这样使攻击者不能了解系统内的基本情况。

(9)设立安全监控中心。为信息系统提供安全体系管理、监控及紧急情况服务。

维护网络安全的具体手段如下。

①物理措施。保护网络关键设备,制定严格的网络安全规章制度,积极采取防干扰、防火以及防断电等措施。

②访问控制。对用户访问网络资源的权限进行严格的认证和控制,如进行身份认证、对口令加密、设置用户访问目录和文件的权限、控制网络设备配置的权限等。

③网络隔离。网络隔离有两种方式,一种是采用硬件隔离卡来实现,另一种是采用网络安全隔离网闸实现。隔离卡主要用于对单台机器的隔离,网闸主要用于对于整个网络的隔离。两者的区别可参见相关资料。

④数据加密。数据加密是对网络中的数据进行加密,到达目的地后再解密还原为原始数据,目的是防止非法用户截获后盗用信息。例如,可以采用一定的算法将重要信息隐藏在一幅电子图片中,即使被盗取,也不会得到有用信息。

⑤防火墙技术。防火墙技术是通过网络的隔离和限制访问等方法来控制网络的访问权限。

三、主要网络安全工具

1. 网络防火墙

网络防火墙是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所



有网络通信均要经过此防火墙。防火墙对流经它的网络通信进行扫描,这样能够过滤掉一些攻击,以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口,还能禁止特定端口的通信流出。另外,它可以禁止来自特殊站点的访问,从而防止入侵者的所有通信。它能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问,而外部的哪些人可以访问系统内部,以及哪些外部服务可以被内部人员访问。要使一个防火墙有效,所有信息都必须经过防火墙,接受防火墙的检查。防火墙只允许授权的数据通过,并且防火墙本身也必须能够免于渗透。

如果没有防火墙,内部网络上的每个节点都暴露给因特网上的其他主机,极易受到攻击。另外,对于网络管理员,如果不能及时响应报警并审查常规记录,防火墙就形同虚设。

2. 安全路由器

目前,大多数路由器都具备了很好的防火墙功能,还有一些有用的 IDS/IPS 功能,强壮的 QoS 和流量管理工具,当然还有很强大的 VPN 数据加密功能。现代的路由器完全有能力为网络增加安全性。

3. 防病毒工具

现在有很多免费和专用的防病毒软件。防病毒软件要不断升级才能持续有效。即使有了防病毒软件也不能高枕无忧,还要安装系统与 IE 的漏洞补丁,这样才能最大限度地保障计算机的安全。

任务实施

- (1) 上网搜寻黑客的手段,撰写总结报告。
- (2) 查找目前网络安全被破坏而造成巨大损失的案例,并进行分析讨论。
- (3) 安装多款防病毒软件,在使用层面进行对比测试。
- (4) 安装防火墙软件,并依照说明进行配置,掌握防火墙软件的使用方法。
- (5) 了解数字签名的相关知识和应用。
- (6) 安装 SNMP(简单网络管理协议)并进行配置。



项目归纳总结

本项目介绍并实际操作了一些常用的网络命令行工具,如 ipconfig、ping、tracert、route 等。这些命令行工具对于网络的诊断和测试来说非常重要,一定要熟练运用。每个命令行工具都带有一些参数,不容易记忆,也不需要记忆,可根据信息提示来使用。在网络应用中,重点介绍了几种服务器的特点、作用和架设方法。每种服务器的构建可采用不同的软件和手段,可以多尝试、多比较。在配置时要理解含义而不是死记硬背。可以尝试自己动手建立一个对外公开的网站。在网络安全方面,重点要知道防范措施和工具的使用,如防火墙、防病毒软件等。多搜集黑客技术,多了解其攻击思路,从相反方面可以提高对构建网络安全措施的理解。



知识与能力考核

课程名称:网络与综合布线系统工程技术		授课地点:		
项目三:网络的测试与诊断		授课教师:	授课学时:	
课程性质:理实一体课程		综合评分:		
知识掌握情况评分(35分)				
序号	知识考核点	教师评价	配 分	实际得分
1	掌握常用的网络命令行工具		10	
2	掌握邮件服务器的构建方法		5	
3	掌握 FTP 服务器的构建方法		10	
4	掌握 Web 服务器的构建方法		5	
5	掌握网络安全防范的概念		5	
工作任务完成情况评分(65分)				
序号	能力操作考核点	教师评价	配 分	实际得分
1	能够正确使用网络命令行工具		25	
2	能够正确构建 Web 服务器		10	
3	能够正确构建 FTP 服务器		10	
4	能够构建邮件服务器		10	
5	能够正确安装并配置网络防火墙		10	
违规扣分(50分)				
序号	违规内容	教师评价	配 分	实际扣分
1	设备、仪器、仪表损坏		10	
2	课上不参与小组工作		15	
3	严重旷课、缺课		15	
4	严重干扰课堂秩序		10	



自测题

1. 网络服务器有哪些?各自的用处是什么?
2. ipconfig、ping、route 命令的作用是什么?
3. 如何测试计算机与网易网站的连接经过了哪些路由器?



4. ping 127.0.0.1 是在检测什么?
5. 什么是 Web 服务器? 如何建立 Web 服务器?
6. 邮件服务器和办公 OA 系统有何不同?
7. 请建立一个局域网内使用的 FTP 服务器。
8. 在内网中建立的 FTP 服务器如何能让外网的人使用?
9. 练习制作某网站,可以在内网中运行。
10. 维护网络安全的技术有哪些?