

清华大学计算机基础教育课程系列教材

计算机网络(第2版) 习题解答与实验指导

张曾科 马喜春 关敬敏 编著

清华大学出版社
北 京

内 容 简 介

本书是和清华大学出版社出版的教材《计算机网络》(第 2 版)配套的习题解答和实验指导,共编写 351 道习题和解答,9 个实验和实验指导。这些习题和实验,反映了计算机网络原理和技术的知识点,有助于学生进一步加深对计算机网络基本概念的理解,有助于学生掌握计算机网络应用的技能,培养实践动手能力。

本书可以作为高等院校非计算机专业本科生和研究生学习计算机网络课程的辅助教材,也可供广大工程技术人员参考。

版权所有,翻印必究。举报电话: 010-62782989 13501256678 13801310933

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。

图书在版编目(CIP)数据

计算机网络(第2版)习题解答与实验指导/张曾科,马喜春,关敬敏编著. —北京:清华大学出版社, 2005. 11
(清华大学计算机基础教育课程系列教材)
ISBN 7-302-11810-8
. 计... . 张... 马... 关... . 计算机网络 - 高等学校 - 教学参考资料 . TP393
中国版本图书馆 CIP 数据核字(2005)第 106227 号

出 版 者: 清华大学出版社	地 址: 北京清华大学学研大厦
http:// www .tup .com .cn	邮 编: 100084
社 总 机: 010-62770175	客户服务: 010-62776969
组稿编辑: 张 龙	
文稿编辑: 顾 冰	
印 刷 者: 北京密云胶印厂	
装 订 者: 三河市新茂装订有限公司	
发 行 者: 新华书店总店北京发行所	
开 本: 185×260 印张: 13.75 字数: 319 千字	
版 次: 2005 年 11 月第 1 版 2005 年 11 月第1次印刷	
书 号: ISBN 7-302-11810-8/ TP · 7678	
印 数: 1~4000	
定 价: 19.00 元	

序

计算机科学技术的发展不仅极大地促进了整个科学技术的发展,而且明显地加快了经济信息化和社会信息化的进程。因此,计算机教育在各国备受重视,计算机知识与能力已成为 21 世纪人才素质的基本要素之一。

清华大学自 1990 年开始将计算机教学纳入基础课的范畴,作为校重点课程进行建设和管理,并按照“计算机文化基础”、“计算机技术基础”和“计算机应用基础”三个层次的课程体系组织教学:

第一层次“计算机文化基础”的教学目的是培养学生掌握在未来信息化社会里更好地学习、工作和生活所必须具备的计算机基础知识和基本操作技能,并进行计算机文化道德规范教育。

第二层次“计算机技术基础”是讲授计算机软硬件的基础知识、基本技术与方法,从而为学生进一步学习计算机的后续课程,并利用计算机解决本专业及相关领域中的问题打下必要的基础。

第三层次“计算机应用基础”则是讲解计算机应用中带有基础性、普遍性的知识,讲解计算机应用与开发中的基本技术、工具与环境。

以上述课程体系为依据,设计了计算机基础教育系列课程。随着计算机技术的飞速发展,计算机教学的内容与方法也在不断更新。近几年来,清华大学不断丰富和完善教学内容,在有关课程中先后引入了面向对象技术、多媒体技术、Internet 与互联网技术等。与此同时,在教材与 CAI 课件建设、网络化的教学环境建设等方面也正在大力开展工作,并积极探索适应 21 世纪人才培养的教学模式。

为进一步加强计算机基础教学工作,适应高校正在开展的课程体系与教学内容的改革,及时反映清华大学计算机基础教学的成果,加强与兄弟院校的交流,清华大学在原有工作的基础上,重新规划了“清华大学计算机基础教育课程系列教材”。

该系列教材有如下几个特色:

1. 自成体系:该系列教材覆盖了计算机基础教学三个层次的教学内容。其中既包括所有大学生都必须掌握的计算机文化基础,也包括适用于各专业的软、硬件基础知识;既包括基本概念、方法与规范,也包括计算机应用开发的工具与环境。
2. 内容先进:该系列教材注重将计算机技术的最新发展适当地引入教学中来,保持了教学内容的先进性。例如,系列教材中包括了面向对象与可视化编程、多媒体技术与应用、Internet 与互联网技术、大型数据库技术等。

3. 适应面广：该系列教材照顾了理、工、文等各种类型专业的教学要求。
4. 立体配套：为适应教学模式、教学方法和手段的改革,该系列教材中多数都配有习题集和实验指导、多媒体电子教案,有的还配有 CAI 课件以及相应的网络教学资源。
- 本系列教材源于清华大学计算机基础教育的教学实践,凝聚了工作在第一线的任课教师的教学经验与科研成果。我希望本系列教材不断完善,不断更新,为我国高校计算机基础教育做出新的贡献。



注：周远清,曾任教育部副部长,原清华大学副校长、计算机专业教授。

前言

计算机网络特别是 Internet 的飞速发展在现代科学技术史乃至人类发展史上都具有划时代的意义和重大的影响。

计算机网络为人们在全世界范围内的信息交流铺设了四通八达的信息高速公路。计算机网络彻底改变了人们的工作、社会活动和生活方式,改变了企事业单位的运营和管理方式。电子商务、网络会议、IP 电话、远程教学和网上会诊,人们的工作变得如些便捷。发往大洋彼岸的电子邮件数分钟就可以送达,异国图书馆的文献资料片刻就可以下载查阅。坐在计算机前,人们就可以浏览全世界网站中各种感兴趣的多媒体信息。小小屏幕连接了全球,大千世界尽收眼底。

今天,掌握计算机网络知识和技术已经成为人们特别是青年一代必备的技能。计算机网络也是目前各类大学教学中都普遍开出的重要课程。

在清华大学非计算机专业学生计算机网络教学的基础上,我们编写出版了教材《计算机网络》(第 2 版)(张曾科编著),由清华大学出版社 2005 年出版。本书是其配套的习题解答与实验指导书。

计算机网络是一门技术性、实践性和实用性很强的学科,为了加强对计算机网络基本原理和技术的理解和掌握,培养计算机网络应用的技能和实践动手能力,我们为《计算机网络》(第 2 版)编写了这本配套的辅助教材。针对计算机网络基本原理和技术中重要的知识点和网络应用中的基本技能,给出了 351 道习题和解答,9 个实验和实验指导,以期对读者的学习有所帮助和裨益。

本书可以作为高等院校非计算机专业本科生和研究生计算机网络课程的辅助教材,也可供广大工程技术人员作为学习、使用计算机网络的参考。

本书习题部分由张曾科和关敬敏编写,实验部分由马喜春编写。由于作者的学识和水平有限,书中难免存在错误和疏漏之处,殷切希望广大读者批评指正。

作 者

2005 年仲夏 于清华园

目 录

第 1 部分 习 题 解 答

第 1 章	计算机网络概述.....	3
第 2 章	计算机网络体系结构	10
第 3 章	数据通信技术	15
第 4 章	数据链路控制	25
第 5 章	局域网体系结构	36
第 6 章	以太网	39
第 7 章	非主流局域网	59
第 8 章	无线局域网(WLAN)	63
第 9 章	广域网传输控制机制	67
第 10 章	广域网实例.....	70
第 11 章	网际层.....	77
第 12 章	传输层	101
第 13 章	应用层	111
第 14 章	Socket 网络通信程序设计	126
第 15 章	网络安全	134

第 2 部分 实 验 指 导

实验一	以太网组建.....	147
1.1	实验设备、器件及测量工具.....	147
1.2	网络连通性测试	150
1.3	多个集线器相连	150
实验二	虚拟局域网.....	151
2.1	实验内容	151
2.2	实验环境	151
2.3	实验步骤	152
实验三	FTP 服务器的配置与管理	161
3.1	实验目的	161
3.2	启动管理控制台	161
3.3	配置 FTP 站点属性.....	162

实验四	Web 服务器的配置	164
4.1	实验目的	164
4.2	实验准备	164
4.3	Web 服务器的配置	164
实验五	DNS 服务器的配置与管理	167
5.1	实验目的	167
5.2	启动 DNS 管理控制台	167
5.3	DNS 配置与管理	168
实验六	电子邮件服务器的配置与管理	173
6.1	实验目的	173
6.2	Imail 的配置与管理	173
6.3	Imail 的使用	177
6.4	客户端使用 Outlook Express 发送/ 接收邮件	179
实验七	DHCP 服务器的配置与管理	185
7.1	实验目的	185
7.2	DHCP 服务的安装	185
7.3	DHCP 服务器的授权	186
7.4	DHCP 服务器的配置与管理	187
7.5	DHCP 服务的测试	192
实验八	常用网络操作命令	194
8.1	实验目的	194
8.2	常用命令	194
实验九	Socket 网络通信程序设计	201
9.1	实验目的	201
9.2	实验条件	201
9.3	实验内容	201
9.4	实验报告	202
9.5	Linux 下常用的指令介绍	202
9.6	Linux 下常用套接字相关函数简介	203
9.7	Socket 网络通信编程实例	204
参考文献		210

第一部分

习题解答

- 第 1 章 计算机网络概述
- 第 2 章 计算机网络体系结构
- 第 3 章 数据通信技术
- 第 4 章 数据链路控制
- 第 5 章 局域网体系结构
- 第 6 章 以太网
- 第 7 章 非主流局域网
- 第 8 章 无线局域网(WLAN)
- 第 9 章 广域网传输控制机制
- 第 10 章 广域网实例
- 第 11 章 网际层
- 第 12 章 传输层
- 第 13 章 应用层
- 第 14 章 Socket 网络通信程序设计
- 第 15 章 网络安全

第 1 章

计算机网络概述

1-1 什么是计算机网络？它由哪些部分组成？它的主要应用是什么？

解答：计算机网络是指自治的计算机 (autonomous computers) 互连起来 (interconnected) 的集合。计算机之间如果能相互通信则称为互连，自治是指计算机是能够独立进行处理的设备，而不是无自行处理能力的附属设备 (如终端)。

计算机网络主要由下列部分组成。

1. 硬件

计算机 按着 ARPANET 沿用下来的术语，也称为主机 (host) 或端系统 ES (end systems)。可以是个人计算机、大型计算机、客户机 (client) 或称工作站 (workstation)、服务器 (server) 等。

通信设备 即中间系统 IS (intermediate systems)，如交换机 (switch) 和路由器 (router) 等，为主机转发数据。端系统和中间系统在网络中称为结点 (node)。

接口设备 网络接口卡 NIC，调制解调器等，作为计算机与网络的接口。

传输媒体 双绞线、同轴电缆、光纤、无线电和卫星链路等。

2. 软件

通信协议 即传输规则，如 TCP, IP, PPP, HTTP 等。

应用软件 如 Web, NFS 等。

计算机网络提供各种各样的应用服务，主要包括如下几类：

共享资源访问 如 Web, FTP 等。

远程用户通信 如 E-mail, IP 电话, 网络会议等。

网上事务处理 如电子商务, 电子政务, 网上储蓄等。

1-2 按覆盖地域划分，计算机网络分为哪几类？它们各自的特点是什么？

解答：按网络覆盖的地域范围计算机网络可以分为三类，即局域网 (LAN)、城域网 (MAN) 和广域网 (WAN)，此外，互联网是若干个 LAN、MAN 或 WAN 互连在一起的集合，目前全世界绝大多数网络都互连在一起，形成了因特网，从覆盖的地域范围的角度讲，它是当今世界上最大的 WAN。

1. 局域网 (LAN) 的主要特点

地理范围有限，通常在 10km 以内。

具有较高的带宽，数据传输率高，一般为 10 ~ 100Mb/s，随着技术的发展，信息传输速率在不断提高。

数据传输可靠,误码率低。误码率通常为 $10^{-7} \sim 10^{-12}$ 。

一般为广播式网络。广播网络上的多台主机共享一条信道,一台主机发送信息,所有主机都能收到。多台主机同时访问信道时就可能产生冲突,因此共享信道的访问控制是首先要解决的问题。

大多数 LAN 采用总线、环型及星型拓扑结构,结构简单,易于实现。

通常是由单一组织专有和使用,容易进行设备的更新和使用最新技术不断增强网络的功能。

2. 广域网(WAN)的特点

WAN 覆盖的地域在 100 公里以上,甚至数千公里,可以覆盖一个地区、一个国家、一个洲甚至更大。

WAN 一般由主机和通信子网组成,通信子网由通信线路和交换机或路由器等交换结点组成,它往往借助于电信部门的公共通信网。

WAN 多为点对点网络,由许多连接构成,每一连接对应一对结点。点对点网络是一种交换式网络。交换式网络的数据传输过程有两个重要特点:一是需要使用交换技术,交换即数据在结点间的转接。WAN 使用最多的是分组交换。二是路由技术,网络要为分组选择一条到达目的结点的合适的路径。

WAN 常常采用多路复用技术,提高传输线路的利用率。LAN 不使用多路复用。

WAN 网络拓扑则一般比较复杂、不规整,多为网状和树型,或者它们的混合。

LAN 通信协议结构包括物理层和数据链路层两层,重点是数据链路层如何解决信道的多点访问控制,而 WAN 通信协议结构还要加上网络层,重点是网络层的路由问题。

3. 城域网(MAN)

MAN 规模介于 LAN 和 WAN 之间,局限在一座城市的范围内,一般在 10 ~ 100km 的区域。MAN 也是公共网络性质,面向多用户提供数据、语音、图像等多业务的传输服务。

IEEE 专门为 MAN 定义了一个标准 IEEE802 .6,称为分布式队列双总线(DQDB),但 DQDB 并没有得到预期的应用。

由于 LAN 功能的不断提高和 WAN 技术的发展,它们都广泛地渗透和应用到 MAN 领域。迅速发展的以太网技术从 LAN 扩展到了 MAN 领域,千兆位、万兆位以太网是 MAN 可以使用的技术。WAN 中使用的同步光纤网/同步数字分级结构(SONET/SDH)、波分多路复用(WDM)和异步传输模式(ATM)技术以及 LAN 中的光纤分布数据接口(FDDI)技术,也都是 MAN 常常选择使用的技术。

4. 互联网

互联网是由若干个物理网络包括 LAN、MAN 和 WAN 等由称为路由器(或称网关)的网络设备连接在一起形成的,互联网是由路由器互连在一起的物理网络的集合,是网络的网络。互联网覆盖的地域范围与它互连了多少个网络有关。目前全世界绝大多数网络都互连在一起,形成了覆盖了全球的互联网——因特网,仅从覆盖的地域范围的角度讲,它是当今世界上最大的 WAN,但它们使用的技术有所不同。

1-3 什么是互联网？什么是 Internet？

解答：互联网是由若干个物理网络包括 LAN、MAN 和 WAN 等由路由器(或称网关)的网络设备连接在一起组成的，互联网是由路由器互连在一起的物理网络的集合，是网络的网络。

Internet 是使用 TCP/ IP 协议族的覆盖全球范围的当今最大的开放的互联网。Internet 已经过了几十年的发展演变过程，目前的 Internet 拓扑结构是松散的分层的，不受某个权威部门的控制，在商业利益驱动下扩展演进。Internet 各个层次的网络干线由不同级别的 Internet 服务提供商 ISP 来建立、经营并向社会提供网络服务。

1-4 试画出 LAN(bus 型)、WAN(交换式网络)和互联网的典型的概念结构。

解答：(1) LAN (bus 型)，如图 1-1-1 所示。



图 1-1-1 LAN 示意图

(2) WAN(交换式网络)，如图 1-1-2 所示。



图 1-1-2 WAN 示意图

(3) 互联网，如图 1-1-3 所示。

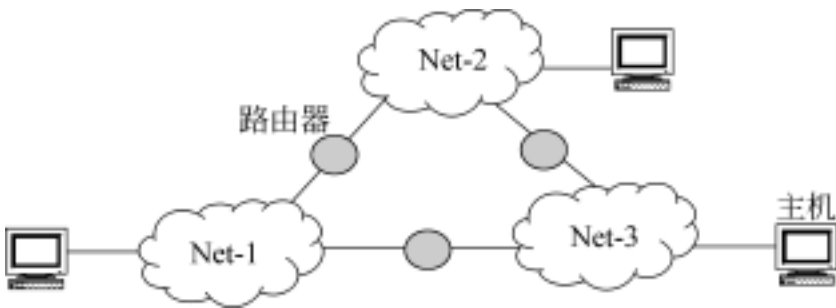


图 1-1-3 互联网示意图

1-5 TCP/ IP 实现网络互联的关键思想是什么？

解答：TCP/ IP 技术的核心是实现网络的互联，其关键的思想是在底层物理网络与高层应用程序和用户之间加入中间层次，屏蔽底层细节，向用户提供通用一致的网络服务。在用户看来，整个互联网是一个统一的整体，虽然在物理上由很多使用不同标准的各种类型的网络互连而成，但在逻辑上是一个统一的网络，提供通用一致的网络服务。

1-6 什么是 ISP？它分为哪几个级别？说明各个级别的 ISP 网络如何组成 Internet，并用图形表示。

解答: ISP(Internet service provider) 意思是 Internet 服务提供商, Internet 各个层次的网络干线由不同级别的 ISP 来建立、经营并向社会提供网络服务。

ISP 可分为本地级、地区级和主干级(BSP), BSP 一般指国家级和国际级的 ISP。大学、公司和企业等可以作为本地 ISP, 本地 ISP 也可以是专门提供网络服务的 ISP。用户的网络、工作站和服务器等可以连接到本地 ISP。本地 ISP 又接入到地区级 ISP, 有时候本地 ISP 也可以直接接入到 BSP。

各级 ISP 都设有网络中心供下一级的 ISP 或用户接入, 网络中心必须有必要的设备, 如路由器、交换机和调制解调器等, 接入点称为存在点 POP (point of presence)。

BSP 要相互连接, 构成一个整体的连通的网络。BSP 一般通过网络接入点 NAP (network access point) 进行连接, NAP 担负着中转巨大网络流量的重任, 通常使用高速交换设备。

Internet 分层的网络结构可用图 1-1-4 表示。

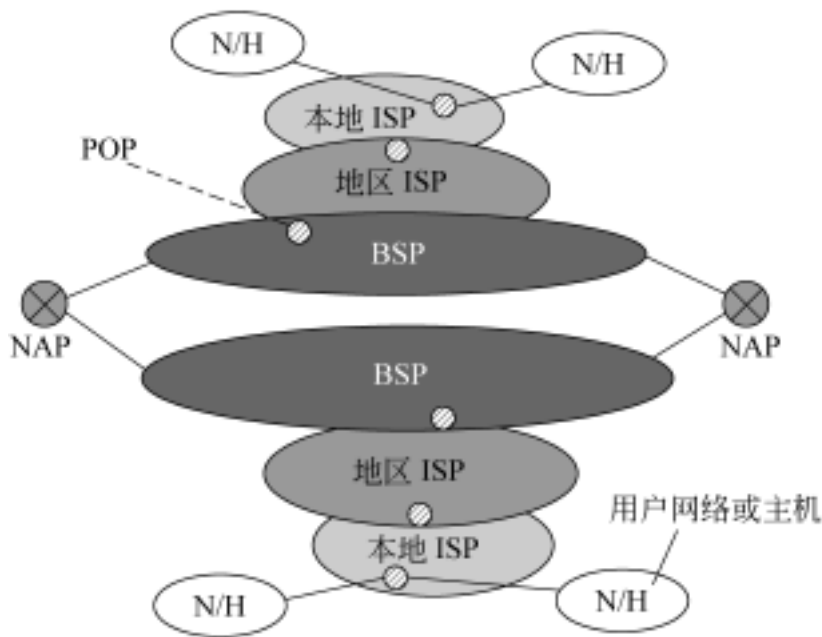


图 1-1-4 Internet 分层的网络结构图

1-7 计算机网络经历了怎样的发展历程? 各个发展阶段的特点是什么?

解答: 计算机网络经历了近半个世纪的发展历程, 大体经历了以下几个发展阶段:

1. 计算机网络的产生

20 世纪 50 年代中期计算机网络产生。早期的计算机网络是计算机和电话通信系统相结合的产物, 是以单台计算机为中心的远程联机系统。连接到中心计算机的终端并没有自主处理能力, 它们使用中心计算机的处理能力。

2. 分组交换网的出现

60 年代后期, 分组交换网的出现, 计算机网络的发展进入了一个新阶段。分组交换网是将多台具有自主处理能力的计算机用通信线路连接起来计算机网络系统, 计算机之间的数据传输使用分组交换方式。这个阶段的分组交换网的典型代表是 ARPANET。

3. 计算机网络体系结构的形成

70 年代到 80 年代, 世界出现了大量的计算机网络, 但它们没有统一的网络体系结构, 难以实现互连, 不能适应更大范围的信息交流与资源共享。

1983 年国际标准化组织 ISO 制定出了开放系统互连基本参考模型(OSI RM)和相关的一系列协议,形成了 OSI 网络体系结构。OSI 标准的基本宗旨就是开放,遵循该国际标准的系统都是相互开放的,能够实现互连。但由于种种原因,OSI 体系结构并没有得到推广。

70 年代末期推出了 TCP/ IP 协议规范,1983 年,ARPANET 上的所有计算机转向 TCP/ IP 协议,并以 ARPANET 为主干建立了 Internet,形成了 TCP/ IP 体系结构。TCP/ IP 体系结构虽然不是国际标准,但它的发展和应用都远远超过了 OSI,成为了事实上的标准。

4. 局域网的产生和发展

LAN 的产生和发展是计算机网络发展中的一个重要事件。LAN 在 70 年代产生,80 年代 LAN 蓬勃发展,多种类型的 LAN 纷纷出现,90 年代后 LAN 成熟。超大规模集成电路技术的发展大大促进了微型计算机技术的发展,大大推动了微型机局域网 PC-LAN 的发展。

以太网是今天 LAN 的主流网络。其速度已由原来的 10Mb/s 提高到现在的 10Gb/s。现在,全世界大部分 LAN 都是以太网,保持了支配性的市场地位。

5. Internet 时代

90 年代以后,计算机网络进入了 Internet 时代。Internet 发展成全球规模最大、增长速度最快的计算机互联网。因特网的应用从用于科研、教育到商用,逐步深入到人类社会生活的各个角落。它大大地改变了人类的生产、工作、生活和思维方式,因特网对人类社会的发展产生了极为深远的影响。

时代的发展对 Internet 提出了新的要求和挑战,不断地发展 Internet 人类共同的任务。下一代 Internet 应该更快、更大、更安全、更高的服务质量和更方便的使用。现在,世界各国的网络科学家都在致力于下一代 Internet 的研究和发展。

1-8 什么是计算机网络的体系结构?两个最著名的计算机网络体系结构是什么?它们发展的结果如何?

解答:计算机网络通常按功能分为若干个层次(layer)。网络中计算机之间要进行正常有序的通信,必须有一定的约定,如信息应按什么顺序进行交互,信息应该如何表示等,称为协议(protocol),协议是同等层次之间信息交互的规则。计算机网络的层次结构及各层协议的集合统称计算机网络的体系结构(architecture)。

两个最著名的计算机网络体系结构是国际标准化组织 ISO 制定的 OSI 网络体系结构和在 Internet 中使用的 TCP/ IP 体系结构。前者受到市场、商业运作和技术等诸多因素的制约,并没有得到预期的推广应用;后者虽然不是国际标准,但它与 Internet 一起推广,其发展和应用远远超过了 OSI,成为了事实上的标准。

1-9 试画出远程联机系统的结构图,它为什么要采用前端处理机和集中器?

解答:远程联机系统的结构图如图 1-1-5 所示。

前端处理机 FEP 分工负责和远程终端通信的任务,中心计算机则专门进行数据运算和处理,减轻了中心计算机的负担,提高了处理效率。集中器可连接多台终端,共享一条通信线路,提高了通信线路的利用率,降低了通信线路的使用费用。

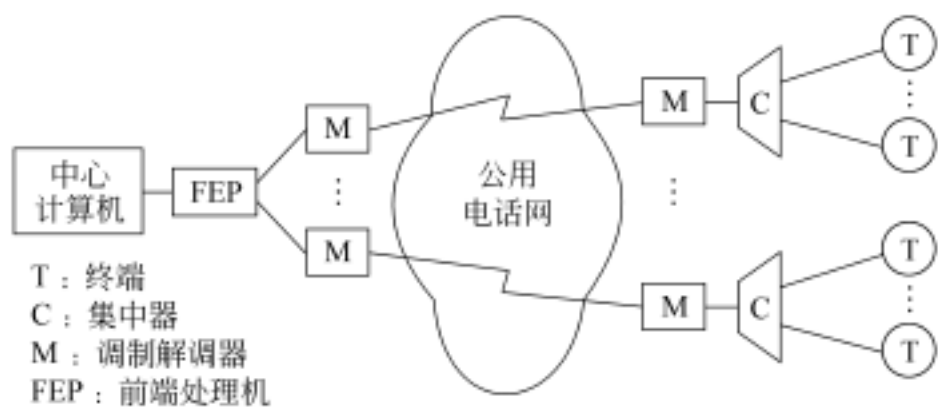


图 1-1-5 远程联机系统结构图

1-10 试画出 ARPANET 的结构图,它划分为哪两种子网?它传输的基本信息单位是什么?用什么方式传输?这种传输方式的优点是什么?

解答:图 1-1-6 是 ARPANET 的结构图。图中,H 代表主机,IMP 代表接口报文处理机,它专门负责通信处理。

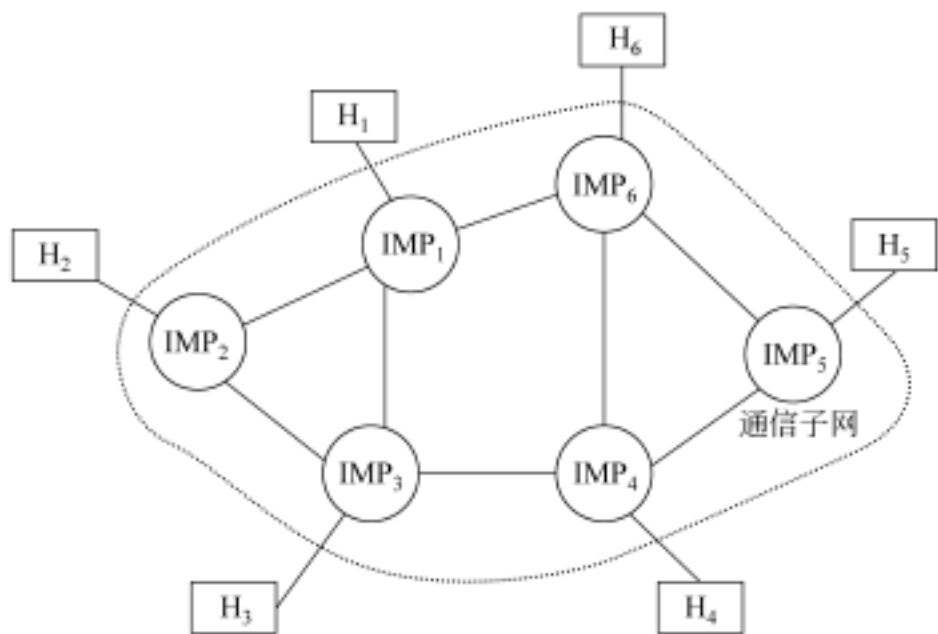


图 1-1-6 ARPANET 结构图

ARPANET 划分为通信子网和资源子网。接口报文处理机及其互连的网络负责通信任务,它们构成了通信子网;网上的主机运行各种应用程序,向网络用户提供各种软件和硬件资源,它们构成资源子网。

ARPANET 中传输的基本信息单位称为分组(或包,packet),用分组交换的方式进行传输,即以存储转发的方式传输分组。

相对于传统的电话网的电路交换方式,这种传输方式的主要优点是通信线路不为某一对结点的通信所独占,可以为多路通信所用,提高了通信线路资源的利用率。

1-11 Internet 的前身是什么?后来它采用了什么著名的网络协议?

解答:Internet 的前身是 ARPANET。1969 年美国国防部高级研究计划局 DARPA 资助建立了一个有 4 个结点的分组交换网——ARPANET,Internet 是从 ARPANET 起步逐步发展壮大起来的。

80 年代初期在 ARPANET 上使用了 TCP/IP 协议,使网络互连成为现实,为因特网

的发展注入了活力。

1-12 Internet 协议标准以什么文档形式发表？对该文档进行简单介绍。

解答：Internet 协议标准以 RFC 文档形式发表，RFC(request for comments)的意思是请求评注。

并不是所有的 RFC 文档都是 Internet 协议标准。任何人都可通过 RFC 发表对 Internet 某些技术的建议，但只有其中的一部分最终才能成为真正的标准。

RFC 文档总体上可以分为 3 类：标准化进程中的(Standards Track)、最好的当前实践 BCP(Best Current Practice)和非标准的(Non-Standards)。

标准化进程中的 RFC 描述正在标准化的协议。一个 Internet 协议标准是由 Internet 草案(Internet draft)开始，然后还要历经三个成熟水平阶段：建议标准(proposed standard)、草案标准(draft standard)和最终的因特网标准(Internet standard)，这三个阶段有相应的 RFC 文档。一旦最终成为因特网标准，就被分配一个 STD 序号 STD #。

BCP 类的 RFC 文档是某些操作规则或 IETF 处理工作方式的标准，它们被给予一个 BCP 序号 BCP #。例如说明标准化程序的 RFC2026(BCP9)就是一例。

非标准的 RFC 文档包括实验的(Experimental)、报告的(Informational)和历史的(Historic)。实验的 RFC 文档可以是 IRTF 下属研究组 RG 或 IETF 下属工作组 WG 的研究结果报告或个人的成果。报告的 RFC 文档来自各个方面，不代表一个 Internet 团体的一致意见或推荐，包括对常见操作问题的回答等。历史的 RFC 文档可以是被新的文档代替的或标准化进程中被中止的。

第 2 章

计算机网络体系结构

2-1 ISO 定义计算机网络体系结构的宗旨是什么？

解答：ISO 定义的 OSI 计算机网络体系结构的宗旨是开放。在 OSI 网络体系结构之前的 SNA、DNA 和 DSA 等计算机网络体系结构都是封闭的，相互难以通信。开放意即不封闭，只要遵循 OSI 规范，一个系统就可以和另外一个也遵守 OSI 规范的任何其他系统互通信。

2-2 ISO 的 OSI/ RM 分为哪几个层次？分层的好处是什么？

解答：ISO 的 OSI/ RM 划为 7 个层次，如表 1-2-1 所示。

表 1-2-1 OSI/ RM 划分的 7 个层次

层号	中文名称	英文名称	英文缩写
7	应用层	application layer	A
6	表示层	presentation layer	P
5	会话层	session layer	S
4	传输层	transport layer	T
3	网络层	network layer	N
2	数据链路层	data link layer	DL
1	物理层	physical layer	PH

分层的方法有利于计算机网络的设计与实现，其好处主要有两个方面：

简化了网络通信的设计。网络通信是一个非常复杂的过程，把整个的过程划分为几个功能层次，各层分工清晰，层内功能单一、易于实现，使整个系统的设计和实现简单化。不同的系统可以根据各自的具体条件，采用不同的方法和技术实现每个层次的功能。

具有层间无关性，系统易于更新。在层次结构中，高层通过层间接口利用低层所提供的功能，并不需要知道低层如何实现这些功能，低层也仅仅是利用由高层传下来的参数，这就是层间无关性。层间无关性使得硬件和软件出现了新技术的时候，容易对某一层进行更新，以新的方法和新的技术取代老的方法和技术，只要这一更新仍然遵循与相邻层间的接口约定即可。

2-3 简述 ISO 计算机网络体系结构各层的主要功能。

解答：OSI 7 层功能简述如下：

1. 物理层

物理层所处理的数据单位是比特(bit)，物理层向上为数据链路层提供物理链路，实现透明的比特流(bit stream)传输服务，物理层向下与物理媒体相连，要确定连接物理媒体的网络接口的机械、电气、功能和过程方面的特性。

2. 数据链路层

数据链路层负责在单个链路上的结点间传送以帧(frame)为 PDU 的数据，在不太可靠的物理链路上实现可靠的数据传输。数据链路层的主要功能包括：建立、维持和释放数据链路的连接，链路的访问控制，流量控制和差错控制。

3. 网络层

网络层传送的 PDU 称为分组或包(packet)，在物理网络间传送分组，负责将源端主机的报文通过中间转发结点传送到目的端。网络层是通信子网的最高层，为主机提供虚电路和数据报两种方式的服务。网络层主要负责分组转发和路由选择，根据路由表把分组逐跳地由源站传送到目的站，并能适应网络的负载及拓扑结构的变化，动态地更新路由表。

4. 传输层

传输层传输的 PDU 称为报文(message)，传输层为源结点和目的结点的用户进程之间提供端到端的可靠的传输服务。端到端的传输指的是源结点和目的结点的两个传输层实体之间，不涉及路由器等中间结点。为了保证可靠的传输服务，传输层具备以下一些功能：面向连接、流量控制与拥塞控制、差错控制和网络服务质量的选择等。

5. 会话层

会话层在传输层服务的基础上增加控制会话的机制，建立、组织和协调应用进程之间的交互过程。会话层提供的会话服务种类包括双工、半双工和单工方式。会话管理的一种方式令牌管理，只有令牌持有者才能执行某种操作。会话层提供会话的同步控制，当出现故障时，会话活动在故障点之前的同步点进行重复，而不必从头开始。

6. 表示层

表示层定义用户或应用程序之间交换数据的格式，提供数据表示之间的转换服务，保证传输的信息到达目的端后意义不变。

7. 应用层

应用层直接面向用户应用，为用户提供对各种网络资源的方便的访问服务。

2-4 在 OSI 术语中什么是实体？什么是对等实体？

解答：实体(entity)是每一层中实现该层功能的软件或硬件，在发送端与接收端同一层次中的实体称为对等实体(peer entities)，在概念上信息是在同一层次中的同等实体之间进行虚拟的传输，协议也是同等层次实体之间的传输控制规程。

2-5 在 OSI 术语中，什么是协议？协议包括哪些要素？它们的含义是什么？

解答：协议(protocol)是某一个层次中对等实体之间通信的控制规程。

协议包含三个方面的要素：

(1) 语法：语法用来规定由协议的控制信息和传送的数据所组成的传输信息应遵循

的格式,即传输信息的数据结构。

(2) 语义:语义是指对构成协议的各个协议元素的含义的解释,不同的协议元素规定了通信双方所要表达的不同含义。

(3) 同步:它规定实体之间通信的操作执行的顺序,协调双方的操作,使两个实体之间有序地进行合作,共同完成数据传输任务。

2-6 在 OSI 术语中,什么是协议数据单元(PDU)?PDU 包含哪两个部分?

解答:各层对等实体之间在协议控制下交换的数据块称为协议数据单元(protocol data unit,PDU)。PDU 包括本层的协议控制信息和用户数据,本层的用户数据就是上层的 PDU。

2-7 在 OSI 术语中,什么是服务?什么是服务访问点(SAP)?什么是服务原语?

解答:在 OSI 网络中,(N)实体在(N)协议的控制下可以向(N+1)实体提供服务,实现某种(N+1)层所需要的功能,只有能为(N+1)层所使用的功能才称为(N)服务,其中(N)实体为服务提供者,(N+1)实体为服务用户。

在同一结点中,相邻两层的实体相互作用的地方称为服务访问点(SAP)。SAP 是上下层实体之间信息交换的接口。

服务用户与服务提供者之间的交换信息使用服务原语来描述。服务原语描述提供的服务,定义服务规范,规定通过 SAP 所必须传递的信息。服务原语只是对服务进行概念性的功能描述,它是描述服务的一种简洁的语句形式,而不是可执行的程序语言。一个完整的服务原语包括名字、类型和参数,例如一个请求建立传输连接的原语是 T-CONNECT.request(被叫地址,主叫地址,...),其中:T-CONNECT 是原语名字,request 是原语类型,括弧中是原语参数。

2-8 所谓“透明传输”是什么含义?

解答:透明传输(transparent transmission)是指所传输的数据块中不管包含什么样的数据,都能够正常进行传输。透明传输功能对上层用户而言是透明的,什么样的数据都能传输,不必进行任何处理。当所传输的数据恰巧与某一控制码完全一样时,必须采取适当措施,使收方不致误认为是控制信息。比如高级数据链路控制 HDLC 使用的位插入方法实现透明传输。

2-9 请填充:RS-232C 是()层的协议,它使用()连接器,使用()V 到()V 电压表示逻辑“1”,使用()V 到()V 电压表示逻辑“0”。

解答:RS-232C 是(物理)层的协议,它使用(25 芯 D 型)连接器,使用(-5)V 到(-15)V 电压表示逻辑“1”,使用(+5)V 到(+15)V 电压表示逻辑“0”。

2-10 传输层为应用进程提供端到端(end to end)的传输服务,这里“端到端”指的是什么?

解答:传输层为应用进程之间提供端到端(end to end)的传输服务,为应用进程提供一条端到端的逻辑信道。这里“端到端”是指源结点和目的结点的两个传输层实体,不涉及网络中的路由器等中间结点。

2-11 TCP/IP 体系结构分为哪几个层次?它们和 ISO/OSI 各层的对应关系如何?

解答:TCP/IP 的体系结构分为 4 个层次,即应用层、传输层、网际层和网络接口层,

不过最下面的网络接口层并没有什么具体的内容。图 1-2-1 给出了 TCP/ IP 的层次结构及与 OSI/ RM 的对应关系。

OSI	TCP/ IP
高层(5 ~ 7)	应用层
传输层(4)	传输层
网络层(3)	网际层
低层(1 ~ 2)	网络接口层

图 1-2-1 TCP/ IP 的层次结构及与 OSI/ RM 的对应关系

2-12 简述 TCP/ IP 体系结构各层的功能,试举出每层的几个主要协议。

解答: TCP/ IP 体系结构各层的简要功能和包含主要协议是:

1 . 网络接口层

负责将网络层的 IP 数据报通过物理网络发送,或从物理网络接收数据帧,抽出 IP 数据报上交网际层。TCP/ IP 标准并没有定义具体的网络接口层协议,只是一个接口,以衔接不同的物理网络。网络接口层使得上层的 TCP/ IP 和底层的物理网络无关。

2 . 网际层

也称互联网层,提供的一种无连接的、不可靠的但尽力而为的数据报传输服务。网际层传送的数据单位是 IP 数据报(IP datagram),也就是分组。网际层最主要的协议是网际协议 IP。与 IP 协议配套的网际协议还有:地址解析协议(ARP),逆向地址解析协议(RARP)和网际控制报文协议(ICMP)等。

3 . 传输层

为应用进程之间提供端到端的传输服务。TCP/ IP 在传输层主要提供了两个协议,即传输控制协议(TCP)和用户数据报协议(UDP)。TCP 提供面向连接的可靠的传输服务,它可在低层不可靠的情况下(如出现分组传输的丢失、乱序等)使用各种传输控制机制,以保证传输的可靠性。UDP 提供无连接、不可靠的传输服务,但它传输的效率高。

4 . 应用层

提供面向用户的网络服务。在这个层次中有许多面向应用的著名协议。如简单邮件传送协议(SMTP)、域名系统(DNS)、超文本传输协议(HTTP)、简单网络管理协议(SNMP)文件传输协议(FTP)和远程通信协议(Telnet)等。

2-13 在 OSI 参考模型中,物理层的功能是__(1)___。对等实体在一次交互作用中传送的信息单位称为__(2)___,它包括__(3)___两部分。上下邻层实体之间的接口称为__(4)___。

- (1) A . 建立和释放连接

B . 透明地传输比特流

C . 在物理实体间传送数据帧

D . 发送和接收用户数据
- (2) A . 接口数据单元

B . 服务数据单元

C . 协议数据单元

D . 交互数据单元
- (3) A . 控制信息和用户数据

B . 接口信息和用户数据

C . 接口信息和控制信息

D . 控制信息和校验信息

- 答案: B, C, A, D

(1) A . 1、2 层 B . 2、4 层 C . 3、5 层 D . 5、6 层

(2) A . 物理层 B . 数据链路层 C . 会话层 D . 传输层

(3) A . 物理层 B . 数据链路层 C . 网络层 D . 传输层

(4) A . 物理层 B . 数据链路层 C . 网络层 D . 传输层

答案: B, D, C, B

- (1) A . 传输层、互联网层、网络接口层和物理层
B . 传输层、互联网层、网络接口层
C . 传输层、互联网层、ATM 层和物理层
D . 传输层、网络层,数据链路层和物理层
- (2) A . 面向连接的、不可靠的
B . 无连接的、不可靠的
C . 面向连接的、可靠的
D . 无连接的、可靠的
- (3) A . 无连接的
B . 面向连接的
C . 无连接的、可靠的
D . 面向连接的、不可靠的
- (4) A . 面向连接的、保证服务质量的
B . 无连接的、保证服务质量的
C . 无连接的、不保证服务质量的
D . 保证服务质量的

答案: B, C, A, C

第 3 章

数据通信技术

3-1 什么是传输信号？它有哪些类？什么是信道？它有哪些类？

解答：传输信号(signal)是数据传输的载体,数据是通过信号进行传输的。数据在发送前要把它转换成某种物理信号,用它的特征参数表示所传输的数据,比如电信号的电平等。实质上,信号在媒体中是通过电磁波进行传输的,因此可以说,传输信号是数据在媒体中传输的电磁波表现形式。传输信号也有模拟信号和数字信号之分。模拟信号是表示数据的特征参数连续变化的信号,而数字信号是离散的信号。

信道(channel)是信号传输的通道。信道一般指连接信号发送方和接收方的传输线路,包括铜缆、光纤等有线传输媒体和无线传输媒体。信道这个词在不同的背景下,可能表示更为广义的概念,比如谈到一个由 4 个粗缆网段组成的以太网信道,除了传输媒体之外,它还包含了 3 个中继器。使用模拟信号传输数据的信道称为模拟信道,使用数字信号传输数据的信道称为数字信道,数字信道有更高的传输质量。

3-2 什么是信息传输速率和码元传输速率？它们之间的关系是什么？

解答：计算机网络的信息传输速率是指每秒传输的数据(编码前的数字数据)的二进制位数,单位为比特/秒,即 b/s 或 bps(bit per second)。信息传输速率又称为比特率。

数字数据经线路编码后的传输信号在信道上的传输速率称为码元传输速率,它是指每秒传输的码元数,即每秒钟传输信号变化的次数,单位为波特(baud)。码元传输速率又称为波特率。

码元传输速率和信号传输速率之间的关系是: $C = B \log_2 M$ (b/s), 其中: C 为信息传输速率, B 为码元传输速率, M 为码元状态数(M 为 2 的整数次幂)。

3-3 若用 -3V、-1V、1V 和 3V 共 4 种电平表示不同的码元状态,对于 4 000baud 的信号传输速率,信息传输速率可以达到多少？如果使用 8 种码元状态呢？

解答：对于 4 000baud 的信号传输速率,信息传输速率可以达到 $C = 4\,000 \log_2 4 = 8\,000$ b/s。如果使用 8 种码元状态,信息传输速率可以达到 $C = 4\,000 \log_2 8 = 12\,000$ b/s。

3-4 计算机的屏幕图像包含 640×480 个像素点,每个像素占 24 个比特,现每秒传输 30 幅屏幕,如果采用四进制编码,问信号能否用 5 类非屏蔽双绞线传输(无噪声)？如果计算机的屏幕图像包含 $1\,024 \times 768$ 个像素点呢？

解答：根据奈奎斯特准则,在一个带宽为 W Hz 的无噪声低通信道上,则最高的码元传输速率 B_{MAX} 为 $2W$ baud,如果编码方式的码元状态数为 M ,那么信道的极限信息传输速率即信道容量 C_{MAX} 为: $C_{\text{MAX}} = 2W \log_2 M$ (b/s)。由于 5 类非屏蔽双绞线的带宽为

100MHz, 当编码方式的码元状态数 M 为 4, 则道的极限信息传输速率为 400Mb/s。

当计算机的屏幕图像包含 640×480 个像素点时, 所需的信息传输速率为: $640 \times 480 \times 24 \times 30 = 221\text{Mb/s}$, 故 5 类非屏蔽双绞线能够传输。如果像素点为 1024×768 , 所需的信息传输速率为 566Mb/s, 故 5 类非屏蔽双绞线不能传输。

3-5 什么是信道的带宽? 单位是什么? 在计算机网络领域, 带宽的含义是什么? 单位是什么?

解答: 信道带宽的定义原本来自通信领域, 原来的通信信道是模拟信道, 带宽是指信道上能够正常通过的模拟的物理信号的频率范围, 即最大最小频率之差, 单位为赫兹(Hz)。

带宽一词后来又借用到计算机网络领域。在计算机网络领域, 通信线路上传输的是数字数据, 人们又沿用已习惯的带宽一词用来表示传输数字数据的能力, 即数字信道的信息传输速率, 单位为 b/s。

3-6 计算机网络数据传输中, 什么是传输时延? 它包括哪几个部分?

解答: 计算机网络数据传输中, 时延(delay)指一个数据块(帧、分组、报文段等)从链路或网络的一端传送到另一端所需要的时间。

时延由以下 3 个部分组成: 发送时间(transmission time)、传播时延(propagation delay)和中间结点的转发时延, 因此:

总时延 = 发送时间 + 传播时延 + 中继结点转发时延。

3-7 卫星通信有较大的传播延时, 如果从地球站到卫星的距离为 40 000km, 问: 从一个地球站经过卫星到另一个地球站的传播延时有多大?

解答: 在自由空间中, 电磁波以光速(speed of light) 300 000km/s 的速度传播, 从一个地球站经过卫星到另一个地球站的距离为 80 000km, 所以传播延时为 $80\,000\text{km} \div 300\,000\text{km/s} = 267\text{ms}$ 。

3-8 什么是信道容量? 它用什么表示? 叙述奈奎斯特准则和香农定理给出的信道容量。

解答: 信道容量(channel capacity)即信道的极限传输能力, 用信道的最大信息传输速率来表示。

奈奎斯特就给出一个准则: 在一个带宽为 $W\text{Hz}$ 的无噪声低通信道上, 则最高的码元传输速率 B_{MAX} 为 $2W\text{baud}$, 如果编码方式的码元状态数为 M , 就得到了信道的信道容量 $C_{\text{MAX}} = 2W\log_2 M$ (b/s)。因为信道总是有噪声的, 因此奈奎斯特准则给出的是理论上的上限。

香农定理给出了有 Gaussian 白噪声干扰情况下的信道容量: $C_{\text{MAX}} = W\log_2(1 + S/N)$ (b/s), 其中: W 为信道的带宽(Hz), S 为信道内所传信号的平均功率, N 为信道内部的高斯噪声功率, S/N 称为信噪比。不管使用多么巧妙复杂的方式编码, 也不能超过此极限速率。

3-9 对于一条带宽为 200MHz 的通信线路, 如果信噪比为 30dB, 其最高信息传输速率能达到多少? 如果信噪比为 20dB 呢?

解答: 信噪比为 30dB 即 $S/N = 1\,000$, 根据香农定理, 最高信息传输速率 $C_{\text{MAX}} =$

$W \log_2 (1 + S/N) = 200 M \log_2 (1 + 1\,000) = 1.99 \text{ Gb/s}$ 。如果信噪比为 20dB, 则 $S/N = 100$, $C_{\text{MAX}} = 200 M \log_2 (1 + 100) = 1.33 \text{ Gb/s}$ 。

3-10 叙述帧同步、位同步和网同步。

解答：当通信在两个点之间进行时, 接收方必须在合适的时刻去测试判断接收到的码元序列, 同步问题有帧同步和位同步。在数据通信中数据经常是以帧为单位传输的, 接收方必须知道收到的帧的起始时刻和结束时刻, 以便接收方时钟对准帧的起始位置, 开始和结束接收数据, 这称为帧同步。另一方面, 接收方定时时钟信号应该和帧的每一码元都对准, 也就是说, 在起始位置对准的前提下, 接收时钟和发送时钟应该有同样的频率和特定的相位关系, 其频率差和相位差保持在允许的容差之内, 这称为位同步, 也称码元同步。

在网络中多结点通信时, 可能还会有新的问题—网同步, 即要求网络的所有结点有统一的基准定时时钟。比如, 在电话主干网时分多路复用 TDM 的数字传输系统中, 如果多路复用设备输入的码流速率都有差异, 处理起来就相当棘手, 需要网同步。

3-11 什么是异步传输方式？

解答：异步传输方式以字符为单位进行数据传输, 每一个字符前后各加一个起始位和一个停止位, 实现字符同步, 通信的双方各自使用独立的基准定位时钟, 但要约定同样的传输速率, 以实现位同步。

3-12 A、B 两台设备进行异步数据传输, 设定为字符位数 8 位、传输速率 9.6kb/s。如果双方的时钟相差 0.1%, 试问每次传输最大能造成多少微秒的累积错位？如果设计要求最大累积错位不超过位宽度的 5%, 是否达到了设计要求？如果双方的时钟相差 1%, 结果又如何？

解答：异步数据传输中, 传输速率 9.6kb/s 则每位时间为: $1\text{b} \div 9.6\text{kb/s} = 104.17\mu\text{s}$, 如果字符位数 8 为位, 加上起始位、奇偶校验位和停止位可以有 12 位, 当双方的时钟相差 0.1%, 最大的累积错位为: $104.17\mu\text{s} \times 12 \times 0.1\% = 1.25\mu\text{s}$, 占 1.2% 的位宽度, 达到了设计要求。

如果双方的时钟相差 1%, 则最大的累积错位为 12.5μs, 占 12% 的位宽度, 超出了设计要求。

3-13 什么是同步传输方式？

解答：同步传输方式中是以称为帧 (frame) 的大的数据块为单位进行传送。同步传输使用特殊的标志进行帧同步, 界定一个帧的始末。由于一个信息帧可以包含的位数很多, 同步传输还必须进行严格的位同步, 要求通信双方使用同一时钟信号进行发送与接收。

3-14 什么是频带传输和基带传输？它们各采用哪种多路复用方式？

解答：频带传输借助于模拟的正弦载波信号, 用数字数据调制载波, 将数字数据寄生在载波的某个参数上, 借助于模拟信道进行传输。使用频带传输方式传输数字数据需要利用调制解调技术对数据进行转换。频带传输可以利用频分多路复用 (FDM) 实现多路复用, 提高传输信道的利用率。

基带传输用于传输基带信号。基带 (Baseband) 即基本频带, 指未经调制 (频率变换) 的信号所占用的频带, 即把数字数据转换为数字传输信号时它所固有的频带。基带传输

中媒体的整个频带范围都用于传输基带信号。基带传输可以利用时分多路复用(TDM)实现多路复用,提高传输信道的利用率。

3-15 什么是调制和解调?其目的是什么?有几种调制方式?

解答:数字数据模拟化的方法称为调制(modulation),将数字数据寄生在正弦载波的某个参数上,把数字数据转换成连续的模拟信号。将已调制信号还原为原来的数字数据,称之为解调(demodulation)。

调制的目的是可以使用频带传输方式传输数字数据,以利用现有的电话传输系统。

正弦载波有 3 个参数可调,即幅值、频率和相位,因此基本的调制方法也相应的有幅度调制、频率调制和相位调制,也称为幅移键控(ASK)、频移键控(FSK)和相移键控(PSK)。如果经调制后载波有的多个幅度、频率和相位,分别为多级幅移键控(MASK)、多级频移键控(MFSK)或多级相移键控(MPSK)。也可由幅度和相位 2 个参数进行复合多级调制,称为幅相键控(APK),APK 也称正交幅度调制(QAM),有 16QAM 和 64QAM 等。

3-16 数字数据在使用基带传输方式传输前为什么还要编码?

解答:数字数据在使用基带传输方式传输前需要按一定方式编码,主要有三个方面的原因:

- 编码更有利于在接收端区分传输的“0”与“1”的值;
- 编码可以在传输信号中携带时钟,方便地实现传输信号的同步问题,不必额外再加专用的同步时钟信号线;
- 采用合理的编码方式,可以充分利用信道的传输能力,达到更高的信息传输速率。

3-17 对于数字数据 01100101,请画出它采用不归零制编码、曼彻斯特编码和差分曼彻斯特编码 3 种编码方式编码后的信号波形。

解答:数据 01100101 的 3 种编码的波形如图 1-3-1 所示。

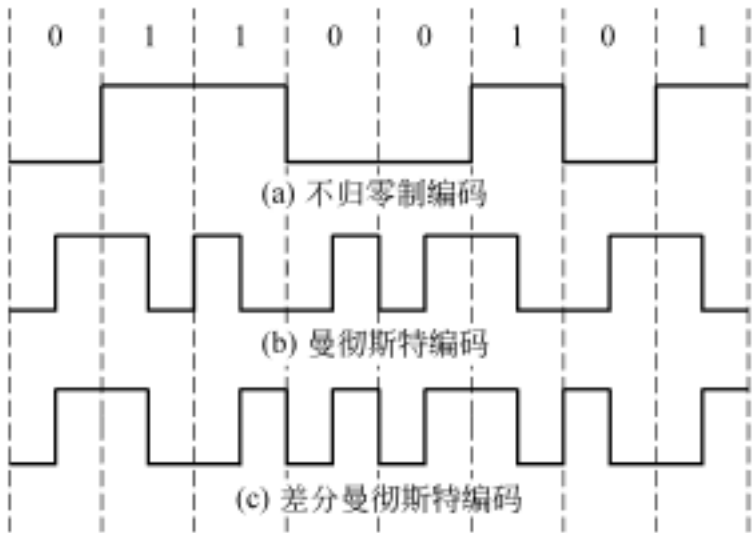


图 1-3-1 题 3-17 解答图

3-18 对于十六进制数字数据 0xDE5615,请画出一种八进制编码方式的编码后的信号波形。

解答:十六进制数字数据 0xDE5615 的二进制位串为: 11011110 01010110

00010101。八进制编码用 8 种电平 - 4 V、- 3V、- 2V、- 1V、1 V、2V、3V 和 4V 分别表示 000、001、010、011、100、101、110 和 111。0xDE5615 的一种八进制编码波形,如图1-3-2 所示。

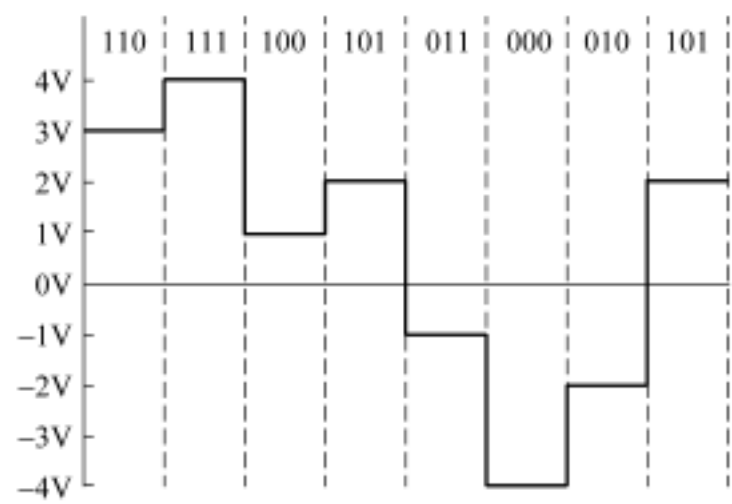


图 1-3-2 题 3-18 解答图

3-19 多路复用的目的是什么？说出常用的多路复用的方式。

解答：一个通信系统的建造和运行费用中传输线路一般要占一半以上,传输线路的多路复用就显得非常重要。尽量把多路通信复用到一条物理干线上,充分利用传输线路的带宽,可以大大节省线路的投资。

电话系统早期的复用方式是空分多路复用 SDM,由多条电线组成一根电缆,每条传送自己的一路信号。后来,采用频分多路复用 FDM 技术。现在,很多国家的电话主干线已经实现了数字化传输,因此时分多路复用 TDM 又成为主流,计算机网络主要使用时分多路复用技术。波分多路复用 WDM 是光信号的多路复用技术,充分挖掘了光纤的巨大带宽潜力。

3-20 什么是 PCM ?目的是什么？它分哪几个步骤？

解答：脉冲代码调制(PCM)是模拟数据数字化的方法,使模拟数据转换为数字数据,可以通过数字传输系统进行传输。PCM 在电话系统的数字传输中广泛使用。

PCM 的处理过程可以分为三个阶段:采样、量化和编码。取样即每隔一个固定的时间间隔对模拟信号进行一次取样,这样原来在时间上连续的信号就变成离散的脉冲。采样的脉冲信号还要进行量化,然后再把量化后的数值表示成二进制数,这个过程称为编码。

3-21 为什么电话的数字传输系统中很多时间间隔都为 125μs ？

解答：根据采样定理,每周期采样 2 次即可恢复原来的信号。电话的数字传输系统中,电话信道带宽为 4kHz,因此每秒采样 8 000 次,即 125μs / 次,就足够捕获和恢复 4kHz 电话信道带宽的信号。在电话 TDM 系统中(T1、E1、SDH、SONET 等)几乎所有的时间间隔都是以 125μs 为基数,以使得每路话音的采样频率都满足采样定理。

3-22 在 T1 和 E1 中,125μs 的时间间隔内如何进行 TDM 复用？T1、E1 和 STS-1 的信息传输速率是多少？写出推导过程。

解答: 在 T1 中, 24 路模拟话音信号以 $125\mu\text{s}$ 为周期被轮回采样, 在 1 个周期内每路被采样 1 次, 每个通道按顺序在输出流中插入 8 比特。7 比特为数据, 1 比特为信令信号, 用于控制。这样每个通道有 $7 \times 8000 = 56\text{kb/s}$ 的信息传输速率。T1 的一个帧分为 24 个时隙, 每个时隙 8 比特, 每帧有 $8 \times 24 = 192$ 比特, 再加上 1 比特用于分帧, 这就构成一个 193 比特的 T1 帧, 因此, T1 的传输速率为: $193 \text{ 比特} \div 125\mu\text{s} = 1.544\text{Mb/s}$ 。

E1 将 32 个 8 比特话音信号封装在 $125\mu\text{s}$ 的帧中, 30 个通道用于数据, 两个通道用于信令。因此, E1 的传输速率为: $8 \times 32 \text{ 比特} \div 125\mu\text{s} = 2.048\text{Mb/s}$ 。

SONET 的一级同步传输信号 STS-1 中包含 1 个 SONET 帧, 它是 $90 \text{ 列} \times 9 \text{ 行}$ 组成的块状帧, 包含 $90 \times 9 = 810$ 字节, 即 $8 \times 810 = 6480$ 比特, 每 $125\mu\text{s}$ 发送 1 帧, 因此, STS-1 的信息传输速率为: $6480 \text{ 比特} \div 125\mu\text{s} = 51.84\text{Mb/s}$ 。

3-23 T1 线路带宽中, 用户传输的话音数据所占比例有多大? 即 1.544Mb/s 中有多大比例在端用户间传输?

解答: $(7 \times 24) \div ((8 \times 24) + 1) = 87\%$ 。

3-24 什么是 WDM? 什么是 DWDM? 什么是 CWDM?

解答: 波分多路复用 WDM 在一根光纤上传输多路不同波长的光信号, 在发送端将多个光信号复合在一起, 送到一根光纤上传输, 在接收端由复合的信号分离出原来的光信号。因为波长是和频率对应的, 从概念上讲, WDM 和 FDM 是相同的, 但 FDM 是对电信号的复合和分离, 而 WDM 是对光信号的复合和分离, 所使用的设备是光处理设备。

同一个波段中通道间隔较小的波分多路复用称为密集波分多路复用(DWDM)。ITU-T 建议的光波之间的间隔是 0.8nm , 还可更小。目前的 DWDM 系统一般使用 $1.55\mu\text{m}$ 的波段。

通道间隔较大的波分多路复用称为稀疏波分多路复用(CWDM), 光波分布的更稀疏, ITU-T 建议的光波间隔是 20nm 。CWDM 以比 DWDM 系统宽得多的波长范围($1.26 \sim 1.62\mu\text{m}$) 进行波分复用, 降低了对波长的窗口要求, 使得 CWDM 系统的成本大大下降, CWDM 可用于距离较短的城域网中。

3-25 描述并比较 TDM 和 STDM。

解答: 时分多路复用(TDM)技术将传输分成固定长度的帧, 每个帧又划分为若干个时隙, 采用固定时隙分配方式, 即一个时隙的数据总是对应于一个固定的数据源, 在接收端根据信号在时隙中的位置就可以分离出各路用户的数据。

统计时分多路复用(STDM)不使用固定时隙分配方式, 可以动态地按需要分配时隙, 时隙位置与数据源没有固定的对应关系, 突发数据的用户可以利用其他 TDM 中的空闲时隙, 从而提高了时隙利用率, 但时隙中必须增加地址信息。

3-26 UTP 是什么意思? 目前主要分为几类? 它们的带宽是多少? 目前 100Mb/s 的以太网主要使用哪种 UTP 布线?

解答: UTP(unshielded twisted pair)指非屏蔽双绞线, 双绞线每一对绞合在一起, 一般在塑料外壳内有 4 对这样的线, 外壳起到保护的作用。TIA/EIA 568B 标准将非屏蔽双绞线分成类(category), 主要有以下几类: 3 类(category 3), 带宽是 16MHz ; 4 类, 带宽是 20MHz ; 5 类和增强型 5 类(Category 5E), 也称超 5 类, 双绞线绞合得更密, 在更长的

距离上信号质量更好;带宽是 100MHz;6 类,可以达到 250MHz 的带宽。

目前 100Mb/s 的以太网主要使用 5 类和增强型 5 类 UTP 布线。

3-27 光纤分为哪两种?它们传输光脉冲的方式有什么不同?

解答:依光在光纤中传播的方式不同,光纤分为多模光纤(multimode fiber)和单模光纤(single mode fiber)两种。

光纤传输光脉冲的方式如下:光从光源进入光纤,如果它的方向与光纤的轴向不完全一致,它就会射向光纤边缘,由于包层的光学性质与光纤不同,光在光纤与包层的边界会产生折射或反射。入射角小于某临界值的光会折射到包层中去,被周围材料吸收。当入射角大于某临界值时,会出现全反射,光会反射回光纤,这个过程不断重复,光就沿着光纤传播下去。

当有多条不同入射角的光线以不同的反射角在一条光纤中传输,这种传输方式的光纤称为多模光纤。当光纤的直径减小到光波长的数量级,光纤几乎没有空间供光线进行来回反射,光都会沿轴向传输,这种传输方式的光纤称为单模光纤。

单模光纤具有更优良的性能,具有更高的带宽和更长的传输距离,但价格也高。

3-28 光传输系统包括哪几个部分?和铜线相比,光纤传输有什么优点?

解答:光传输系统主要包括光源、光纤和光敏元件接收装置 3 个部分。可以作为光源的有发光二极管(LED)和激光二极管(ILD)。接收端使用光敏元件来检测光脉冲,比如光电二极管(photodiode),当光照到它时会产生电流。在一根光纤的两端各安装一个发光二极管和一个光电二极管,就构成一个单工的传输系统。光传输系统一般需要两根光纤,构成全双工的数据传输系统。

光纤和铜线比较有很多优点。光纤可以提供比铜线高得多的带宽,因此它可以应用于高速的网络。光纤传输比铜线传输衰减小,长距离传输可以使用较少的中继器。光纤传输不受电磁干扰,因而减少了误码率。光纤难于拼接,但因此光纤传输也难于被窃听,安全性高。

3-29 什么是光速?光速等于多少?写出光速、频率和波长的关系。

解答:电磁波每秒振动的次数称为频率(frequency) f ,单位为赫兹(Hz)。两个相邻的波峰间的距离称为波长(wavelength),记为 λ 。

光速是电磁波在真空中的传播的速度,与它的频率无关,大约为 $300\,000\text{km/s}$,即 $300\text{m}/\mu\text{s}$ 。在真空中光速 c 和频率 f 、波长 λ 有下述关系: $f = c/\lambda$,波长 λ 的单位为 m。

3-30 铜线和光纤中电磁波的传播速度是多少?电磁波在铜线中传播 1km 需多少时间?

解答:在铜线或光纤中,电磁波的速度大约降低到光速的 $2/3$,为 $200\,000\text{km/s}$ ($200\text{m}/\mu\text{s}$)。电磁波在铜线中传播 1km 需 $5\mu\text{s}$ 。

3-31 一条 20km 的电缆传输 E1 速率的数据,电信号从该电缆的一端传播到另一端需多少时间?该电缆中可以容纳多少个比特?

解答:在铜线电磁波的速度是 $1\text{km}/5\mu\text{s}$,电信号从一条 20km 的电缆的一端传播到另一端需 $100\mu\text{s}$ 。E1 的信息传输速率是 2.048Mb/s ,该电缆中可以容纳的比特数是 $2.048\text{Mb/s} \times 100\mu\text{s} = 204.8$ 个,此即该电缆的比特长度。

3-32 什么是微波？什么是微波通信和卫星通信？

解答：微波(mircowave)是频率较高的电磁波，频率范围在 300MHz ~ 300GHz，但主要使用 2 ~ 40GHz。

微波沿着直线传播，微波通信通过抛物状天线把所有的能量集中于一小束发射出去，发射天线和接收天线必须精确地对准。地面微波通信是在地球表面建造微波塔进行中继的无线通信。卫星通信是在地球站之间利用人造同步卫星作为中继的一种微波通信，卫星就相当于在太空中的无人值守的微波通信中继站。

3-33 若电磁波的波长为 1.3μm，它对应的频率是多少？以 1.3μm 为中心的 0.17μm宽的波段相应的频段的带宽有多少赫兹？它允许的最高码元传输速率是多少？在无噪声的情况下，如果采用 4B/ 5B 编码，信息传输速率可以达到多少？

解答：由光速 c 和频率 f 、波长 λ 的关系 $f = \frac{c}{\lambda}$ ，有： $\frac{df}{d\lambda} = -\frac{c}{\lambda^2}$ ，那么，波段的带宽 Δf 近似为： $\Delta f = \frac{c}{\lambda^2} \times \Delta \lambda$ (Hz)，对于以 1.3μm 为中心的 0.17μm 宽的波段有：

$$\Delta f = \frac{3 \times 10^8 \text{m/s}}{(1.3 \mu\text{m})^2} \times 0.17 \mu\text{m} = 20 \text{THz}。$$

根据奈奎斯特准则，在一个无噪声带宽有 20THz 的波段上，最高的码元传输速率可达 40Tbaud，如果采用 4B/ 5B 编码，信息传输速率可以达到 32Tb/ s。

3-34 数据通信系统一般包括信源、发送装置、__(1)__、接收装置和信宿。当采用卫星进行通信时，数据一般被变换成__(2)__。为了增大模拟传输系统的传输距离，应采用的设备是__(3)__。现在在模拟电话网上利用调制解调器传输数据往往采用幅度和相位两个参数进行调制，这种调制方式称为__(4)__。

- (1) A . 信号放大器 B . 编码译码器 C . 传输系统 D . 交换系统
- (2) A . 数字信号 B . 模拟信号
- C . 数字信号或模拟信号 D . 数字信号和模拟信号
- (3) A . 网桥 B . 放大器 C . 路由器 D . 交换机
- (4) A . ASK B . FSK
- C . PSK D . QAM(正交幅度调制)

答案：C, B, B, D

3-35 图 1-3-3 为曼彻斯特编码表示的数据为__(1)__, 使用这种编码的网络是__(2)__. 如果该编码波形的最高和最低电平分别为正负 5V, 其直流分量是__(3)__ V。



图 1-3-3 曼彻斯特编码

- (1) A . 10100 B . 01110 C . 10101 D . 00011
- (2) A . 广域网 B . 城域网 C . 以太网 D . 任意局域网
- (3) A . 5 B . - 5 C . 2.5 D . 0

答案：A, C, D

3-36 在一个带宽为 3kHz、没有噪声的信道,传输二进制信号时能够达到的最高码元传输率为__ (1) __ baud。一个带宽为 3kHz、信噪比为 30dB 的信道,能够达到的极限信息传输率为__ (2) __ b/s。上述结果表明,__ (3) __。

- (1) A . 3k B . 6k C . 56k D . 10M
- (2) A . 12k B . 31k C . 56k D . 10M
- (3) A . 有噪声信道比无噪声信道具有更大的带宽
- B . 有噪声信道比无噪声信道可达到更高的极限数据传输率
- C . 有噪声信道与无噪声信道没有可比性
- D . 上述问题数据的单位不同,数据不能进行直接比较

答案: B, B, D

3-37 设信道的码元速率为 300 波特,采用 4 相 PSK 调制则信道的数据速率为__ b/s .

- A . 300 B . 600 C . 800 D . 1 000

答案: B

3-38 4B/ 5B 编码是将数字数据转换为数字信号的编码方式,其原理是__ (1) __ 位编码表示__ (2) __ 位数据。该编码是__ (3) __ 采用的编码方法,编码效率是__ (4) __,相对于曼彻斯特编码,效率高了__ (5) __。

- (1) A . 4 B . 5 C . 8 D . 10
- (2) A . 4 B . 5 C . 8 D . 10
- (3) A . 10Mb/s 以太网 B . 100BaseT4 以太网
- C . 1000Mb/s 以太网 D . FDDI
- (4) A . 50% B . 60% C . 75% D . 80%
- (5) A . 30% B . 50% C . 60% D . 80%

答案: B, A, D, D, C

3-39 TDM 可分为同步 TDM 和异步 TDM。若采用同步 TDM 多路复用技术,为了区分不同数据源的数据,发送端应采取的措施是__ (1) __,接收端则按照__ (2) __ 来接收数据,就可以将多路信号复原。在异步 TDM 中,只有当数据源有数据要发送时才分配时隙,并在时隙中__ (3) __,以便接收端准确地分发数据。同步 TDM 和异步 TDM 分别是__ (4) __。

- (1) A . 在数据中加上数据源标识 B . 在数据中加上时间标识
- C . 各数据源使用固定时隙 D . 各数据源使用随机时隙
- (2) A . 时间片上的目标地址 B . 数据上的时间标识
- C . 数据上的数据源标识 D . 与源端相同的时间顺序
- (3) A . 附加填充字段 B . 附加校验信息
- C . 附加地址字段 D . 无需附加信息
- (4) A . 固定帧长和可变帧长 B . 固定帧长和固定帧长
- C . 可变帧长和可变帧长 D . 可变帧长和固定帧长

答案: C, D, C, A

3-40 对一路信号进行 FSK 调制时,若载波频率为 f_c ,调制后的信号频率分别为 f_1 和 f_2 ($f_1 < f_2$),则三者的关系是__ (1) __。信号到达接收端后通过__ (2) __分离各路信号。波分多路复用(WDM)与频分多路复用(FDM)工作方式相似,但 WDM 调制的是__ (3) __。

(1) A . $f_c - f_1 = f_2 - f_c$ B . $f_2 - f_1 = f_c$ C . $f_2 + f_1 = f_c$ D . $f_1 \times f_2 = f_c$

(2) A . 解调器 B . 带通滤波器 C . 载波发生器 D . 终端软件

(3) A . 时间 B . 频率 C . 波长 D . 相位

答案: A, B, C

第 4 章

数据链路控制

4-1 什么是数据链路？理想的数据链路基于哪两个假设？如果它们不满足，需分别进行什么控制？

解答：在数据链路层，通信的对等实体之间的数据传输通道称为数据链路（data link），它是一个逻辑概念，包括物理链路和必要的传输控制规程。

- 一个完全理想化的数据链路，可以实现理想的可靠的数据传输，它基于以下两个假设：
- （1）不管发方以多快的速率发送数据，收方总能够来得及接收、处理并上交主机。也就是收方有足够的接收缓冲区和处理速度；
 - （2）链路是理想的传输信道，传输的任何数据既不会出现差错也不会丢失。

假设（1）不满足就必须进行流量控制，流量控制用来保证发送数据在任何情况下都不会“淹没”收方的接收缓冲区，即不会使收方的接收缓冲区溢出而丢失数据；假设（2）不满足，就必须进行差错控制，在有线路干扰和传输差错的情况下，实现可靠的数据传输。

4-2 试画出正常传输和帧丢失情况下停等 ARQ 工作过程的示意图。

解答：停等 ARQ 机制的基本思想是在发送方发出一个数据帧后停下来不再发送，等待接收方的 ACK 到达，ACK 到达后才发出下一帧。

图 1-4-1 是停等 ARQ 工作过程的示意图。图中包括了正常发送和确认、发送的数据

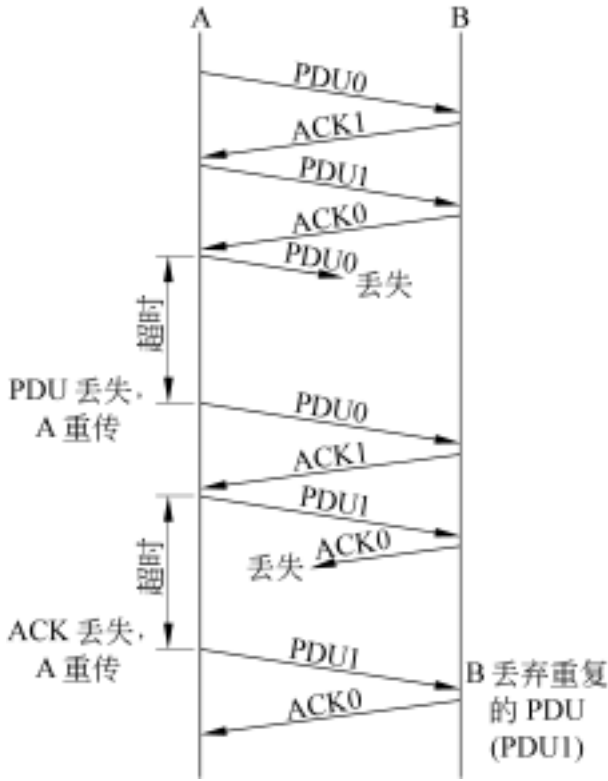


图 1-4-1 停等 ARQ 工作过程的示意图

帧丢失和确认帧丢失等不同的情况。图中的水平方向表示了发送站 A 和接收站 B 之间的距离,垂直方向为时间,向下是时间增长方向。

4-3 停等 ARQ 无差错的传输情况下,如果链路传输速率为 1Mb/s , 帧长 $1\,000$ 字节,传播延时 $= 1\text{ms}$, 那么,链路的利用率可达到多少?(忽略确认帧的发送时间)。如果是传播延时 $= 270\text{ms}$ 的卫星链路呢?

$$\begin{aligned}\text{解答: 链路的利用率} &= \text{帧的比特长度} / (\text{帧的比特长度} + 2 \times \text{链路的比特长度}) \\ &= 8 \times 1\,000\text{b} / (8 \times 1\,000\text{b} + 2 \times 1\text{Mb/s} \times 1\text{ms}) \\ &= 80\%\end{aligned}$$

卫星链路情况:

$$\begin{aligned}\text{链路的利用率} &= \text{帧的比特长度} / (\text{帧的比特长度} + 2 \times \text{链路的比特长度}) \\ &= 8 \times 1\,000\text{b} / (8 \times 1\,000\text{b} + 2 \times 1\text{Mb/s} \times 270\text{ms}) \\ &= 1.46\%\end{aligned}$$

4-4 描述滑动窗口控制机制及其作用。

解答: 滑动窗口是数据链路控制的一个重要机制,滑动窗口机制在发送方和接收方分别设置发送窗口和接收窗口,在数据传输过程中受控地向前滑动,控制数据传输的过程。

发送窗口用来对发方进行流量控制,其大小指明在收到对方 ACK 之前发送方最多可以发送多少个数据帧,只有序号在窗口覆盖范围内的数据帧是可以连续发送的。

接收窗口控制哪些数据帧可以接收,只有到达的数据帧的序号落在接收窗口之内时才可以被接收,否则将被丢弃。一般,当收方收到一个有序且无差错的帧后,接收窗口向前滑动,准备接收下一帧,并向发送方发出一个确认。为了提高效率,收方可以采用累计确认或捎带确认。

当发方收到收方的确认后,发送窗口才能向前滑动,滑动的长度取决于收方确认的序号。向前滑动后,又有新的帧落入发送窗口,可以被发送。滑动后被确认正确收到的帧落在窗口的后边。

可见,收方的确认作为授权发方发送数据的凭证,收方通过确认控制发方发送窗口向前滑动。收方可以根据自己的接收能力来控制确认帧的发送,从而实现对传输流量的控制。另外,由于滑动窗口中使用了确认机制,因此它也兼有差错控制的功能。

4-5 回退-N ARQ 对停等 ARQ 的主要改进是什么?其中“回退-N”的含义是什么?

解答: 回退-N ARQ 是对停等 ARQ 的改进主要是可以使用大的发送窗口,停等 ARQ 的发送窗口 $W_T = 1$,限制了传输流量,而回退-N ARQ 的 W_T 可以大于 1,发方可以连续地发送窗口内多个帧,最大传输流量由回退-N ARQ 的每往返时间 1 个数据帧的水平,提高到 W_T 个数据帧的水平,提高了传输效率。

回退-N ARQ 中,若因发送帧丢失、出现校验差错或确认丢失使重传定时器超时而发方仍未收到收方的 ACK,发方则要重发此帧,而且还必须重发此帧后面所有的已发帧(不管这些帧是否有传输差错),也就是说,指向发送数据的指针必须回退若干个帧,这就是“回退-N”的含义。

4-6 回退-N ARQ 的接收窗口 W_R 是多大?为什么?

解答：回退-N ARQ 的接收窗口 $W_R = 1$ ，因为回退-N ARQ 机制规定，收方不保存失序(out-of-order)的帧，前面的帧丢失时，发方还要重发这些失序的帧。

4-7 回退-N ARQ 的发送窗口 W_T 有什么限制？如果帧的序号用 3 比特编号，发送窗口最大序号为多少？假设 $W_T = 8$ ，对于回退-N ARQ，假定收方对每一个正确收到的帧都发回一个 ACK。试举例分析：当对数据帧的 ACK 丢失时会产生什么问题。

解答：回退-N ARQ 对发送窗口的大小是有限制的，如果帧的序号用 n 比特编号，则发送窗口 W_T 应满足： $W_T \leq 2^n - 1 = \text{最大序号}$ 。若 $n = 3$ ，最大序号为 7，要求 $W_T \leq 7$ 。

本题中， $n = 3$ ， $W_T = 8$ ，对于回退-N ARQ， $W_R = 1$ ，收方对每一个正确收到的帧都发回一个 ACK。开始，假设发方发送窗口是 $[0, 1, 2, 3, 4, 5, 6, 7]$ ，共 8 个帧，收方接收窗口是 $[0]$ ，准备接收 0 号帧，开始的发送窗口和接收窗口如图 1-4-2 中灰色格所示。

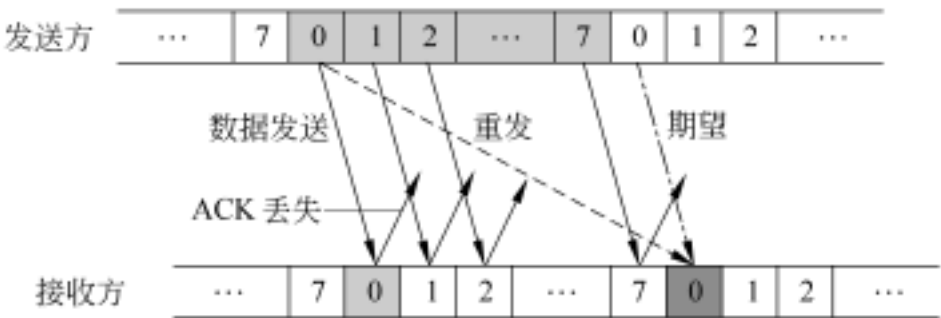


图 1-4-2 $W_T = 2^n$ 时接收中的不确定性

现在，假定发方发送了窗口内的这 8 个帧，并依次正确地到达收方，收方将的接收窗口也依次向前滑动并发回 ACK1 ~ ACK7 和 ACK0。接收窗口共向前滑动 8 个序号，正好一个序号轮回，现在接收窗口又是 $[0]$ (图 1-4-2 中深色格)，但意思是期望接收新的 0 号帧(图 1-4-2 中点划线)。

如果下面的传输一切正常，接收方就开始接收新的 0, 1, ... 号帧。但是出现了差错：假设收方的确认 ACK 全丢失了。0 号帧重发定时器到时，发方将回退重发原 0 号帧(图 1-4-2 中虚线)及其后面的原 1 ~ 7 号帧。重发的 0 号帧的序号也符合滑动后的接收窗口，因此收方接收重发的原 0 号帧并将接收窗口向前滑动，继续接收后面的帧。这样，收方就把重发的原 0 ~ 7 号帧错误地当成新的一组帧而接收，它们在接收缓冲区重复出现。

不难看出，造成上述问题的原因是接收窗口中新的 0 号与发送窗口内原 0 号为完全一样的序号，但它们相差一个轮回(2^n)，发方发来的 0 号帧可能是新的(正常情况)，也可能是原来的(重发原 0 号帧)，收方无法判断这种不确定性，一概接收。

如果 $W_T \leq 2^n - 1$ ($W_T \leq 7$) 时，比如 $W_T = 7$ ，发送窗口将是 $[0, 1, 2, 3, 4, 5, 6]$ ，滑动后的接收窗口将是 $[7]$ ，发送窗口内就不会有和 7 相差一个轮回的同样序号，也就不会出现上述的不确定性问题。

4-8 选择重传 ARQ 的发送窗口 W_T 有什么限制？如果帧的序号用 3 比特编号，选 $W_T = W_R = 5$ ，并假定收方对每一个正确收到的帧都发回一个 ACK。试举例分析试：当对某一序号的数据帧的 ACK 丢失时会产生什么问题。

解答：选择重传 ARQ 对发送窗口的大小是有限制的，如果帧的序号用 n 比特编号，则发送窗口 W_T 应满足： $W_T \leq 2^{n-1}$ 。

本题中, $n = 3$, $W_T = W_R = 5 = 2^n / 2$, 收方对每一个正确收到的帧都发回一个 ACK。开始, 假设发方发送窗口和收方接收窗口都是 $[0, 1, 2, 3, 4]$, 共 5 个帧, 如图 1-4-3 中灰色格所示。

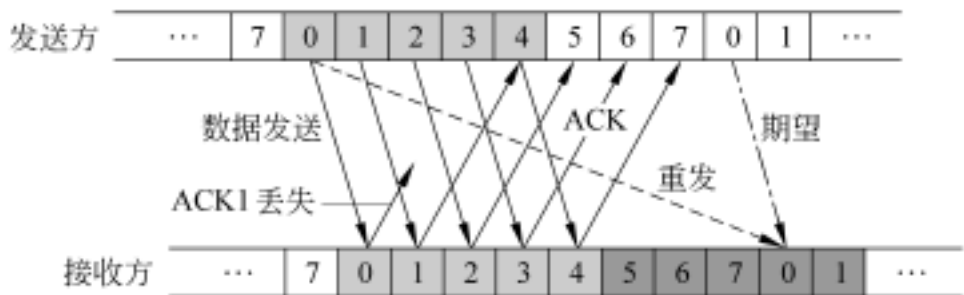


图 1-4-3 $W_T = 5$ 时接收中的不确定性

现在, 假设发方发送了窗口内的这 5 个帧, 并依次正确地到达收方, 收方将接收窗口也依次向前滑动并发回 ACK1 ~ ACK5。接收窗口共向前滑动 5 个序号, 现在接收窗口是 $[5, 6, 7, 0, 1]$ (图 1-4-3 中深色格)。

如果下面的传输一切正常, 接收方就开始接收新的 5, 6, ... 号帧。但是出现了差错: 假设收方对 0 号帧的确认 ACK1 丢失了。0 号帧重发定时器到时, 发方将回退重发原 0 号帧 (图 1-4-3 中虚线)。重发的 0 号帧的序号也在滑动后的接收窗口内, 因此收方接收重发的原 0 号帧, 它在接收缓冲区重复出现。由图 1-4-3 不难看出, 当 ACK2 丢失, 也会重复接收 1 号帧。

不难看出, 造成上述问题的原因是接收窗口中新的 0 号与发送窗口内原 0 号为完全一样的序号, 但它们相差一个轮回 (2^n), 发方发来的 0 号帧可能是新的 (正常情况), 也可能是原来的 (重发原 0 号帧), 收方无法判断这种不确定性, 一概接收。

如果 $W_T = W_R = 2^n / 2$ ($W_T = W_R = 4$) 时, 比如 $W_T = 4$, 发送窗口将是 $[0, 1, 2, 3]$, 滑动后的接收窗口将是 $[4, 5, 6, 7]$, 发送窗口内就不会有和接收窗口相差一个轮回的同样序号, 也就不会出现上述的不确定性问题。

从数学上讲, 发送窗口和接收窗口滑动时序号都是按模 2^n 增长, 因此会按模 2^n 重复, 当窗口大到一定程度时, 就会出现上述发送窗口有和接收窗口相同的序号的现象, 造成接收的不确定性。当 $W_T + W_R \text{ 模} = 2^n$ 时, 就不会出现上述现象。对于回退-N ARQ, $W_R = 1$, 因此有 $W_T = 2^n - 1$; 对于选择重传 ARQ, $W_T = W_R$, 因此有 $W_T = 2^n / 2$ 。

4-9 如果卫星通信地面站距离卫星 36 000km, 那么:

(1) 数据经卫星转发即由地面站—卫星—地面站的传播延时是多少? (忽略卫星转发的处理时间)。

(2) 若使用停等 ARQ 以 56kb/s 速率发送 1 250 字节长度的数据帧, 信道可能达到的最大信息传输速率是多少?

(3) 将(2)改为使用滑动窗口的回退-N ARQ 协议, 发送窗口大小为 7, 单工信道可能达到的最大信息传输速率是多少?

解答: (1) 数据经卫星转发即由地面站—卫星—地面站的传播延时 为:

$$= (2 \times 36\,000\text{km}) \div 300\,000\text{km/s} = 240\text{ms}。$$

(2) 以 56kb/s 速率发送 1 个 1 250 字节长度的数据帧, 所需的发送时间 T_{DATA} 是:

$$T_{DATA} = (8\text{b/字节} \times 1\,250\text{字节}) \div 56\text{kb/s} = 179\text{ms}$$

停等 ARQ 一个数据帧的往返传输时间:

$$2 + T_{DATA} = 659\text{ms} = 0.659\text{s}$$

信道的最大信息传输速率可达:

$$(8\text{b/字节} \times 1\,250\text{字节}) \div 0.659\text{s} = 15.2\text{kb/s}$$

(3) 以 56kb/s 速率连续发送 7 个 1 250 字节长度的数据帧,所需的发送时间 T_{DATA} 是:

$$T_{DATA} = 7 \times 179\text{ms} = 1\,253\text{ms}$$

单工信道回退-N ARQ 方式 7 个数据帧的往返传输时间:

$$2 + T_{DATA} = 1.733\text{s}$$

最大信息传输速率可达:

$$7 \times (8\text{b/字节} \times 1\,250\text{字节}) \div 1.733\text{s} = 40.4\text{kb/s}$$

可见,回退-N ARQ 方式比停等 ARQ 提高了可能达到的最大信息传输速率。

4-10 选择重传 ARQ 对回退-N ARQ 机制作了什么改进?选择重传 ARQ 的接收窗口的大小与回退-N ARQ 有什么不同?选择重传 ARQ 的滑动窗口有什么限制?

解答:选择重传 ARQ 也是一种连续 ARQ,在回退-N ARQ 机制的基础上作了如下两点改进:

接收窗口 $W_R > 1$,这样可以接收和保存正确到达的失序的帧;

出现传输差错时只重传出错的帧,后续的正确到达的帧不再重传,这样就提高了信道的利用率。

选择重传 ARQ 中,接收窗口 $W_R > 1$,一般使 $W_T = W_R$ 。当使用 n 个比特对帧编号时,应该满足: $W_T = W_R = 2^n / 2 = 2^{n-1}$ 。

4-11 什么是奇校验/偶校验?奇偶校验能校验出哪种类型的传输错误?假设发送字符的位串(8 位)是 11010101,现进行的是偶校验,加入的校验位是什么?如果奇校验呢?

解答:奇校验/偶校验是在发送数据后附加一个校验位,校验位的取值使得包括数据和校验位中的“1”的个数分别为奇数/偶数。奇偶校验简单,易于实现。

奇偶校验只能检测出奇数个错而不能检测出偶数个错。

如果发送字符的位串(8 位)是 11010101,进行的是偶校验,加入的校验位应该是“1”,使数据和校验位中“1”的个数是 6,为偶数。如果进行的是奇校验,则加入的校验位应该是“0”,使数据和校验位中“1”的个数是 0,为奇数。

4-12 CRC 如何由信息码生成冗余码?

解答:由信息码 $K(x)$ 产生冗余码 $R(x)$ 的过程,是用码多项式的算术运算来实现。方法是:通过用一个特定的 r 次生成多项式 $G(x)$ 去除 $x^r K(x)$,即 $x^r K(x) / G(x)$,得到的 r 位余数作为冗余码 $R(x)$ 。 $G(x)$ 是事先约定的,除法中使用模 2 减(无借位减,相当于作异或 XOR 运算)。要进行多项式除法,只要用其相应的系数进行除法运算就可以。

4-13 给定一个信息位串 $K(x) = 10111010$ 和生成多项式 $G(x) = 11101$,问:冗余码应该是几位的?请计算出冗余码 $R(x)$,并验证: $C(x)$ 整除 $G(x)$ 。

解答:生成多项式 $G(x)$ 是 4 次的,冗余码应该是 4 位的。

$x^4 K(x) = 101100100000$, 用长除法:

$$\begin{array}{r} \overline{11110001} \\ 11101 \overline{) 101110100000} \\ \underline{11101} \\ 10100 \\ \underline{11101} \\ 10011 \\ \underline{11101} \\ 11100 \\ \underline{11101} \\ 10000 \\ \underline{11101} \\ 1101 \end{array}$$

得冗余码 $R(x) = 1101$ 。

$C(x) = x^4 K(x) + R(x) = 101110101101$, 用长除法求 $C(x)/G(x)$:

$$\begin{array}{r} \overline{11110001} \\ 11101 \overline{) 101110101101} \\ \underline{11101} \\ 10100 \\ \underline{11101} \\ 10011 \\ \underline{11101} \\ 11100 \\ \underline{11101} \\ 11101 \\ \underline{11101} \\ 0 \end{array}$$

可见, 余数为 0, $C(x)$ 整除 $G(x)$ 。

4-14 HDLC 定义了几种类型的站点、几种链路配置和几种工作模式?

解答: HDLC 定义了三种类型的站点, 两种链路配置和三种工作模式:

三种类型的站点:

主站(primary station)、从站(secondary station)和复合站(combined station)。

两种链路配置:

非平衡配置 用于点对点链路和多点链路。链路上的站点分为主站和从站, 由主站控制链路的工作过程, 主站发出命令帧, 从站发送响应帧。在多点链路中, 主站和每一个从站都有一个分开的逻辑链路。

平衡配置 用于点对点链路。链路两端的站点平等, 同时具有主站和从站的功能, 称为复合站, 每个复合站都可发出命令和响应。

三种工作模式:

正常响应模式 NRM 用于非平衡配置, 由主站发起数据传输, 只有主站向它发送命令帧进行轮询时, 从站才能以响应帧的形式回答。

异步响应模式 ARM 用于非平衡配置, 允许从站发起向主站的数据传输, 从站不需要等待主站的命令帧, 可以主动发送响应帧。主站仍负责链路的管理。

异步平衡模式 ABM 用于平衡配置, 每个复合站都可以平等地发起数据传输。

4-15 HDLC 定义了几种类型的帧? 简述帧格式和它们的功能。

解答: HDLC 有三种类型的帧: 信息帧 I、监督帧 S 和无编号帧 U。它们的帧结构如图 1-4-4 所示, 分为 6 个字段:

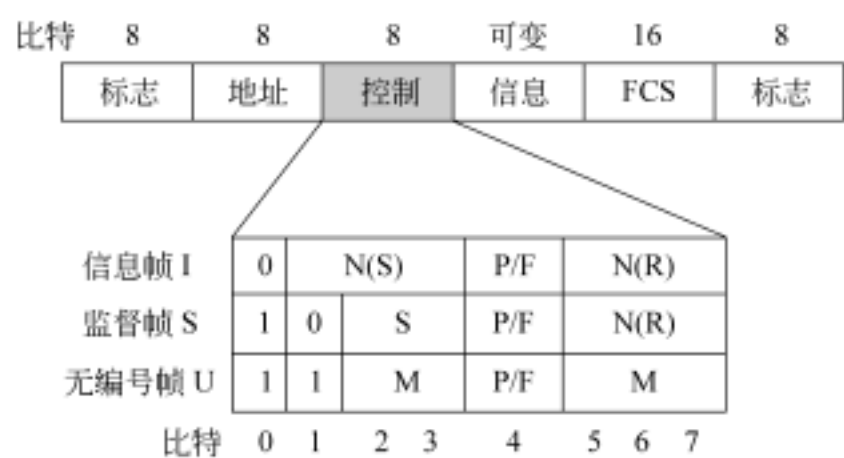


图 1-4-4 HDLC 的帧结构

标志 在一帧信息的开始及末尾附加有标志符 7E, 标记一个帧的开始及结束, 作为同步标志进行帧同步。为了防止在信息段中出现与标志符相同的位串 7E 而导致错误的处理, 使用比特填充法实现信息的透明传输。

地址 非平衡配置时总是写入从站地址, 平衡配置总是写入应答站地址。当地址全为“1”时表示广播地址, 全为“0”时无效。

控制 是非常重要和复杂的字段, 定义不同类型的帧, 进行链路的建立与拆除、信息的传输以及流量和差错控制等。

信息 信息字段携带用户数据。

帧校验序列 FCS 采用循环冗余校验 CRC 进行差错校验。

三种类型帧的主要功能如下:

信息帧: 用于传输数据。发送序号 N(S) 表示当前发送的信息帧的序号, 接收序号 N(R) 表示所期望接收的帧的序号。N(R) 带有确认的意思, 它表示序号为 N(R) - 1 的帧以及其以前的帧都已正确地接收到了。信息帧中也设置了接收序号 N(R), 可用于捎带确认。

监督帧: 不能传送数据, 用于传输过程的控制。监督帧共有 4 种, 用 S 比特即控制字段的第 2 ~ 3 比特来标识, 其功能如表 1-4-1 所示。这 4 种类型的监督帧, 前 3 种可用在后退 N-ARQ 协议, 第 4 种用于选择重传 ARQ。

表 1-4-1 监督帧的 4 种类型

S: 2 ~ 3 比特	监督帧名称	功 能 描 述
00	RR(Receive Ready) 接收准备就绪	准备接收下一帧, 确认序号为 N(R) - 1 及其以前的帧。
10	RNR(Receive Not Ready) 接收未就绪	暂停接收下一帧, 确认序号为 N(R) - 1 及其以前的帧。
01	REJ(REJect) 拒绝	否认 N(R) 及其以后的帧, 但确认序号为 N(R) - 1 及其以前的帧。
11	SREJ(Selective REJect) 选择性拒绝	只否认序号为 N(R) 的帧, 但确认序号为 N(R) - 1 及其以前的帧。

在 RR 和 RNR 两种监督帧相当于正确确认机制, REJ SREJ 相当于负确认机制。RR 帧和 RNR 帧具有流量控制的作用。RR 帧表示已做好接收帧的准备,对方可以继续发送,而 RNR 帧则指示对方暂停发送。

无编号帧:不带编号,其控制字段无 N(S)和 N(R)。无编号帧用于数据链路的模式设置、链路的建立与释放等链路管理功能。

4-16 结合图 1-4-5 描述 HDLC 在正常响应工作模式 NRM 下的数据传输过程。

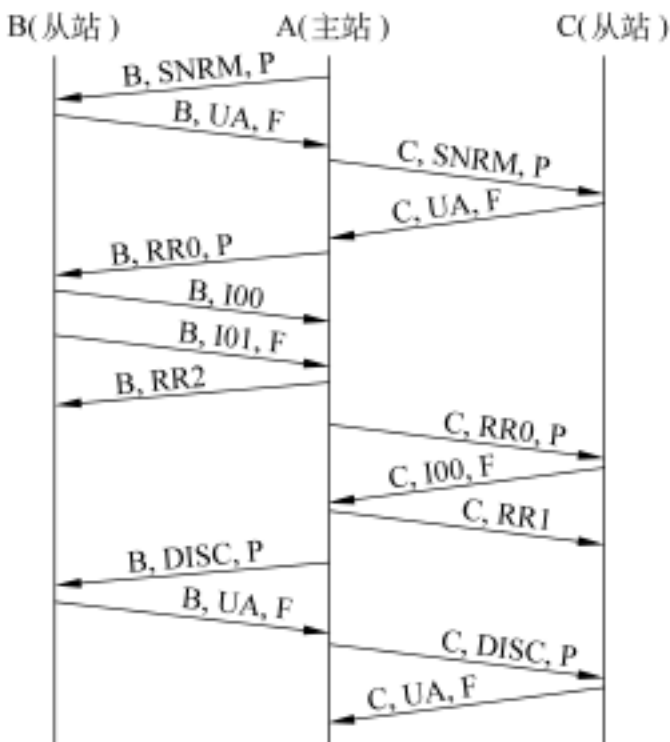


图 1-4-5 NRM 下 HDLC 数据传输过程

解答: 该图描述了 NRM 下 HDLC 数据传输过程。HDLC 一个非平衡配置的多点链路,配置为正常响应工作模式 NRM,共有 A、B 和 C 三个站,其中 A 是主站,B 和 C 是从站。数据传输过程分为三个阶段:(1)数据链路建立,(2)数据传输,(3)数据链路释放。

首先,主站 A 与从站 B 和 C 建立连接,设置为 NRM。主站 A 向从站 B 发送置正常响应模式 SNRM 无编号帧以设置为正常响应工作模式并建立连接(B, SNRM, P),B 以无编号确认帧 UA 响应(B, UA, F),同意建立连接。主站 A 与从站 C 建立连接的过程类似。

连接建立之后,就可以进行数据传输了。主站 A 使用接收准备就绪 RR 监督帧轮询从站 B(B, RR0, P),其中“0”表示 $N(R) = 0$,即期望收到对方的 0 号帧。从站 B 响应两个信息帧(B, I00)和(B, I01, F),其中“00”表示 $N(R)$ 、 $N(S)$,最后一帧以 $F = 1$ 终止。主站 A 发回确认(B, RR2)然后主站 A 轮询从站 C,过程类似。

数据传输完毕,主站发送无编号帧断开连接命令 DISC 释放连接(B, DISC, P),从站以无编号确认 UA 响应(B, UA, F)。从站 C 的连接释放过程类似。

4-17 PPP 是一种什么样的协议?它主要包含哪几个部分?

解答: 点对点协议(PPP)是 Internet 广泛使用的链路层通信协议,它为点对点链路上直接相连的两个结点之间提供了一种数据传输的方式。

PPP 主要包括三个部分:

- (1) 将 IP 数据报封装到串行链路的规程。PPP 既支持面向字符的异步链路(无奇偶检验的 8 比特字符), 也支持面向比特的同步链路。
- (2) 建立、配置和测试数据链路连接的链路控制协议(LCP)。通信的双方可通过 LCP 协商一些选项。
- (3) 网络控制协议(NCP)。它包含多个协议, 其中的每一个协议支持不同的网络层协议, 如 IP、OSI 网络层和 Netware 的网络层 IPX 等。

4-18 PPP 如何保证传输数据的透明性? 十六进制字符串数据:5E 7E 5D 7D 在使用 PPP 的异步链路中以什么形式传输?

解答: 为了保证 PPP 的帧界标记 0x7E 对传输数据的透明性, PPP 既支持零比特插入也支持字符插入。这是因为 PPP 既用于路由器到路由器的面向比特的同步链路, 也用于主机通过 RS-232、调制解调器和电话线到路由器的面向字符的异步链路。

当 PPP 用于同步链路时, 使用硬件进行零比特插入。当 PPP 在 RS-232 上进行异步传输操作时, 则采用字符插入, PPP 帧由整数字节组成。PPP 在发送首尾两个帧界标志之间的部分时, 将字符 0x7E 编码为 0x7D 和 0x5E, 将字符 0x7D 编码为 0x7D 和 0x5D。PPP 接收帧时, 删除 0x7D, 并将其后面的字符与 0x20 进行异或, 还原成原来的字符。

十六进制字符串数据:5E 7E 7D 5D 在使用 PPP 的异步链路中以下列形式(十六进制)传输:5E 7D 5E 7D 5D 5D。

4-19 画出并说明 PPP 的帧格式。

解答: PPP 的帧格式与 HDLC 帧近似, 如图 1-4-6 所示。



图 1-4-6 PPP 的帧格式

- 帧界标志 F 为 0x7E, 与 HDLC 相同。
- 地址 A 为 0xFF, 对应广播地址。PPP 只用于点到点链路, 实际上不需要数据链路层地址。
- 控制 C 为 0x03, 对应 HDLC 的无编号帧, PPP 不使用 HDLC 那种序号和确认机制, 没有差错控制和流量控制, 不能实现无差错传输(可进行 CRC 差错校验)。
- 地址和控制字段是固定值, 没有实质意义, 今后可以进行扩展。
- 协议 协议字段是 HDLC 中没有的, 说明数据字段封装的是哪类协议的分组。高位为 0 的协议号说明是某网络层的分组, 如 IP 的分组或 IPX 的分组等, 每种网络层协议对应一个协议号, 如 IP 的协议号是 0x0021。高位为 1 的协议号说明是 LCP 的分组或 NCP 的分组。
- 数据 长度可变, 默认长度是 1 500 字节。最常使用的是数据字段封装 IP 数据报。
- 帧校验序列 FCS 差错校验的循环冗余校验码。

4-20 画图说明住宅用户 PC 使用 PPP 拨号接入 Internet 的网络结构和协议结构。

解答: 住宅用户计算机使用 PPP 协议通过 modem 拨号连接公共交换电话网 PSTN

进行 Internet 接入是 PPP 应用的常见例子。图 1-4-7 表示这种应用的网络结构,图中,M 为 modem,R 为路由器,ISP 为提供远程用户接入设备和接入服务 Internet 服务提供商。图 1-4-8 是协议结构,用户的 IP 数据报封装在 PPP 帧中,由 modem 调制为模拟信号,通过公共电话网拨号传输到远程的 Internet 服务器。这种 Internet 接入服务一般是由 ISP 提供的。

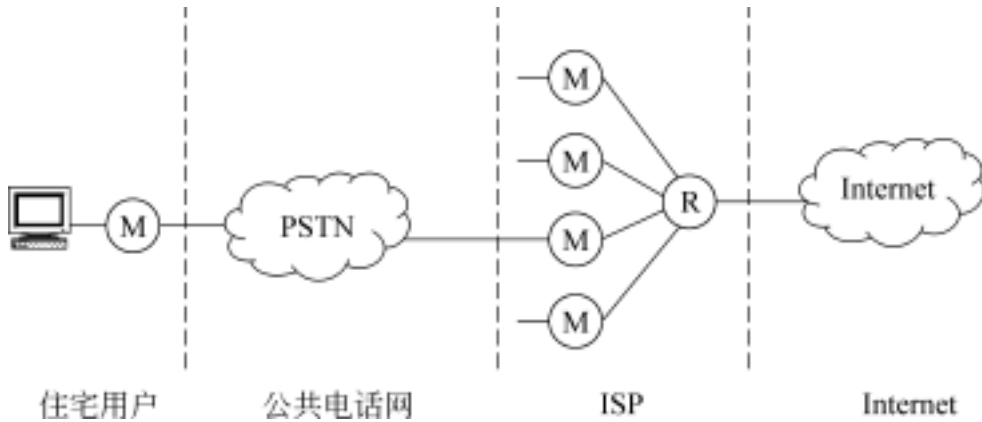


图 1-4-7 使用 PPP 拨号入网的网络结构

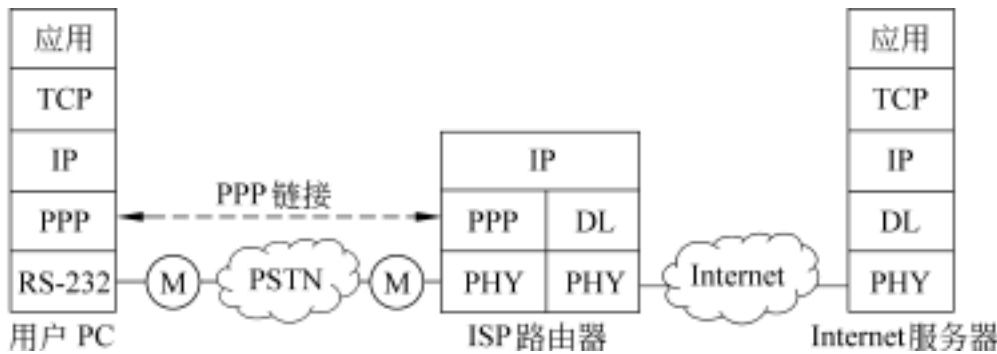


图 1-4-8 使用 PPP 拨号入网的协议结构

4-21 为了进行差错控制,必须对传送的数据帧进行校验。在数据链路层广泛使用的校验方法是__ (1) __ 校验,接收端发现帧校验错误后采取的措施一般是__ (2) __。CRC-16 标准规定的生成多项式为 $G(x) = x^{16} + x^{15} + x^2 + 1$,它产生的校验码是__ (3) __ 位。如果 CRC 的生成多项式为 $G(x) = x^4 + x + 1$,信息码字为 10110,则计算出的 CRC 校验码是__ (4) __。

- | | | | |
|--------------|----------|------------|--------------|
| (1) A . 奇偶 | B . 海明 | C . 校验和 | D . 循环冗余 |
| (2) A . 自动纠错 | B . 报告上层 | C . 自动请求重发 | D . 重新生成原始数据 |
| (3) A . 2 | B . 4 | C . 16 | D . 32 |
| (4) A . 0100 | B . 1010 | C . 0111 | D . 1001 |

答案: D, C, C, D

4-22 HDLC 是一种_____协议。

- | | |
|-----------------|------------------|
| A . 面向比特的同步链路控制 | B . 面向字节数的异步链路控制 |
| C . 面向字符的同步链路控制 | D . 面向比特的异步链路控制 |

答案: A

4-23 PPP 是 Internet 中使用的__ (1) __,其功能对应于 OSI 参考模型的__ (2) __,以__ (3) __ 协议为基础。PPP 使用面向__ (4) __ 的填充方式。

- (1) A . 报文控制协议

B . 分组控制协议

C . 点到点协议

D . 高级数据链路控制协议
- (2) A . 数据链路层

B . 网络层

C . 传输层

D . 应用层
- (3) A . TCP/ IP

B . NetBEUI

C . SLIP

D . HDLC
- (4) A . 比特

B . 字符

C . 透明传输

D . 帧

答案: C, A, D, B

第 5 章

局域网体系结构

5-1 IEEE802 LAN/ RM 和 OSI/ RM 的对应关系如何?IEEE802 LAN/ RM 把数据链路层分为哪两层?为什么这样分?

解答: IEEE802 LAN/ RM 和 OSI/ RM 的下两层即物理层和数据链路层相对应。

IEEE802 LAN/ RM 把数据链路层分为逻辑链路控制(LLC)子层和媒体接入控制(MAC)子层,媒体接入控制也称为介质访问控制。LLC 在上,MAC 在下。

这样划分使得数据链路层中与媒体接入无关的部分都集中在 LLC 子层,而和媒体接入相关的部分集中到 MAC 子层去处理。也就是说在 LLC 子层上看不到具体的局域网,隐藏了各种 IEEE802 物理网络的差异,向网络层提供统一的帧格式和接口,提供与媒体无关的链路控制,包括差错控制和流量控制等。在 MAC 子层才能看见所连接的是什么标准的局域网,是总线网、令牌环还是令牌总线网等,MAC 子层依赖物理媒体的不同而各不相同。

5-2 LAN 的共享信道访问要解决什么问题?有哪两种媒体接入控制技术?它们各有什么特点?

解答: LAN 由多个站点共享同一信道,任何一个站都可以使用信道,但任何时候信道只能由一个站点占用。因此,共享信道访问要解决一个重要问题就是信道争用问题,媒体接入控制(MAC)就是解决这一问题的技术。

共享信道的多点接入亦称多点访问(multiple access)技术可以划分为两类,即受控接入和随机接入。

受控接入的特点是网上的各个站点不能随意访问信道,而必须受到一定的制约。一般,受控接入方式每一时刻只有一个站点访问信道。受控接入又分为两种:集中式控制和分散式控制。集中式控制方式在网上设置一台主机,由它控制站点的访问权,多点轮询(polling)就属于集中式控制方式。分散式控制不设主控站点。令牌环网就属于分散式控制方式,环网上的站点只有持有令牌者才能发送信息,发送后立即将令牌传递下去。

随机接入的特点是网上的各个站点都可以根据自己的意愿随机地接入信道。总线型网属于这一类。随机接入方式中,如果两个或两个以上站点同时发送信息则会产生冲突,因此应该尽量避免冲突的产生并要解决冲突带来的问题。

5-3 描述 IEEE802 LAN 6 字节 MAC 地址的结构。

解答: IEEE802 3 规定的 6 字节 MAC 地址是目前广泛使用的 LAN 物理地址。

IEEE802 规定 LAN 地址字段的第一个字节的最低位表示 I/G (Individual/ Group) 比特, 即单地址/ 组地址比特。当它为“0”时, 表示它代表一个单播地址, 而这个位为“1”时, 表示它代表一个组地址。

IEEE802 规定 LAN 地址字段的第一个字节的最低第二位表示 G/L (Global/ Local) 比特, 即全球/ 本地比特。当这个比特为“0”时表示全球管理, 物理地址是由全球局域网地址的法定管理机构统一管理, 全球管理地址在全球范围内不会发生地址冲突。当这个比特为“1”时, 就是本地管理, 局域网管理员可以任意分配局部管理的网络上的地址, 只要在自己网络中地址惟一不产生冲突即可, 对外则没有意义, 局部管理很少使用。

在 6 个字节的其他 46 个比特用来标识一个特定的 MAC 地址, 46 位的地址空间可表示 2^{46} 约 70 万亿个地址, 可以保证全球地址的惟一性。

5-4 IEEE802.2 数据链路层使用哪两种地址? 它们分别用在哪两个子层? 分别用于什么寻址?

解答: IEEE802 局域网数据链路层通信使用 MAC 地址和 SAP 地址。MAC 地址在 MAC 子层使用, 标识网络中的站点, SAP 地址在 LLC 子层的地址, 提供对高层(网络层)的接口, 标识该站点中网络层的通信进程。

有了这两种地址的定义, IEEE802 局域网中的寻址分为两步: 首先用 MAC 帧的 MAC 地址信息找到网络中的某一个站点, 然后用 LLC 帧的目的 SAP 地址 DASP 找到该站点中网络层的某一个进程。

5-5 IEEE802.2 逻辑链路控制协议向上层提供哪几种服务?

解答: IEEE802.2 逻辑链路控制协议向上层主要提供 3 种服务:

LLC1, 不确认的无连接服务

LLC1 相当于数据报服务, 不建立连接, 也不使用确认机制, 不提供可靠性, 实现起来非常简单, 在以太网等局域网中应用。

LLC2, 可靠的面向连接的服务

LLC2 相当于虚电路服务。每次通信都要进行两个 LLC 实体之间连接建立、数据传送和连接断开这三个过程, LLC2 还提供了差错控制和流量控制, 以实现可靠的服务。

LLC3, 带确认的无连接服务

LLC3 不建立连接而直接发送数据, 但收方给予确认。适合于传送某些非常重要且实时性也很强的信息, 如自动控制系统中的报警信息或控制信号等, 如不要确认则不够可靠, 但若先建立连接又嫌太慢。

5-6 在 OSI 的哪些层上描述了以太网的功能?

- A . 应用层 B . 传输层 C . 网络层 D . 数据链路层
E . 物理层

答案: D, E

5-7 局域网中下列哪种拓扑结构是逻辑上的, 而不是物理上?

- A . 星型 B . 环形 C . 总线型 D . 令牌总线

答案: D

5-8 从哪里可以获取 MAC 地址 ?

A . DHCP 服务器

B . 由网络管理员配置

C . 网卡的 ROM 中

D . 在计算机的网络配置中

E . 在微处理器芯片中

答案: C

第 6 章

以太网

6-1 简介以太网的两个重要的规范。

解答：以太网有 DIX 以太网和 IEEE802.3 以太网两个重要规范。

1980 年,美国 DEC 公司、Intel 公司和 Xerox 公司合作,共同提出了 DIX 1.0 版以太网规范,1982 年 DIX 以 2.0 版作为终结,称为 DIX 以太网。这是世界上第一个局域网规范,并使用到今天。

1983 年底,在 DIX 以太网的基础上,IEEE 提出了 IEEE802.3 10Base5 以太网规范,这是 IEEE802.3 的第一个以太网标准。1989 年 ISO 以标准号 ISO8802.3 采纳了 IEEE802.3 标准。自 1983 年 IEEE802.3 10Base5 标准之后,以太网又不断发展前进,形成了 IEEE802.3 以太网系列标准,成为 IEEE802 标准中最成功的标准。

DIX 以太网和 IEEE802.3 以太网是以太网发展中的两个历史性的规范,有着非常重大的影响和广泛的应用。它们只有很小的差别,主要是对帧格式中个别字段的定义不同。

6-2 描述 ALOHA 的随机接入的工作原理,并用图形说明。

解答：ALOHA 中,只要某一个站点想发送信息,它就把信息发出去。然后它听一段时间,如果在规定的时间内(信息的最大的往返时间)之内收到了确认,则发送成功;否则,重发信息帧。发生冲突的各站不宜在知道发生冲突后马上就重发,因为这样会继续产生冲突。ALOHA 采用的重发策略是冲突的各站等待一段随机时间,然后再重发。如果重发多次仍然收不到确认,就放弃发送。

接收站点收到信息后,比较自己的地址和信息帧头部的目的地址,如果相符就接收此帧。接收站点还通过检查帧的校验序列字段来决定传输是否正确。如果正确,则发回一个确认。如果因为线路的噪声干扰或有其他站同时发送而产生冲突,会使收到的帧的校验不正确,接收站点将抛弃此帧。

图 1-6-1 说明 ALOHA 的工作情况,假设共有 N 个站点,用 T_0 代表发送一个帧所需的时间。

当站 1 发送帧 1 时,其他站都未发送数据,所以站 1 发送成功。而随后站 2 和站 3 发送的帧 2 和帧 3 在时间上有重叠,因而产生冲突。冲突的结果是使冲突的各方发送的数据都出现差错,因而都必须重发。

6-3 分隙 ALOHA 对 ALOHA 的改进是什么? 最大吞吐量提高到了多大?

解答：分隙 ALOHA 是将所有站在时间上都同步起来,并将时间划分为一段段等长的时隙,规定不论帧在何时产生,它只能在每个时隙开始时刻才能发送。一个帧若要发送

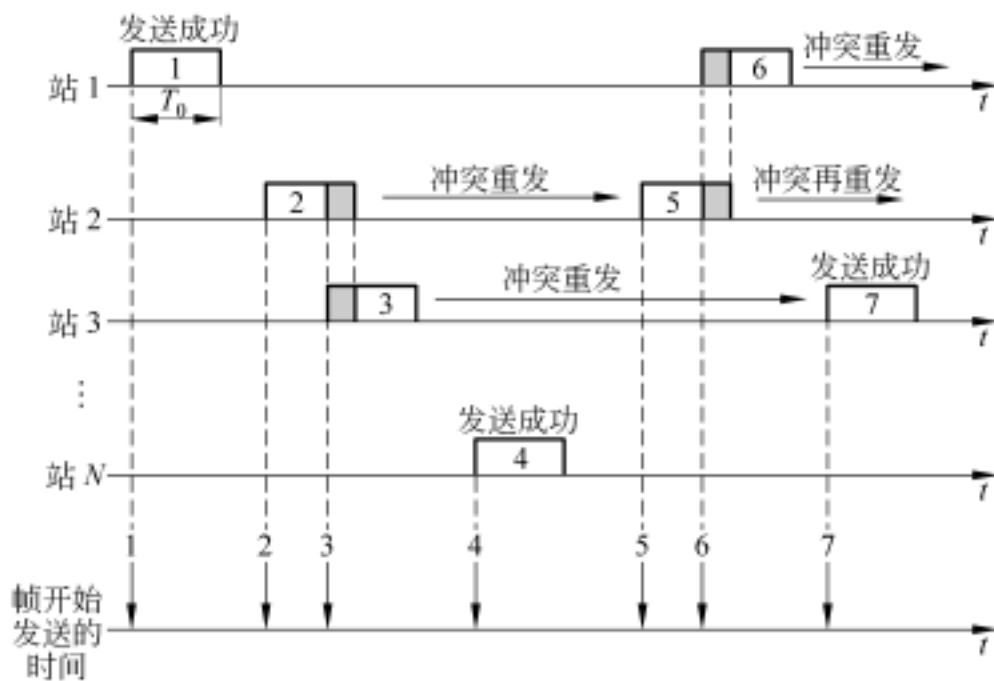


图 1-6-1 ALOHA 的工作情况

成功,ALOHA 则需要 $2T_0$ 时间间隔内没有其他帧发送,而分隙 ALOHA 只要求 T_0 时间间隔内没有其他帧发送。因此,如果网络上发送帧的情况相同,分隙 ALOHA 比 ALOHA 更容易发送成功,更不容易产生冲突,因而有更好的性能。

分隙 ALOHA 将 ALOHA 系统的 0.184 的最大吞吐量提高到了 0.368。

6-4 CSMA 对 ALOHA 的改进主要是什么?目的是什么?

解答:载波监听多点接入 CSMA 是从 ALOHA 演变出的一种协议,主要改进是增加了载波监听的机制,即每个站在发送数据前先监听信道上其他站是否在发送数据,如果监听到有其他站发送的信号,就暂不发送。

这一改进的目的是减少发送时机的随意性和盲目性,从而避免不必要的冲突,提高系统的吞吐量。

6-5 CSMA 有哪 3 种算法?描述这些算法。

解答:CSMA 的 3 种算法是:非坚持 CSMA、1 坚持 CSMA 和 p 坚持 CSMA。

非坚持 CSMA,欲发送的站点监听信道并按以下规则执行:

- (1) 若信道空闲,发送;否则,转到(2)。
- (2) 若信道忙,等待一段随机延迟时间,重复(1)。

等待随机延迟时间可以减少冲突的可能性。假设有一个传输在进行中时,又有两个站点准备发送并监听,如果这两个站点等待相同的时间,它们会试图在同一时刻发送而产生冲突。

非坚持 CSMA 有一个明显的缺点,由于一旦监听到信道忙就延迟一个随机时间再重新监听,但很可能在再次监听之前信道就已经空闲了,不能从信道刚一变成空闲的时刻起就开始利用它,这样降低了信道的利用率。

1 坚持 CSMA,欲传输的站点监听信道并按以下规则执行:

- (1) 若信道空闲则发送;否则,转到(2)。
- (2) 若信道忙,一直监听,直到信道空闲马上发送。

1 坚持算法可以在信道刚一空闲时就开始利用,增加了信道的利用率,但如果有两个或两个以上的站点都要发送,那么就会发生冲突,因而冲突的机会则比非坚持方式增加了。

p 坚持 CSMA,规则如下:

- (1) 若信道空闲,按 p 概率发送,按 $(1 - p)$ 的概率延迟一个时间单位。这个时间单位一般等于最大的传播时延。
- (2) 若信道忙,继续监听直到信道变为空闲,重复(1)。
- (3) 若传输被延迟了一个时间单位,重复(1)。

p 坚持 CSMA 是非坚持方式和 1 坚持方式之间的折衷,可根据通信量多少设定不同的概率 p ,以达到较高的信道利用率。

6-6 CSMA 使用了载波监听的机制,但还可能产生冲突,为什么? 试画图分析。

解答: CSMA 使用了发送前先监听信道的机制,减少了发送冲突的机会,但并不能完全避免冲突,还可能产生冲突,这是因为信号传播时延引起的。

图 1-6-2 表示 CSMA 总线上的两个站 A 和 B,它们之间的信号传播时延为 τ ,A 向 B 发出的数据经 τ 之后才能传播到 B。因此,在 A 开始发送数据 DATA(A)起 $0 \sim \tau$ 这个范围内,B 的载波监听检测不到 A 在发送数据,若这段时间内 B 也有自己的数据 DATA(B)要发送,它也可以发送,那么必然会和 A 发送的帧发生冲突,DATA(B)和 DATA(A) 在总线上混叠,图中表示了这种情况。可见,虽然是在监听到信道空闲时开始发送,但由于信号传播时延的影响,若两个(多个)站的发送间隔在 $0 \sim \tau$ 的范围内,CSMA 算法仍会产生冲突。

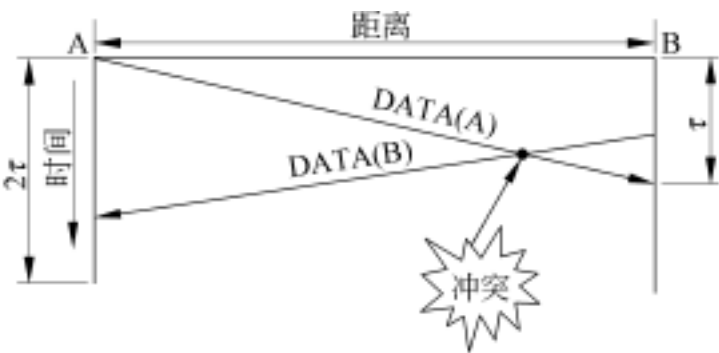


图 1-6-2 信号传播时延引起的冲突

6-7 CSMA/ CD 对 CSMA 的改进主要是什么? 目的是什么? 对于 10Mb/s 的帧长 1 500 字节的以太网,改进后可以减少多长时间的因冲突造成的信道浪费?

解答: CSMA 的发送前监听的措施减少了冲突的机会,但由于传播时延的原因,冲突不可能完全避免,而且冲突引起的信道的浪费是相当大的。CSMA/ CD 对 CSMA 的改进主要是增加了冲突检测的机制,检测到冲突时停止数据的发送,这样就可以减少无意义的的数据发送时间,因而降低了冲突时信道带宽的浪费。

对于帧长 1 500 字节的数据帧,发送它需要 12 000 位时,对于 10Mb/s 的比特率,则发送完一帧需要 1 200 μ s。如果一旦检测到冲突立即停止发送而不要将一帧全部发完,就可以节省无意义发送时间。节省的时间为 1 200 μ s 减去冲突处理的时间。冲突时信道占用的时间最大为 $3 \tau + T_1$ (2τ 和 T_1 分别为以太网的时槽和冲突后阻塞信号的发送时间),

对应 800 位时,对于 10Mb/s 比特率的以太网为 80μs。这样,冲突检测节约的时间可达 $1\,200 - 80 = 1\,120\mu\text{s}$ 。

6-8 为什么说 CSMA/CD 是一种半双工工作方式?

解答:CSMA/CD 方式中,每个时刻总线上只能有一路传输,如果有两路传输就会产生冲突,但总线上的数据传输方可以是两个方向,因此,CSMA/CD 媒体接入控制方式的以太网是一种半双工传输方式。

6-9 在 Internet 中,为什么说以太网为 IP 数据报提供的是无连接、不可靠的传输服务?

解答:以太网的 CSMA/CD 媒体接入方式在数据传输前并不建立连接,接收方虽然进行 CRC 校验,但并不使用确认机制,既无连接又不确认。对校验错误的帧,DIX 以太网只是简单的丢弃;IEEE802.3 以太网丢弃并通知 LLC 子层,不同类型的 LLC 子层可以进行不同的差错处理,但 IEEE802.3 本身并不作处理。因此,以太网向上层提供的是无连接、不可靠的帧传输服务。

在 Internet 世界中,一般 IP 数据报使用 DIX 以太网封装,而使用 IEEE802.3 以太网时,通常使用逻辑链路层的 LLC1,即不确认无连接的服务,因此以太网为 IP 数据报提供的是无连接、不可靠的传输服务。在 Internet 中,传输的可靠性由上层协议来保证,一般是 TCP。

6-10 以太网帧所携带数据的最小长度是多少?为什么?

解答:以太网帧所携带数据的最小长度是 46 个字节。10Mb/s 以太网的时槽规定为 512 位时,也就是说,总线上信号往返的最大时间为 512 位时。产生冲突时,CSMA/CD 为了能够正常进行冲突检测,在最大往返时间之后,从总线上接收的信号必须是自己发送信号和其他站信号的混叠信号,也就是说,此时自己必须仍然在发送数据。这就要求以太网最小帧长度为 64 个字节,即 512 位。那么,以太网帧数据字段的最小长度为 46 个字节。46 个字节加上 12 字节的源地址和目的地址、2 字节的数据长度及 4 字节的 FCS,最小帧长度共 64 字节。

6-11 什么是冲突域?在 10Mb/s、100Mb/s 和 1 000Mb/s 以太网中,时槽规定为多大?相应的冲突域的最大网络跨距有多大?

解答:冲突域指一个 CSMA/CD 以太网区域,同一个冲突域中的两个或多个站点同时发送数据就会产生冲突,CSMA/CD 在冲突域内能正常进行冲突检测,超出冲突域 CSMA/CD 就不能正常工作。冲突域限制了 CSMA/CD 以太网的最大网络跨距。

时槽的长度和冲突域的最大网络跨距是相对应的。10Mb/s 和 100Mb/s 以太网,时槽规定为 512 位时,即 51.2μs 和 5.12μs,最大网络分别直径为 2 000m 和 200m。对于 1 000Mb/s 以太网,时槽扩大为 4 096 位时,冲突域的最大网络直径仍为 200m。需要说明的是,上面所说的冲突域的最大网络跨距并不是一个精确的概念。

6-12 什么是冲突碎片?冲突碎片的长度是多少?

解答:CSMA/CD 检测到冲突后就停止发送数据并发送阻塞信号,这些已发送的有冲突的不完整数据称为冲突碎片。由于 CSMA/CD 的冲突只能发生在 512 位时的冲突窗口范围之内,因此发送站检测到冲突后停止发送而产生的冲突碎片的长度小于 512

比特。

6-13 自己设计一个 CSMA/CD 网络,信息传输速率 100Mb/s,网络最大长度 10km,电缆中信号传播速度为 1km/5μs,网络设备的处理时延共 10μs,要保证网络正常进行冲突检测,最小帧长度应该是多少?若数据发送速率为 1Gb/s 呢?

解答:信号在总线上的往返的最大时间 $2\tau = 2 \times (10\text{km} \div 1\text{km}/5\mu\text{s} + 10\mu\text{s}) = 120\mu\text{s}$
 $100\text{Mb/s} \times 120\mu\text{s} = 12\,000\text{b} = 1\,500\text{ 字节}$
 $1\,000\text{Mb/s} \times 120\mu\text{s} = 120\,000\text{b} = 15\,000\text{ 字节}$

因此,当数据速率 100Mb/s 时,最小帧长度应该是 1 500 字节,当数据速率 1Gb/s 时,最小帧长度是 15 000 字节。

6-14 以太网冲突以后采用什么回退重试算法?对该算法进行说明。在严重突出的情况下,以太网的重试时机最多可以达到多少个?

解答:以太网采用截断二进制指数回退算法控制回退重试时间。截断二进制指数回退算法是由二进制指数回退算法改进而来的。二进制指数后退算法为:

$$T = 2^i \times (2^i - 1)$$

式中: T 为回退时间范围; i 为冲突次数,每冲突一次 i 加 1; 2^i : 时槽。以太网使用上式求得回退时间范围,并将 T 划分为长度为 2^i 的 $2^i - 1$ 个时槽,重试时机在这些时槽的开始时刻随机选取。比如 $i = 3$,重试延时时间将在 0,1,2,3,4,5,6 或 7 个时槽共 $2^3 = 8$ 种情况中随机选取。这种方式减小了再次发生冲突的概率。

IEEE802.3 规定重试次数 i 上限为 16,即尝试了 16 次仍然不能发送成功,则放弃本次发送。IEEE802.3 还规定 $i > 10$ 后 T 值不再增加,即第 10 次重试之后回退时间维持不变,此时延时时间上限为 $2^{10} - 1 = 1\,023$ 个时槽,不再加长,到此截断。因此这种改进的二进制指数回退算法称为截断式二进制指数回退算法。

在严重冲突的情况下,重试时间最多在 0 ~ 1 023 个 2^i 范围里随机选择,一个站可能有 1 024 个可能的重试时机。

6-15 以太网的回退算法中,假设总线上总是有 2 个站(包括冲突后回退到时的和新加入的)要发送数据,问:第 2 次冲突后,发生冲突和发送成功的概率是多少?第 3 次和第 i 次冲突之后呢?

解答:第 2 次冲突后,每个站的重试时机有 $2^i = 2^2 = 4$ 个,因此,每个站在某个重试时刻发送的概率是 $1/4$,2 个站在同一重试时刻发送的概率是 $1/4 \times 1/4 = 1/16$ (因为是独立的事件)。那么,4 个重试时刻发生冲突的总概率为 $4 \times 1/16 = 1/4$ 。

第 3 次冲突后,发生冲突的总概率为 $8 \times (1/8 \times 1/8) = 1/8$ 。

第 i 次冲突后,发生冲突的总概率为 $2^i \times (1/2^i \times 1/2^i) = 1/2^i$ 。

6-16 参数 a 即归一化的传播时延与以太网性能有很大关系,试举例分析参数 a 对以太网利用率的影响(不考虑冲突)。

解答:归一化的传播时延 $a = \tau / T_0 = \text{总线单程比特长度} / \text{帧的比特长度}$,它对以太网的利用率有很大的影响。比如, $a = 0.05$,帧的比特长度是总线单程比特长度的 20 倍,如果在 $t = 0$ 时开始发送一帧数据,在 $t = \tau$ 时,经过了总线单程传播时延,总线已被比特流填满,而此时一帧数据才发送了 5%,到 $t = 20\tau$ 时,一帧数据的最后一个比特送入总线,此时

总线上仍填满了比特流,直到 $t=21$ 时,最后一个比特到达接收站,总线才空闲下来。可见,在 $0\sim 21$ 的传输时间中, $0\sim$ 和 $20\sim 21$ 的时间段里总线平均被比特流填满一半,而 ~ 20 的大部分时间段里总线都被比特流填满,总线利用率高达 $20/21(95\%)$ 。

如果 a 增大,比如 $a=0.5$, $T_0=2$, 帧的比特长度是总线单程比特长度的 2 倍,同样可以分析,此时总线利用率只有 $2/3(67\%)$ 。

可见,在其他条件不变时, a 越小,总线的利用率越高,可以达到的吞吐量越大。

6-17 在 DIX 以太网和 IEEE802.3 以太网的帧结构中,长度/类型字段的意义有什么不同?

解答:在 DIX 以太网标准中这一字段定义为类型字段,它指明数据字段中携带哪种网络层协议的数据,以太网可以为多种网络层协议提供传输服务。类型字段使得 DIX 以太网和上层协议绑定起来。在发送方,多个上层网络层协议可以复用一個以太网发送数据;在接收方,以太网根据接收的帧的类型字段决定将数据送给网络层的哪一个进程,这一过程称为解复用。

在 IEEE802.3 以太网标准中这一字段定义不同。老的 IEEE802.3 标准将这个字段定义为长度字段,指明其后数据字段中数据的字节数。1997 年后,新的 IEEE802.3 标准将这个字段修改为长度/类型字段。当它的值大于等于 1536(0x0600)时为类型,否则为长度,这不会发生混淆。这一修改适应了技术的发展,1997 年制定的 IEEE802.3x 全双工以太网标准中,定义了 MAC control 帧,进行流量控制,因而使用了类型字段,其值为 0x8808。

6-18 IEEE802.3 10Mb/s 以太网的物理层包括哪几个部分?它们的功能是什么? 10Mb/s 以太网网络接口卡 NIC 包括哪几个部分?它们的功能是什么?

解答:IEEE802.3 10Mb/s 以太网的物理层包括以下 3 个部分:

1. 媒体连接单元 MAU

MAU 一般称为收发器,它包括物理媒体连接 PMA 子层和媒体相关接口 MDI,它在计算机和传输媒体之间提供机械和电气的接口,其中机械接口由 MDI 实现,电气接口由 PMA 实现。MAU 的主要功能如下:

提供与传输媒体的机械连接 媒体相关接口 MDI 在机械上提供和媒体的机械连接,媒体不同,MDI 也不同。

信号发送与接收 发送时从物理信号 PLS 子层经收发器电缆得到曼彻斯特码信号向总线发送;反方向,从总线接收曼彻斯特码信号经收发器电缆传送给 PLS 子层。

冲突检测 检测总线上发生的数据帧冲突。

超长控制 当发生上述故障时,站点有可能向总线连续不断地发送无规律的数据使其他站点不能正常工作。当检测到某一数据帧超过此上限时,自动禁止该站向总线发送数据。

2. 物理层信号 PLS

它的主要功能如下:

编码解码 发送时,将由 MAC 子层来的串行数据编为曼彻斯特码并通过收发器

电缆送到收发器;反之,接收接入单元接口 AUI 送来的曼彻斯特码信号并进行解码,并以串行方式送给 MAC。

载波监听 确定信道是否空闲,载波监听信号送给 MAC 部分。

3. 接入单元接口 AUI

AUI 接口连接 PLS 和 MAU, AUI 上的信号有 4 种:发送和接收的曼彻斯特码信号、冲突信号和电源。

网络接口卡 NIC 主要涉及 IEEE802.3 以太网的物理层和 MAC 子层,包括以下 5 个部分:

1. 媒体接入单元 MAU

2. 物理层信号 PLS

3. 接入单元接口 AUI

以上 3 个部分属于 IEEE802.3 以太网的物理层,其功能上面已讲到。

4. 媒体接入控制 MAC 子层

它属于 IEEE802.3 的数据链路层,主要功能如下:

数据的封装与解封 发送数据时,将 LLC 子层提交下来的 LLC 帧装上 MAC 子层的首部和尾部,成为 MAC 帧;接收数据时,将 MAC 帧剥去首部和尾部成为 LLC 子层数据帧,交 LLC 子层。

实现发送和接收数据的并-串和串-并转换,它与 PLS 之间传送串行数据。

帧的定界和寻址处理,接收的目的地址不匹配的帧将被丢弃。

媒体接入控制 实现以太网 CSMA/CD 媒体接入控制协议。

差错校验 发送数据时,生成 FCS;接收数据时,校验 FCS。

5. 计算机总线接口

该接口(如 PCI 总线接口),实现和计算机的连接。

6-19 以太网中继器工作在什么层次?它的主要功能是什么?

解答:中继器工作在 IEEE802.3 的物理层,接收、恢复并转发物理信号,扩展以太网,但不能扩大以太网的冲突域。

中继器的主要功能如下:

中继器连接以太网网段,接收、恢复并转发物理信号 当某一端口接收信号时,中继器进行放大、整形并将其转发到其他每个端口(不包括接收信号的端口),消除信号经过一段长电缆传输后造成的幅度衰减和波形失真,使之不会在传输线路上积累。

检测并传播冲突 多口中继器(集线器)若检测到两个或多个端口都接收到信号,将向所有端口(包括接收信号的端口)发出阻塞(jam)信号,以通知其他站点,这使发送信号的计算机也能检测到冲突。

检测并隔离故障端口 如果中继器发现某一端口连接的网段上出现故障,如所连接的站点超长发送,中继器将发生故障的端口和其他部分自动隔离开来,以使网络正常工作。

6-20 描述 10BaseT 以太网的连网方法和网络扩展方式。

解答: 一个最基本的 10BaseT 以太网由一个集线器(hub)和若干台计算机连接而成。所有的站点都通过 UTP 点到点连接到 hub 上,形成一个以 hub 为中心的星型结构。hub 和每个站点之间的 UTP 电缆最大距离规定为 100m。计算机和 hub 的连接方式是通过 RJ45 连接器相连。

10BaseT 双绞线以太网扩展方法主要有 hub 间的级连和堆叠两种。

级连是把 hub 连在一起扩大双绞线以太网覆盖范围的一种方法。在每一条通路上, 10BaseT 一般最多可以串接 5 个网段 4 个 hub。不过部分公司的产品允许级连的 hub 个可以超过 4 个。hub 与 hub 之间 UTP 电缆的最大长度也是 100m。hub 级连扩展了网络的跨距,也扩大了网络连接的站点数。

hub 可以堆叠在一起。可堆叠 hub 上专门设有 hub 堆叠的连接接口,用专用的电缆把几台堆叠的 hub 连接在一起。这样,多台堆叠的 hub 逻辑上就视同一台 hub,它们的端口都连到公共的总线上。堆叠的 hub 所能连网的站点数等于每台 hub 上能连接的站点数的总和。可堆叠的 hub 数量一般为 4~8 个。hub 堆叠只是扩展 10BaseT 以太网连接的站点数量,并不能扩展网络跨距。

通过级连和堆叠扩展的双绞线以太网,最大网段数和站点数均为 1024,都在一个冲突域中。而且,扩展连接的工作站数量越多,每个工作站所平均得到的带宽就越小。

6-21 比较 100BaseT 和 10Mb/s 以太网的 MAC 子层。

解答: 100BaseT 保持了与 10Mb/s 以太网同样的 MAC 子层,使用同样的 CSMA/CD 协议和相同的帧格式。它们包括同样的基本内容:最大帧长 1518 字节,最小帧长 64 字节,重试上限 16 次,后退上限 10 次,时槽 512 位时,阻塞信号 32 比特,帧间间隔 IFG 96 比特。

但是,因为 100BaseT 传输速率是 10Mb/s 以太网的 10 倍,100BaseT 的时槽的位数虽然和 10Mb/s 以太网一样,但时间小了 10 倍,变为 5.12μs,这使得 100BaseT 以太网冲突域的网络跨距也差不多减小了 10 倍,减小到 200m。

6-22 100BaseT 高速以太网有哪几个物理层标准?简述它们的特点。

解答: 100BaseT 标准包括 4 种不同的物理层规范。

1. 100BaseTX

100BaseTX 是 100BaseT 中使用最广泛的一种。100BaseTX 使用 5 类及以上的 UTP 的两对线芯,一对用于发送,另一对用于接收,但其他两对线芯不能做它用,以避免其他信号共享电缆引起的干扰。100BaseTX 最大网段长度为 100m,也可使用 IBM 的 1 型屏蔽双绞线 STP。100BaseTX 使用 RJ45 连接器,但插座必须是 5 类的。100BaseTX 采用 4B/5B-MLT3 编码。

2. 100BaseT4

100BaseT4 是使用 3 类 UTP 的快速以太网。已经安装的以太网多使用 10BaseT 标准,它使用 3 类 UTP 4 对双绞线中的 2 对线芯,但大多数 3 类布线都安装了 4 对,这给由 10BaseT 迁移到 100Mb/s 的用户带来了方便。这正是制定 100BaseT4 标准的初衷。

100BaseT4 支持 3 类及以上的 UTP 电缆上使用 4 对双绞线路的 100Mb/s 数据传

输,其中 3 对线用来传输数据,第 4 对线用作冲突检测的接收信道。100BaseT4 的最大网段长度也为 100m。100BaseT4 也使用 100BaseTX 使用的 8 针 RJ45 连接器。100BaseT4 使用 8B/6T 编码方式,即 8 位二进制/6 位三进制编码,三进制编码对应着 3 种电平信号。

3 . 100BaseT2

100Base T2 设计成在话音级 3 类 UTP 或更好的 UTP 的 2 对信号线上传送 100Mb/ s 的信号。为了在 2 对 3 类 UTP 上传输 100Mb/ s 的信号,100BaseT2 使用了非常复杂的 PAM5×5 编码方式,将 4 位半字节数据编成 5 个电平的脉冲振幅调制系统的编码。100BaseT2 也使用 RJ45 连接器,网段最大长度也为 100m。

4 . 100BaseFX

100BaseFX 是使用光缆的快速以太网。光缆的传输距离远于 UTP,常用于高速主干网,以及有电气干扰的环境和有较高保密要求的情况。100BaseFX 一般使用一对 62.5/125(62.5μm 光纤芯/125μm 外包层)的多模光缆。在半双工模式下,站点间连接距离不超过 412m。当工作在双工模式下,最大连接长度可达到 2 000m。100BaseFX 使用与 FDDI 相同的 4B/5B-NRZI 编码方法。100BaseFX 的媒体接口推荐使用 SC 连接器,也可使用 ST 连接器及 MIC 连接器。

6-23 100BaseT4 如何用 3 类双绞线实现了 100Mb/ s 的信息传输速率 ?

解答: 100BaseT4 使用 8B/6T 编码方式,即 8 位二进制/6 位三进制编码,三进制编码对应着 3 种电平信号。6 位三进制可表示 $6^3 = 729$ 种码,其中的 256 种表示 8 位二进制码。

100Mb/ s 的数字信号用 8B/6T 编码后电信号传输速率为 $100M \times 6/8 = 75\text{Mbaud}$,电信号又以循环方式分送到 3 对线上传输,这样每对线上传输的电信号的波特率为 25Mbaud。3 类 UTP 的带宽为 16MHz, 根奈奎斯特准则,最高码元传输速率可达 32Mbaud,高于 25Mbaud,因此可以使用 3 类 UTP 传输 100BaseT4 的信号。

6-24 什么是 10/ 100Mb/ s 自动协商模式 ?

解答: 自动协商模式能自动把 UTP 线路两端的速率调节到最高的公共水平。自动协商模式使得以太网保持了即插即用的功能,简化了网络管理员的工作。

自动协商是链路初始化时进行的一种准静态的机制,在正常运行期间不能动态地改变链路性质。它工作在点到点链路上而不是整个网络。具有自动协商模式的网卡和 hub 等设备,在上电、人为或故障后重启后发送一个称为快速链路突发脉冲 FLP 的序列给链路的对方,其中包含了自己的链路类型及流量控制配置等信息,链路另一端的自动协商模式设备能够识别 FLP,协商选择双方都具备的最优的工作模式并进入工作状态。FLP 每 16ms 重复一次,直至协商完成。

链路类型协商的优先级由高到低是: 100BaseT2 全双工, 100BaseTX 全双工, 100BaseT2 半双工, 100BaseT4, 100BaseTX 半双工, 10BaseT 全双工, 10BaseT 半双工。

可见,自动协商功能协商的内容包括 10M/ 100Mb/ s 线路速率、全双工/ 半双工模式,另外,自动协商功能也支持不使用/ 使用全双工以太网的流量控制。

6-25 和 10Mb/ s 和 100Mb/ s 以太网相对比,简述半双工千兆以太网的 MAC 子层。

解答：(1) 与 10Mb/ s 和 100Mb/ s 以太网相同的帧格式和基本相同的 CSMA/ CD：最大帧长 1 518 字节，最小帧长 64 字节，重试上限 16 次，后退上限 10 次，阻塞信号 32 位，帧间间隔 IFG 96 位等。

(2) 时槽由 512 位时增大到 4 096 位时(512 字节时)，这使得它的最大网络跨距可达到能够实用的 200m。

(3) 为了使短帧的传输与大的时槽协调，千兆以太网增加了载波扩展措施。

(4) 为了改善短帧的传送效率，千兆以太网标准又增加了帧突发的功能。

6-26 千兆以太网有哪两种物理层标准？它们使用什么传输媒体？链路长度有多少？

解答：IEEE 制定的两类千兆以太网物理层标准：1000BaseX(802 .3z)光纤千兆以太网标准和 1000BaseT(802 .3ab)双绞线千兆以太网标准。

(1) 1000BaseX 包括 3 种不同的媒体。

1000BaseLX 基于波长为 1 270 ~ 1 355nm 的长波长激光传输器，可使用 62 .5/ 125μm、50/ 125μm 的多模光纤和 10μm 纤芯的单模光纤。

1000BaseSX 基于波长为 770 ~ 860nm 的短波长光纤激光传输器，可使用 62 .5/ 125μm 和 50/ 125μm 的多模光纤。

1000BaseCX 使用铜媒体，高质的 STP。

(2) 1000BaseT 使用 4 对 5 类 UTP(超 5 类 UTP 和 6 类的 UTP)，最长 100m。

千兆以太网各种物理层在半双工和全双工模式的链路长度限制汇总于表 1-6-1：

表 1-6-1 千兆位以太网各物理层在半双工和全双工模式下链路长度限制汇总

物理层标准	50μm MMF	62 .5μm MMF	10μm SMF	150 STP	5 类 UTP
	半双工/ 全双工	半双工/ 全双工	半双工/ 全双工	半双工/ 全双工	半双工/ 全双工
1000BaseSX	110 / 550	110 / 275			
1000BaseLX	110 / 550	110 / 550	110 / 5 000		
1000BaseCX				25 / 25	
1000Base T					100 / 100

6-27 千兆以太网为什么要进行载波扩展？载波扩展如何进行？

解答：千兆以太网标准将时槽从 512 位时增大到 4 096 位时(512 字节时)，使最大网络跨距仍可达 200m。但千兆以太网仍维持最小帧长度 64 字节不变。这样，千兆以太网中最小帧长的传输时间远小于时槽，不能正常进行 CSMA/ CD。为了使短帧的传输与大的时槽协调，以保证正常进行 CSMA/ CD，千兆以太网采取了载波扩展措施。

载波扩展是在发送长度小于一个时槽的短帧时，使用非数据信号的扩展位使得载波信号在网络上保持 4 096 位时。对于长度为 46 ~ 493 字节的数据段，载波扩展的长度为 448 ~ 1 字节。在发送帧信号和载波扩展信号的过程中，无论在什么时候检测到冲突，都会停止发送其余的帧或载波扩展位，发出阻塞信号，并执行回退重试算法。

在接收方,在接收到前导码和帧起始定界符 SFD 后,开始位计数,并把非载波扩展位存入接收缓冲区直至帧结束。若收到的位数小于一个时槽的位数,则收到的帧作为冲突碎片丢弃。即使接收到的帧的前部(帧头、数据和 FCS)是完整正确的,只是载波持续时间小于一个时槽,表明帧后部的载波扩展部分在传输中发生了冲突,此帧也要丢弃。因为此时发方因检测到冲突要进行重发,如不丢弃就会造成收方收到重复帧,而协议不能处理接收重复帧的情况。

6-28 千兆以太网为什么要采用帧突发机制?帧突发如何进行?

解答:千兆以太网采用载波扩展扩大了冲突域直径,但在传送短帧时带来了额外的开销,影响了效率。为了改善短帧的传送效率,千兆以太网标准在 MAC 子层定义了帧突发的功能。

帧突发的机制如下:

发方被允许连续发几个帧,其中第一个帧按 CSMA/CD 规则发送。如果第一个是短帧,必须发送载波扩展位直至发送时间满一个时槽。若该帧发送成功,发方就可继续发其他帧直至发完数据或达到一次帧突发的最大长度限制。帧突发机制规定,连续发送的总长度限制在 8 192 字节之内。

发方为了连续占有信道,用 96 位载波扩展填充帧间间隔(IFG),这样其他主机在 IFG 期间仍可继续侦听到载波,不会启动发送。发送主机在成功发送第一个帧后不会再遇到冲突。因此,以后连续发送的帧即使是短帧也不必再进行载波扩展。帧突发机制是对载波扩展带来的传输效率低的补救措施。

6-29 叙述万兆以太网的特点和应用。

解答:万兆以太网有以下特点:

MAC 子层仍使用 IEEE802.3 帧格式,维持其最大、最小帧长度。

不再支持半双工的 CSMA/CD 媒体接入控制方式,只定义了全双工方式,这使万兆以太网的传输将不受 CSMA/CD 冲突域的限制,从而突破了局域网的概念,进入了城域网和广域网范畴,成为通用的组网技术。

在通用网的指导思想下,万兆以太网标准定义了两种物理层:局域网物理层和广域网物理层,它们都使用光纤作传输媒体,不再使用双绞线。局域网物理层传输速率 10Gb/s,而广域网物理层标准是通过 SONET/SDH 链路支持以太网帧,以 SONET OC-192c (9.584 64Gb/s) 的速率运行,这种方式的好处是可与现有的电信网络的 SONET/SDH 兼容,保护了原有的投资。

目前万兆以太网还不能定位于桌面应用,主要是在企业网、园区网和城域网作主干网,还可以通过万兆以太网将众多的企业网、园区网等局域网,通过 SONET/SDH 广域网络实现广域的高速连接。

6-30 简述万兆以太网物理层标准。

解答:目前定义了 3 种万兆以太网物理层标准:

(1) 10GBaseX LAN 类型的物理层,与使用光纤的 1000BaseX 相对应的物理层标准,使用与 1000BaseX 相同的 8B/10B 编码,信息传输速率 10Gb/s。

10GBaseX 只包含一个规范:并行的 LAN 物理层 10GBaseLX4。为了达到 10Gb/s 的信息传输速率,使用稀疏波分复用 CWDM 技术,在 1310nm 波长附近以 25nm 为间隔并列地配置了 4 对激光发送器/接收器组成的 4 条通道,为了保证每条通道的信息传输速率达到 2.5Gb/s,每条通道的 10B 码的码元速率为 3.125Gbaud。10GBaseLX4 使用多模光纤(MMF)和单模光纤(SMF)的传输距离分别为 300m 和 10km。

(2) 10GBaseR 串行的 LAN 类型的物理层,使用 64B/66B 编码,相比千兆以太网的 8B/10B 编码,它产生的编码开销由 25% 降到 3.125%,信息传输速率 10Gb/s。

10GBaseR 和下面要讲到的 10GBaseW 都属于串行的物理层技术,串行方式是指数据流发送接收直接进行,不拆分成多列,66B 码的码元速率高达 10.3125Gbaud。串行技术在逻辑上比并行技术简单,但对物理层器件的要求更高。

10GBaseR 包含三个规范:10GBaseSR、10GBaseLR 和 10GBaseER,分别使用 850nm 短波长、1310nm 长波长和 1550nm 超长波长。10GBaseSR 使用 MMF,传输距离一般为几十米,10GBaseLR 和 10GBaseER 使用 SMF,传输距离分别为 10km 和 40km。

(3) 10GBaseW 串行的 WAN 类型的物理层,采用 64B/66B 编码格式,它使用 SONET OC-192c 基本一致的帧格式和相同的 9.58464Gb/s 的信息传输速率。

10GBaseW 包含三个规范:10GBaseSW、10GBaseLW 和 10GBaseEW,分别使用 850nm 短波长、1310nm 长波长和 1550nm 超长波长。10GBaseSW 使用 MMF,传输距离一般为几十米,10GBaseLW 和 10GBaseEW 使用 SMF,传输距离分别为 10km 和 40km。

10GBaseW 可以向 SONET/SDH 基础设施提供访问能力,这使得以太网可以将 SONET/SDH 作为其主干传输网。

万兆以太网的 LAN 类型的物理层,并不意味着只用于 LAN,它也可用于 WAN。命名为 LAN 类型的物理层和 WAN 类型的物理层的原因是前者更适合支持原来基于以太网的业务和应用,而后者适合以现有的 WAN 中的 SONET/SDH 为传输网。

除了上述 3 种物理层标准外,IEEE 正在制定一项使用铜缆的称为 10GBaseCX4 的万兆以太网标准 IEEE802.3ak,可以在双芯同轴电缆上实现 10Gb/s 的信息传输速率,提供数据中心的以太网交换机和服务器群的(15m 之内)短距离 10Gb/s 连接的经济方式。10GBaseT 是另一种正在研究的万兆位以太网物理层,通过双绞线提供 100m 以内的 10Gb/s 以太网传输链路。

6-31 和中继器相比,网桥有什么特点?

解答:中继器在物理层扩展局域网,进行物理信号的放大、整形和转发。和中继器相比,网桥的主要特点是:

工作在 MAC 子层 网桥要检查帧的 MAC 地址,并据此查找转发表进行帧的转发。端口-地址表是网桥在转发过程中通过学习逐步建立起来的。

过滤了帧减少了通信量 网桥使同一个网段上各工作站之间的通信量不会经过网桥传到其他网段上去,仅局限于本网段的范围之内,减少了无谓的传输,减轻了局域网上总的负荷。

隔离了冲突域扩大了网络跨距 帧过滤功能使得在网桥连接的不同以太网网段

上同时传送数据时,不会产生冲突。网桥每个端口所连接的网段属于一个冲突域,而各个端口所连接网段被隔离为独立的冲突域,使网络跨度不受单个以太网冲突域的限制。

可连接不同类型的局域网 网桥可以连接不同类型的局域网。如通过网桥可以把以太网、令牌总线网和令牌环网连接在一起。

6-32 透明网桥如何通过学习建立起端口-地址桥接表？

解答：一个网桥刚刚连接到局域网上时,其桥接表是空的,网桥暂时还无法做出转发决策。此时网桥若收到一个帧,就采用泛洪法转发它,向除接收此帧的端口以外的所有端口转发。

网桥在转发过程中通过逆向学习法将其桥接表逐步建立起来。假若网桥收到从某一个端口 1 发来的帧,从帧的头部信息就可得知其源站地址 A。于是,网桥就可以推论出,在相反的方向上,只要以后收到发往目的站 A 的帧,就应当将此帧由端口 1 转发出去。于是就将站 A 的 MAC 地址和端口 1 作为一个表项登记在桥接表中。

局域网的拓扑可能会发生变化。为了使桥接表能动态地反映出网络的最新拓扑,可以在建立一个表项时将帧到达网桥的时间记录下来。超过规定的时间范围的表项,网桥将予以清除,重新学习。

6-33 交换机为什么能提高网络传输的流量？一个 24 口的 100Mb/s 的交换机可提供的最大带宽是多少？

解答：交换机(第二层交换机),工作在 MAC 子层,通过一个端口-地址表进行帧的转发。这使得交换机的多个端口可以并行地工作,可以同时接收从不同端口上发来的帧,又能将帧转发到许多其他端口上。交换机突破了共享带宽的限制,交换式以太网的带宽可以随着用户的增加而增加。

n 个端口的 RMb/s 快速以太网交换机最大可提供 $0.5 \times n \times RMb/s$ 的总带宽,当 n 增大时,总的网络带宽也随之增大。而 n 个端口的 RMb/s hub 只能提供 RMb/s 的带宽。

对于一个 24 口的 100Mb/s 的交换机最大可提供 1200Mb/s 的总带宽。

6-34 交换机由哪几个部分组成？帧转发机构有哪几种类型？它们的特点是什么？

解答：交换机由四个部分组成：端口、端口缓冲器、帧转发机构和底板体系。

帧转发机构在端口之间转发信息,有三种类型的交换机转发机构：

(1) 存储转发型 在数帧发送到一个端口之前先全部存储在内部缓冲器中,交换机的延迟时间等于整个帧的传输时间。存储转发类型交换机以 CRC 校验形式进行帧错误校验,能滤掉有问题的帧。

(2) 直通类型 只查看到帧的目的地址就立即转发,帧几乎可以立即转发出去,延迟时间大大缩短。但它把目的地址有效的所有信息帧全部转发出去,包括有差错的帧,不进行错误校验。

(3) 无碎片交换 结合上述两种类型交换机的优点,其作法是只暂存查看帧的前 64 字节,如果是有冲突的帧,冲突碎片小于 64 字节,就立即舍弃,否则就转发。它不进行差错校验,无法查出有校验错误的帧。在转发的效率和速度上是前两种方式的折衷。

6-35 一个工作组级的 100BaseTX 以太网,由一台 16 口 hub 连接 16 台计算机组成。现在要把它改造为交换式以太网,需要更新什么设备?改造前网络的带宽是多少?改造后网络能提供的最大带宽是多少?

解答:改造前网络是共享式以太网,把它改造为交换式以太网,需要将原来的 16 口 hub 更换为一台 16 口交换机,其余网络设备如网卡、双绞线及 RJ45 连接器等不动。改造前网络的带宽是 100Mb/s,改造后网络能提供的最大带宽是 800Mb/s。

6-36 全双工以太网的特点是什么?

解答:全双工以太网主要有如下特点:

全双工以太网使用交换机通过点对点链路连接计算机组成,在点对点媒体段上只能连接一对站点。计算机的网络接口和交换机必须支持全双工模式,能够配置成全双工模式。

全双工以太网能够同时发送和接收数据,因此它比半双工模式可以提供两倍的带宽。为此,需要使用支持全双工传输的媒体类型,支持同时进行数据发送和接收,10BaseT、10BaseFL、100BaseT4、100BaseTX、100BaseFX、100BaseT2、1000BaseX 的媒体系统支持全双工模式。

使用和半双工以太网同样的帧格式、最小帧长、帧间间隔 IFG 和 CRC 校验等。

不再使用 CSMA/CD 媒体接入控制方式,不使用载波监听,也不进行冲突检测,网络跨距也就不受 CSMA/CD 时槽的限制。

定义了显式的流量控制。

6-37 全双工以太网如何进行流量控制?

解答:全双工以太网的流量控制在 IEEE802.3x 标准进行了定义。IEEE802.3x 标准把 IEEE802 的数据链路层进一步分成了 3 个子层,在原来的 MAC 子层之上又加入了可选的 MAC 控制子层,它们一起对应原来 IEEE802 RM 的 MAC 子层。

全双工以太网在 MAC 控制子层定义了显式的流量控制。它使用 MAC control 帧传送 PAUSE 命令(也称为 PAUSE 帧),使全双工链路另一端的站点在一段时间内停止发送数据。

MAC control 帧由以太网帧“长度/类型”字段的值来标识,使用大于 0x0600 的类型值 0x8808。MAC control 帧的数据字段长度为以太网数据字段的最小长度 46 字节,它的前 2 个字节是操作码 opcode,PAUSE 命令的 opcode 为 0x0001。除了 opcode 外,还有 2 个字节表示请求链路对方暂停发送数据的时间长度,以 512 位时为单位,长度范围为 0~65536 个单位。

PAUSE 帧的目的地址统一使用保留的组播地址 0x0180C2000001,发送方无须知道对方的 MAC 地址,而且标准的交换机都能识别这个地址,不把它转发到其他端口。

是否使用流量控制以及流量控制的方式可以通过自动协商进行配置。

6-38 什么是 VLAN?

解答:VLAN 不是一个新型的网络,是局域网给用户提供服务的一种服务。VLAN 建立在交换式网络的基础之上,主要的交换设备是以太网交换机,在像交换式以太网这样的支

持 VLAN 的网络上,使用 VLAN 技术将网络从逻辑上划分出一个个与地理位置无关的子集,每个子集就可构成一个 VLAN。在 VLAN 中,一个站点的广播帧只能发送到具有相同 VLAN 标识的其他站点,不管它们在什么物理位置,就好像在一个 LAN 中一样。

因此,VLAN 是由一些局域网网段构成的与物理连接和地理位置无关的逻辑工作组,相当于一个广播域。

6-39 描述 IEEE802 标准中定义的 VLAN 帧格式,它将以太网帧格式作了什么变动?

解答: VLAN 开始是在 IEEE802 .1Q 标准中定义的,但定义中要求发送帧中携带 VLAN 信息,影响到帧的长度,为此又有了 IEEE802 .3ac 文档,它和 IEEE802 .1Q 相关。

IEEE802 .1Q 和 IEEE802 .3ac 定义的以太网帧中需携带一个 VLAN 标记(Tag),它是一个 4 字节的域,插入到原始以太网帧的源地址域和长度/类型域之间。是一个“插入性”的标记,插入或去掉时必须重新计算 CRC 校验值,而且插入后帧长度也应加上 4。

为了容纳这一标记,IEEE802 .3 以太网帧长度也作了相应修改。最大帧长由 1 518 字节扩大到 1 522 字节,最小帧长 64 字节不变,但 1 522 字节只适用于 VLAN。

VLAN 插入性的 4 个字节标记分为两个字段:

TPID (tag protocol identifier) 标记协议标识符,2 个字节,是一个全局赋予的 VLAN 以太网类型,其值为 0x8100。

TCI (tag control information) 标记控制信息,2 字节。它分为 3 个字段。3 比特的用户优先级 0~7 级,0 级最高,允许以太网支持服务级别的概念。1 比特的规范格式指示器 CFI,以太网不使用这一位,置为 0;当置 1 时表示以太网帧封装令牌环帧。其余 12 比特作为 VLAN 的标识,与某个 VLAN 关联。

6-40 图 1-6-3 表示了基于端口的 VLAN 的划分,划分了 3 个 VLAN: VLAN1、VLAN2 和 VLAN3,分别包含 6、6 和 2 台计算机。结合图 1-6-3 说明计算机 2-1 向广播地址发送的广播帧的传送过程。

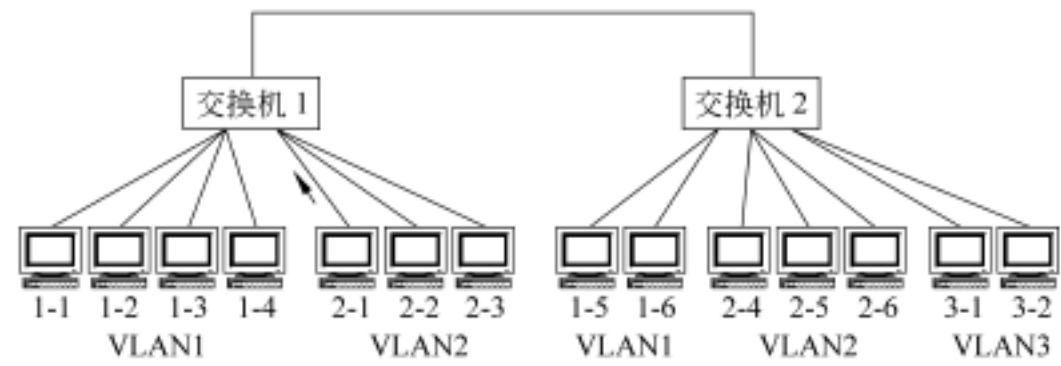


图 1-6-3 基于端口的 VLAN 的划分

解答: 计算机 2-1 广播帧的传送过程如图 1-6-4 所示。
交换机 1 收到计算机 2-1 的广播帧后,根据交换机 1 中维护的 VLAN 和端口的关联信息,它会转发到连接计算机 2-2 和 2-3 端口。

连接两个交换机的“标记端口”属于所有 VLAN 的成员。因此交换机 1 也通过连接

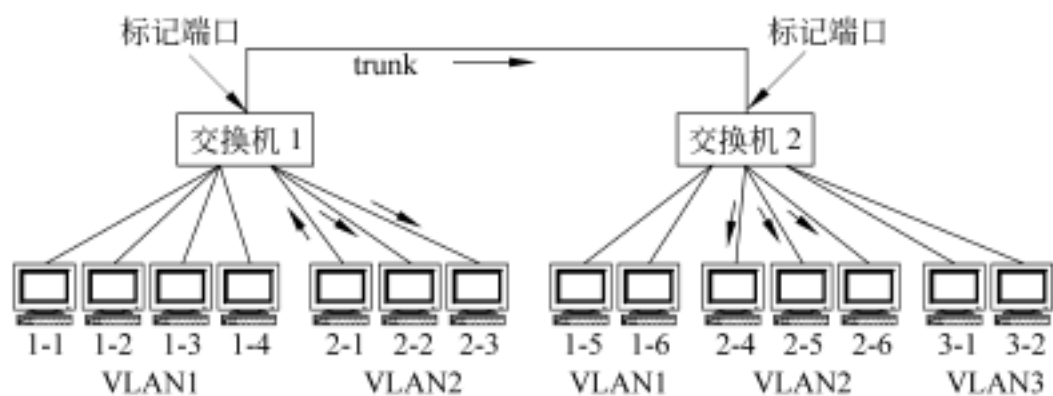


图 1-6-4 计算机 2-1 广播帧传送的过程

两个交换机的链路 trunk 向交换机 2 的端口转发计算机 2-1 的广播帧。但当广播帧向标记端口转发时,它将被打上标记,注明它属于 VLAN2。当交换机 2 接收到这一打了 VLAN2 标记的广播帧后,它将去掉标记并根据标记的信息和本交换机中维护的 VLAN 和端口的关联信息,转发到所有连接了 VLAN2 成员的端口,这样,广播帧又发送到计算机 2-4、2-5 和 2-6。

6-41 下列哪些对于 CSMA/ CD 的描述是正确的？

- A . 是局域网的一种介质访问方法
- B . 是在 FDDI 网络中使用的介质访问方法
- C . 一个站点要传输数据时,它首先检查介质是否可用
- D . 一个站点要传输数据时,不检查介质是否可用,因为每个站点由平等的访问权限
- E . 在同一时刻只有一个站点能成功发送数据

答案：A, C, E

6-42 载波监听多路访问 CSMA 控制策略中有三种坚持算法,其中一种是:一旦介质空闲就发送数据,假如介质是忙的,继续监听,直到介质空闲后立即发送数据。这种控制算法称为__(1)__算法。这种算法的主要特点是__(2)__。CSMA/ CD 在 CSMA 的基础上增加了冲突检测功能。网络中的某个发送站点一旦检测到冲突,它就立即__(3)__。如果站点发送时间为 1,任意两个站之间的传播延迟为 t ,若能正常检测到冲突,对于基带总线网络, t 的值应为__(4)__。

- | | | | |
|------------------------|---------------------|-------------|-------------------|
| (1) A . 1-坚持 CSMA | B . 非坚持 CSMA | | |
| C . p -坚持 CSMA | D . ρ -坚持 CSMA | | |
| (2) A . 介质利用率低,但可以避免冲突 | B . 介质利用率高,但无法避免冲突 | | |
| C . 介质利用率低,且无法避免冲突 | D . 介质利用率高,且可以避免冲突 | | |
| (3) A . 停止发送 | B . 停止发送并重新竞争发送权 | | |
| C . 停止发送并发送阻塞信号 | D . 继续发送数据 | | |
| (4) A . $t \leq 0.5$ | B . $t > 0.5$ | C . $t = 1$ | D . $0.5 < t < 1$ |

答案：A, B, C, A

6-43 以太网中,当数据传输率提高时,帧的发送时间要按比例缩短,这样有可能会

影响冲突的检测。为了能有效地检测冲突,可以__ (1) __ 或者 __ (2) __。快速以太网仍然遵循 CSMA/ CD, 它采取 __ (3) __ 而将最大电缆长度减少到 100m 的方式, 使以太网的数据传输率提到 100Mb/ s。为了支持不同的传输介质, 快速以太网提供了 4 种技术标准, 即: 100BaseTX、100BaseT4、100BaseT2 和 100BaseFX, 其中 100BaseT4 使用 __ (4) __, 100BaseTX 使用 __ (5) __。

- (1) A . 减小电缆介质的长度 B . 增加电缆介质的长度
C . 降低电缆介质损耗 D . 提高电缆介质的导电率

(2) A . 减小最短帧长 B . 增大最短帧长
C . 减小最大帧长 D . 增大最大帧长

(3) A . 改变最短帧长 B . 改变最大帧长
C . 保持最短帧长不变 D . 保持最大帧长不变

(4) A . 4 对, 3 类线 B . 2 对, 3 类线 C . 4 对, 5 类线 D . 2 对, 5 类线

(5) A . 4 对, 3 类线 B . 2 对, 3 类线 C . 4 对, 5 类线 D . 2 对, 5 类线

答案: A, B, C, A, D

6-44 在局域网总线/树拓扑的多点介质传输系统中,要使多个站点共享单个数据通道,需要特别考虑解决(1)的问题。采用 50 同轴电缆作为传输介质并构成总线拓扑的网络系统,可使用基带技术传输数字信号,总线上(2),总线两端加上终端匹配器用以(3)。

- (1) A . 数据帧格式
C . 通信协议类型
 - (2) A . 整个带宽由单个信号占用
C . 可传输视频或音频信号
 - (3) A . 防止信号衰减
C . 降低介质损耗
- B . 介质访问控制方法
D . 信道分配方案
 - B . 整个带宽被分成多路数据信道
D . 数据只能单向传输
 - B . 增强抗干扰能力
D . 阻止信号反射

答案：B, A, D

6-45 下列哪些设备扩展了冲突域 (1) ? 哪些设备用于分割冲突域 (2) ?

- A . 中继器 B . 路由器 C . 交换机 D . 集线器
- E . 网桥

答案: (1) A, D (2) B, C, E

6-46 透明网桥从其某一端口收到正确的数据帧后,在其地址转发表中查找该帧要到达的目的站,若查找不到,则会__(1)___。图 1-6-5 为两个局域网 LAN1 和 LAN2 通过网桥 1 和网桥 2 互连后形成的网络结构。设站 A 发送一个帧,但其目的地址均不在这两个网桥的地址转发表中,这样结果会使该帧__(2)___。为了有效地解决该类问题,可以在每个网桥中引入生成树算法,这样一来__(3)___。

- (1) A . 向除该端口以外的桥的所有端口转发此帧
B . 向桥的所有端口转发此帧
C . 仅向该端口转发此帧
D . 不转发此帧, 而由桥保存起来

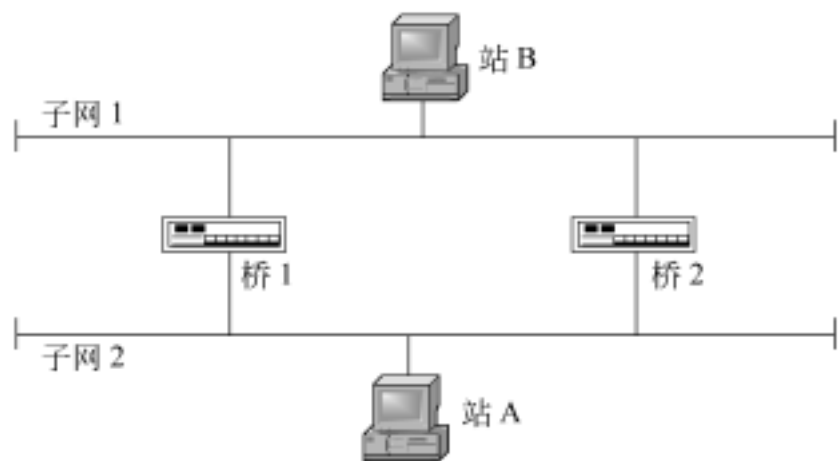


图 1-6-5 LAN1 和 LAN2 互连的网络

- (2) A . 经桥 1(或桥 2)后被 B 站接收
B . 被桥 1(或桥 2) 丢弃
C . 在整个网络中无限次地循环下去
D . 经桥 1(或桥 2) 到达 LAN2,再经桥 2 (或桥 1)返回 LAN1 后被站 A 吸收
- (3) A . 网络资源也会得到充分利用
B . 网络的最佳路由也会得到确定
C . 也限制了网络规模
D . 也增加了网络延时

答案: A, C, D

6-47 图 1-6-6(a)为一 10Mb/ s 数据传输率的以太网,其上连接有 10 个站,在理想状态下每个站的平均数据传输率为 1Mb/ s。若通过网桥连接后成为图 1-6-6(b)所示的结构时,每个站的实际的平均数据传输率为_____ Mb/ s。

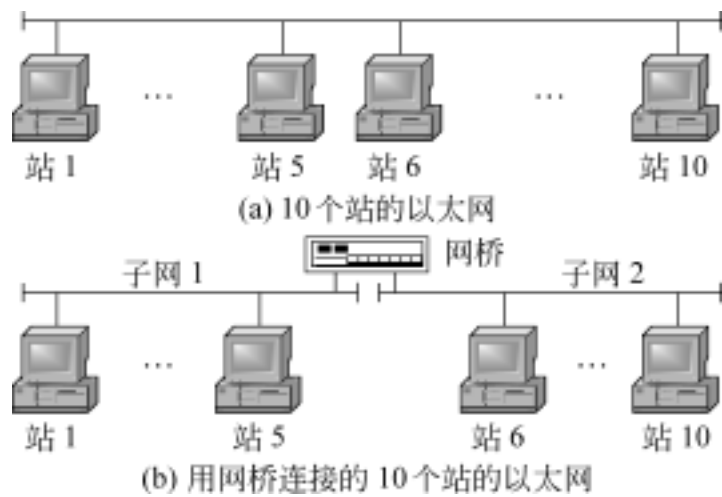


图 1-6-6 以太网与用网桥连接的以太网

- A . 0 至 1 B . 1 C . 2 D . 1 至 2

答案: D

6-48 图 1-6-7 中哪些设备必须拥有 MAC 地址 ?

- A . 只有 PC B . 只有路由器 C . PC 和路由器
D . PC, hub 和路由器 E . PC, 打印机和路由器

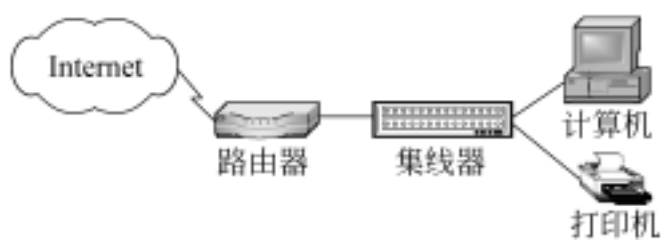


图 1-6-7 6-48 题图

答案：E

6-49 图 1-6-8 中共有多少冲突域？

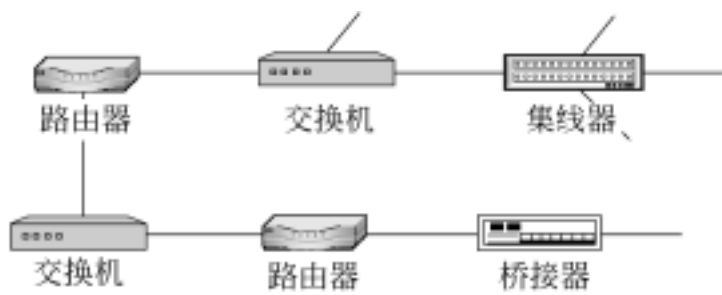


图 1-6-8 6-49 题图

- A . 3
- B . 4
- C . 5
- D . 6
- E . 7
- F . 8

答案：E

6-50 两台主机 A 和主机 B 需要建立以太网的连接。但是 2 个站点之间的距离超过了规定的线缆的最大长度。如下哪些设备是在 OSI 的物理层将 2 台主机互连起来的设备？

- A . hub
- B . 路由器
- C . 网桥
- D . 中继器
- E . 交换机

答案：A，D

6-51 下述用于 10Base-T 的线缆标准中,哪个描述是正确的？

- A . 10Mb/ s 传输速率，基带信号，500m 线缆长度，同轴电缆
- B . 10Mb/ s 传输速率，宽带信号，100m 线缆长度，同轴电缆
- C . 10Mb/ s 传输速率，基带信号，100m 线缆长度，非屏蔽双绞线
- D . 10Gb/ s 传输速率，宽带信号，500m 线缆长度，非屏蔽双绞线

答案：C

6-52 某单位的网络为总线 LAN,总线长度为 1 000m,数据率为 10Mb/ s,信号在总线上的传播速度为 2×10^8 (c为光速),则每个比特信号占据的介质长度为__(1)__米。当采用 CSMA/ CD 访问方式时,如只考虑信号在总线上的传播时延而忽略其他因素,则最小时槽长度应为__(2)__μs,最小帧长度应是__(3)__位。

- (1) A . 10
- B . 20
- C . 100
- D . 200
- (2) A . 1
- B . 1.5
- C . 3
- D . 10
- (3) A . 100
- B . 512
- C . 10 000
- D . 12 144

答案：B，D，A

6-53 在以太网的 10Base5 标准中,粗同轴电缆的特性阻抗为__(1)__,物理层采用__(2)__编码;100BaseTX 采用的是__(3)__物理拓扑结构,传输介质通常采用__(4)__类双绞线;传输介质段最大距离是__(5)__ m。100BaseFX 采用的传输介质是__(6)__。

- | | | | |
|----------------|------------|----------------|-------------------|
| (1) A . 50 | B . 75 | C . 100 | D . 150 |
| (2) A . 4B/ 5B | B . 8B/ 6T | C . Manchester | D . 差分 Manchester |
| (3) A . 环型 | B . 星型 | C . 总线型 | D . 网状 |
| (4) A . 3 | B . 4 | C . 5 | D . 8 |
| (5) A . 100 | B . 185 | C . 400 | D . 500 |
| (6) A . 屏蔽双绞线 | B . 光纤 | C . 非屏蔽双绞线 | D . 同轴电缆 |

答案: A, C, B, C, A, B

第 7 章

非主流局域网

7-1 简述令牌环的拓扑结构和媒体接入控制的方式,简述令牌环进行信息传输的过程。

解答:令牌环物理上是环型拓扑结构,所有结点逐个邻接形成的一个首尾相连的闭合环路。环路由许多称为环接口的网络设备相连,而工作站接到环接口上。

令牌环使用基于令牌的分散控制方式的受控媒体接入技术,只有获得令牌的站点才有权在环路上发送数据,因而避免了信道访问的冲突。

令牌环进行信息传输的过程大致如下:令牌持有者发送出信息,信息帧单方向地沿环路进行传输,每个结点从它的前连结点接收信息并向后连的结点传递。结点对帧的地址有识别能力,当地址与本站地址符合时,将帧接收入本站并继续向前传送;不符则只是继续传送,直至返回到发送站,帧绕环路一周后由发送站清除。这种传输方式使得目的站可以向发送站反馈确认信息,还可以实现多播和广播。另外,令牌重新插入环路也是由发送站负责。

7-2 环接口的工作方式是什么?环接口中继输入比特流时造成多大的传输延时?

解答:环接口在令牌环网中有两种工作方式:发送方式和收听方式。

当环接口工作于发送方式时,数据以帧为单位由环接口的输出端发送到后连站点环接口的输入端。

当环接口处于收听方式时,其主要任务是:

中继由环接口输入端输入的比特流。接收 1 个比特到 1 比特缓冲区,经整形、放大后由输出端重新送到环上,这里只造成 1 比特延迟。此时,环接口和所连接的工作站实际上处于断开状态。

监听通过的比特流的组合模式,主要是监听两种比特流组合:本站的地址和令牌并做相应处理。环接口一旦监听到有本站的地址,则将环路输入的比特流转送到与它相连的工作站。同时,环接口仍然执行上述中继功能,将输入的比特流也输出给下一个站点。环接口若监听到令牌,若此时本站有数据发送,将截获令牌,将空令牌中的空令牌标志改为忙令牌标志,然后将目的地址、源地址和欲发送的数据附在截获的令牌后面,组成信息帧,并把环接口置为发送方式,把帧发送出去;若此时本站无数据发送,则把空令牌继续向下传递。

7-3 假设环的周长为 2 000m,共连接了 30 站点,那么速率为 4Mb/s 的令牌环,环路上能容纳多少比特?

解答: 环路的比特长度 = $4\text{Mb/s} \times (2\,000\text{m} \div 200\text{m}/\mu\text{s}) + 30\text{b} = 70(\text{b})$, 即环路上能容纳 70 比特。

7-4 简述 IEEE802.5 令牌环的优先级控制策略。

解答: IEEE802.5 采用了 AC 字段中的 PPP 优先级比特与 RRR 预约比特配合工作的方式来实现环网中优先级控制。在 AC 字段中, 优先级为 3 个比特, 可以提供 0~7 共 8 个优先级, 0 级最低。优先级是由发送该信息的工作站根据信息对实时性的要求自行规定的。

若某站点有待发信息, 可以在转发信息帧时通过把待发信息的优先级写入转发帧的 RRR 中进行预约, 当待发信息的优先级大于 RRR 中原来已经预约的值时, 可取而代之。当下一个令牌发出时, 它的优先级 PPP 被置为预约的优先级。各站环接口监听令牌, 若此时某站有待发信息且优先级大于等于 PPP, 则可以获得令牌发送信息。

7-5 IEEE802.5 采用什么方法进行令牌的维护?

解答: IEEE802.5 使用一个监控站进行令牌维护。为了检测令牌丢失, 监控站使用一个有效帧定时器, 设定的定时时限大于信息通过整个环网的时间。任何一个有效令牌或信息帧经过它后, 定时器重新启动, 如果定时器超时, 监控站发出一个 0 优先级的令牌。为了检测一个永久忙令牌(指令牌标志 T 置“1”的信息帧在环网上循环而没有工作站对它进行清除), 监控站在任何帧首次经过它时, 都将监视比特由 0 置为 1。若它发现任何监视比特为 1 的帧经过它, 则吸收此帧并发出一个 0 优先级的令牌。

7-6 简述 IEEE802.4 令牌总线的结构特点。

解答: 令牌总线的结构特点是: 物理上是总线结构, 逻辑上是令牌环。

令牌总线的工作站点以总线形式进行物理连接, 但使用令牌进行总线接入控制, 总线上的站点只有得到令牌帧, 才能传输信息。逻辑环是一种逻辑上的连接关系, 它由进行信息发送的站点组成, 不参与任何信息传输的站点虽然在网上也可以不加入逻辑环。逻辑上各站点并不按站点物理连接的顺序排序而是按站点地址编码值递减的顺序排序。

7-7 简述 FDDI 的主要特点。

解答: FDDI 是一种物理层和数据链路层标准, 规定了基于令牌控制的双环网络技术, 使用光纤达到 100Mb/s 的传输速率。FDDI 的主要特点如下:

使用基于 IEEE802.5 令牌环标准的令牌传递 MAC 协议, 帧格式也类似 IEEE802.5;

使用 802.2 LLC 协议, 与 IEEE802 局域网兼容;

使用双环拓扑, 具有容错能力;

主要使用多模或单模光纤, 还可使用双绞线;

信息传输速率为 100Mb/s , 使用 4B/5B-NRZI 编码, 光信号码元传输波特率为 125Mbaud;

最大结点数 500; 站间最大距离 2km(多模光纤)或 60~100km(单模光纤);

最大帧长度 4 500 字节。

7-8 FDDI 的令牌重插策略是什么? 为什么采用这种策略?

解答: FDDI 的令牌重插策略是: 发送站发完数据帧后就紧接着发出一个新令牌。这

样,在某个站的数据帧在环内循环过程中,环中其他有待发数据的站也可以获得令牌进行数据发送,因此令牌重插后环路上可以同时存在一个以上的数据帧,这就提高了信道的利用率。

采用这种策略是和 FDDI 有 100Mb/s 的高信息传输速率和长环路距离相适应的。举例来说,假如在 60km 长的环路上,环路的比特长度可达 30 000 比特(忽略中间结点的延迟),如果发送 1 000 字节长度的帧,环路上可容纳 3 个帧。

7-9 信息传输速率 100Mb/s 的 FDDI, 1 000 字节的帧在 50km 的环上传输,它占用多少公里的网络长度? 帧从发出到完全收回需要多长时间?(忽略中间结点延时)

解答: 帧发送时间 $T_1: (8b \times 1\,000) \div 100Mb/s = 80\mu s$;
帧占的网络长度 = T_1 时间的传播距离 = $200m/\mu s \times 80\mu s = 16km$;
帧在 50km 环上的传播时间 $T_2 = 50km \div 200m/\mu s = 250\mu s$;
帧从发出到完全收回需要的时间 = $T_1 + T_2 = 80\mu s + 250\mu s = 330\mu s$ 。

7-10 简述几种典型的 FDDI 网络拓扑结构。

解答: 将双连接站串接在一起就构成了 FDDI 网络最基本的双环拓扑结构。使用集中器又可构造树型拓扑,它们相结合又形成双环树拓扑结构。下面是几种典型的 FDDI 网络的拓扑结构。

独立集中器星型 由一个集中器连接多台工作站。这种拓扑可用于连接若干台设备组成一个工作组。

集中器树 如果连接大量的用户设备可以采用这种结构。多台集中器可连于不同层次,其中一台作为树根。集中器上连接工作站,构成一个集中器树的拓扑结构。

双环树 这是最具代表性的 FDDI 网络结构,服务器之类的重要设备作为双连接站连入双环,双环中连有双连接集中器 DAC,由 DAC 再下连单连接集中器 SAC 和单连接站 SAS,这样构成双环树结构。

7-11 IEEE802.5 令牌环网中,时延是由__(1)__决定。要保证环网的正常运行,环的时延必须有一个最低限度,即__(2)__。如果达不到这个要求,可以采用的一种办法是通过增加电缆长度,人为地增加时延来解决。

设有某一个令牌环网长度为 300m,环上有 28 个站点,其数据传输率为 4Mb/s,环上信号的传播速度为 200m/ μs ,每个站点具有 1 比特时延,则环上可能存在的最小和最大时延分别是__(3)__比特和__(4)__比特。当始终有一半站点打开工作时,要保证环网的正常运行,至少还要将电缆的长度增加__(5)__m。

- | | | | |
|---------------------|------------------|------------|----------|
| (1) A . 站点时延和信号传播时延 | B . 令牌帧长短和数据帧长短 | | |
| C . 电缆长度和站点个数 | D . 数据传输率和信号传播速度 | | |
| (2) A . 数据帧长 | B . 令牌帧长 | C . 信号传播时延 | D . 站点个数 |
| (3) A . 1 | B . 6 | C . 20 | D . 24 |
| (4) A . 9 | B . 28 | C . 34 | D . 48 |
| (5) A . 50 | B . 100 | C . 200 | D . 400 |

答案: A, B, B, C, C

7-12 FDDI 采用了__(1)__块编码以获得足够多的同步信息,编码效率为__(2)__。

(1) A . 4B/ 5B B . 5B/ 6B C . 8B6T D . 8B/ 10B

(2) A . 25 % B . 50 % C . 80 % D . 100 %

答案: A, C

7-13 FDDI 协议是由__(1)__协议改进而来的。FDDI 为了更快地传送数据,__(2)__产生令牌,因此在一个环上__(3)__。FDDI 使用双环结构可以提高网络的__(4)__。

(1) A . IEEE802 .3 B . IEEE802 .4 C . IEEE802 .5 D . IEEE802 .6

(2) A . 站点在收到自己发出的数据帧时

B . 站点可随时

C . 站点在发送数据帧前

D . 站点在发送完数据帧时

(3) A . 可以同时存在多个帧

B . 最多存在一个帧

C . 不允许同时存在多个帧

D . 允许同时存在多个令牌

(4) A . 可靠性

B . 数据速率

C . 编码效率

D . 优先级

答案: C, D, A, A

第 8 章

无线局域网 (WLAN)

8-1 说明 IEEE802 .11 WLAN 的网络结构, 涉及关键词: 基本服务集(BSS)、接入点(AP)、分布系统(DS)、扩展服务集(ESS)和自组网络。

解答: IEEE802 .11 WLAN 的最小组件称为基本服务集(BSS), 是一个有限的区域。一个 BSS 包括一个基站和若干个移动站, 它们共享 BSS 内的无线传输媒体, 使用 IEEE802 .11 WLAN 媒体接入控制 MAC 协议通信。基站也称接入点(AP)。

一个 BSS 可以是独立的, 也可以通过 AP 连接到一个分布系统 DS, AP 的作用类似于网桥。分布系统 DS 是一个有线或无线的主干 LAN, 最常用 802 .3 以太网。这样, BSS 中的移动站点就可以访问 DS 连接的主机。

多个 BSS 通过 DS 连接就构成了扩展服务集(ESS)。ESS 还可为无线用户提供到 Internet 的访问, 这种访问是通过称为门桥的设备实现的。

IEEE802 .11 还支持另一种结构的 WLAN, 称为自组网络(ad hoc network), 它在一些对等的移动笔记本电脑之间通信, 没有接入点。

8-2 画图说明 IEEE802 .11 WLAN 中移动站通过 AP 接入以太网 DS 的通信协议结构。

解答: 如果 DS 是一个 802 .3 以太网, 移动站通过 AP 与以太网上的计算机通信的协议结构如图 1-8-1 所示。BSS 中的移动站点使用 802 .11 物理层和 MAC 子层, 802 .3 以太网上的主机使用 802 .3 物理层和 MAC 子层, 接入点 AP 像一个网桥, 支持这两种类型的物理层和 MAC 子层, 在它们之间中继 LLC 帧。

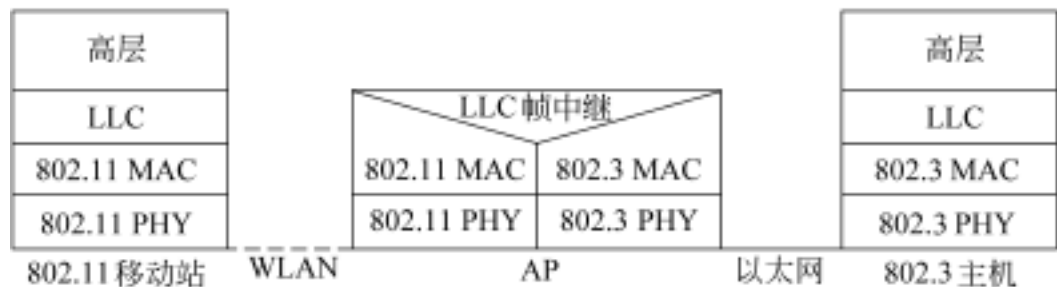


图 1-8-1 移动站通过 AP 与以太网 DS 通信的协议结构

8-3 IEEE802 .11 WLAN MAC 层定义了哪两个子层? 它们向上提供什么样的服务?

解答: MAC 层定义了分布协调功能(DCF)和点协调功能(PCF)两个子层。

DCF 在每个结点使用载波监听多路接入 CSMA 的媒体接入控制机制, 使各个结点

通过竞争得到发送权。WLAN 使用的是一种改进的带冲突避免的 CSMA 协议,即 CSMA/CA 协议。DCF 是一种基本的接入方法,所有的移动站点都要求支持 DCF,自组网络站点只使用 DCF。DCF 向上提供争用服务。

PCF 位于 DCF 之上。PCF 使用集中控制式的媒体接入方式,用类似轮询的方法使各个结点得到发送权,在 AP 实现集中控制。PCF 向上提供无争用服务,可用于对时间敏感的业务,如话音等多媒体传输。

8-4 IEEE802.11 CSMA/CA 定义了哪 3 种帧间间隔 IFS? IFS 的作用是什么?

解答: IEEE802.11 定义了 3 种帧间间隔 IFS:

SIFS 短帧间间隔(short IFS),是 3 种 IFS 中最短的,确认帧 ACK、CTS 帧和长的 MAC 帧分片后的数据帧等使用 SIFS。

PIFS 点协调功能帧间间隔(PCF IFS),PCF 轮询时使用。在 SIFS 的基础上加上一个时隙长度。

DIFS 分布调功能帧间间隔(DCF IFS),在 DCF 方式中使用,在 PIFS 的基础上加上一个时隙长度,是最长的 IFS。发送数据帧一般使用 DIFS。

不同的 IFS 可以产生不同的发送优先级,协调 MAC 层 DCF 和 PCF 的不同操作,减少发送冲突。欲发送的站点先监听信道,如果信道空闲,它就继续监听一个 IFS 时间段,若信道仍然空闲,站点就可以进行发送。监听到信道空闲后再继续监听一个 IFS 时间,这样不同的 IFS 将帧划分为不同的优先级,IFS 越小帧的优先级就越高。若同时监听到信道空闲,小的 IFS 就先占用信道得到发送权,大的 IFS 随后监听到信道忙只得推迟发送。这样,不同 IFS 的帧就不会产生发送冲突。

8-5 叙述 IEEE802.11 CSMA/CA 的回退算法。

解答: 使用 CSMA/CA 欲发送数据的站点先监听信道。如果信道空闲,它就继续监听一个 DIFS,若信道仍然空闲,站点就可以把第一个数据帧发送出去。如果信道忙,不管是开始监听时信道忙还是继续监听的 DIFS 时间段内信道忙,站点将为下次重试计算一个随机回退时间,设置回退定时器,并继续监听直至信道空闲。

当信道由忙变空闲后,继续监听一个 DIFS,若信道仍然空闲,进入争用窗口,执行回退算法。回退定时器开始倒计时,如果回退定时器减到 0 时信道仍然空闲,站点就占用信道得到发送权。竞争的结果是,多个欲发送数据的站点中回退时间短的站点将争得信道并发送数据。其他回退时间长的站点听到信道变忙后将暂停回退定时器,监听信道到再次空闲,并继续监听一个 DIFS,启动回退定时器继续倒计时,重新争用信道。此时,其回退定时器在剩余的回退时间基础上回退,这有利于各发送站点公平地争用信道。

信道争用中,如果多个站点回退定时器同时减到 0,会发生发送冲突,它们要调整回退时间,进行重试。另外,如果一个站点发送完第一个数据帧,后面还要发送,则后面的发送都必须进入争用窗口,执行回退算法。只有站点发送第一个数据帧且监听信道为空闲时,才不执行回退算法。

随机回退时间的计算采用和 IEEE802.3 类似的二进制指数算法,站点回退时间随重试次数的增加呈指数增长。其算法是:第 i 次回退时,在 2^{i+2} 个时隙中随机选取一个回退时间。例如第 2 次回退时,要在 0~15 个时隙中随机选取。

8-6 叙述网络分配向量(NAV)及其作用。

解答：在 IEEE802 .11 MAC 层,网络分配向量(NAV)提供了一种虚拟载波监听的机制。数据帧及 RTS、CTS 帧的第二个字段为持续时间字段,利用它发送站显式地告诉其他站本次传输(从开始到 ACK 结束)在媒体中的持续时间,其他站检测到这个字段就调整其 NAV,它们的信道接入要延迟这样长的时间。因此,除使用物理载波监听方式外,NAV 又提供了一种虚拟载波监听方式。在 CSMA/ CA 信道监听中,站点将同时利用虚拟载波监听和物理载波监听信号。如果虚拟载波监听发现 NAV 信号存在,会继续监听直到 NAV 信号消失,然后 MAC 层就会监听信道的物理信号。

8-7 画图说明什么是隐蔽站点问题,它的影响是什么？

解答：在无线局域网中,由于传输信号强度随距离增长而快速衰减或移动站点之间可能有传输屏障等因素,超出接收范围或被物体屏蔽的站点接收不到信号,这导致了隐蔽站点问题。

图 1-8-2 说明隐蔽站点问题。图 1-8-2(a)中,假设无线电信号的传输范围因衰减只能到达邻站。A 站先向 B 站发送数据。由于 C 站收不到 A 站的信号,误认为网上无人发送数据,因此 C 站也向 B 站发送数据,B 站同时收到 A 站和 C 站的数据,因而发生了冲突。这种冲突也可以发生在另一种情况:虽然 A、B 和 C 三个站都在信号的有效传输距离之内,但在 A 和 C 之间有一个信号屏蔽物体,如图 1-8-2(b)所示。因此,A 或 C 在发送前可能检测不到媒体上已存在的信号,因而发生冲突。这就是隐蔽站点问题,A 和 C 相互隐蔽。

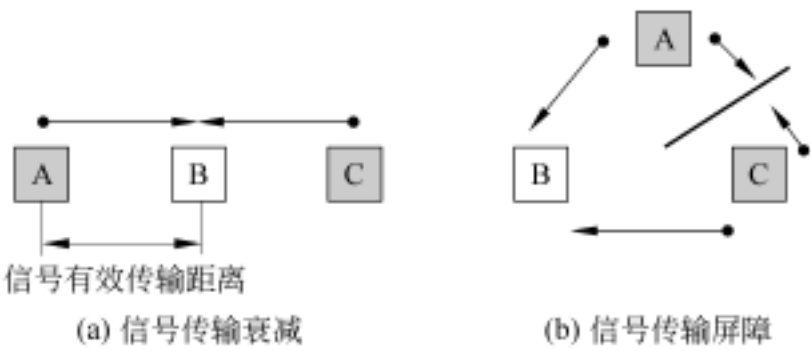


图 1-8-2 WLAN 的隐蔽站点问题

因为 WLAN 中存在隐蔽站点问题,CSMA 只能告诉站点在它的信号有效传输范围之内是否有传送活动存在。如果两个隐蔽的站点同时发送数据,CSMA 发送前监听不到对方的信号,但发送后会在其他站点产生冲突,两个同时发送数据的隐蔽站点也都无法检测到发送冲突,冲突检测失去效果。另外,对于无线射频信号,进行冲突检测(边发送边接收)也非常难实现。因而 WLAN 不采用 CSMA/ CD。

8-8 IEEE802 .11 定义了无线局域网的两种工作模式,其中的__ (1) __模式是一种点对点连接的网络,不需要无线接入点和有线网络的支持,用无线网卡连接的设备之间可以直接通信。IEEE802 .11 的物理层规定了三种传输技术,即红外技术、直接序列扩频(DSSS)和跳频扩频(FHSS)技术,后两种扩频技术都工作在__ (2) __的 ISM 频段。IEEE802 .11 MAC 层具有多种功能,其中分布式协调功能采用的是__ (3) __协议,用于支持突发式通信,而用于支持对时间敏感的多媒体应用的是__ (4) __功能,在这种工作方式

下,接入点逐个询问客户端,被查询到的客户端通过接入点收发数据。后来提出的 IEEE802 .11a 标准可提供的最高数据速率为__ (5) __。

- | | | | |
|------------------|--------------|--------------------|---------------|
| (1) A . Roaming | B . ad hoc | C . Infrastructure | D . DiffuseIR |
| (2) A . 600MHz | B . 800MHz | C . 2 .4GHz | D . 19 .2GHz |
| (3) A . CSMA/ CA | B . CSMA/ CB | C . CSMA/ CD | D . CSMA/ CF |
| (4) A . BCF | B . DCF | C . PCF | D . QCF |
| (5) A . 1Mb/ s | B . 2Mb/ s | C . 5 .5Mb/ s | D . 54Mb/ s |

答案: B, C, A , C, D

第 9 章

广域网传输控制机制

9-1 分组交换和报文交换相比,把传送的数据单位从报文变成长度较小的分组,这带来什么好处?

解答:分组交换和报文交换相比,把传送的数据单位从报文变成若干个长度较小的分组,带来了如下优势:首先,由于分组长度小,因此在转接过程中就可以缓存于转发计算机的内存中,而无须像报文交换那样存于外存储设备,大大提高了存储转发的速度。其次,发送站发出第一个分组后,即可再发第二个、第三个、……分组,并不需要等待前面的分组到达目的站,这些分组在各个转发结点同时被存储转发,被并行处理,降低了整体的传输时间。另外,对于传输中的错误,只需重发出错的分组,而不必重发整个报文,因此也提高了差错控制的效率。

9-2 数据报和虚电路分组交换各有什么特点?它们提供什么样的网络服务?

解答:数据报分组交换方式不需要建立连接,每个分组的传输都是独立寻径。分组的传输可能经过不同路径,因此不能保证分组按顺序到达目的站。分组在发送时必须标上表示顺序的标志,以便在目的结点重组。数据报分组交换方式分组的路由选择方法复杂,分组传输延时较大。

虚电路分组交换方式首先要建立一个连接,然后使用这一固定的路径进行分组传输,传输完成便释放这一连接。虚电路建立连接的过程并不是进行了一次实际的物理线路的连接,而是在现有的网络中指定了一条传输通道,而且这一连接也不是专用的,其上的结点和通路还可以为转发其他的传输服务。虚电路方式中所有的分组都走同一条路径,因而不会出现分组乱序的情况。虚电路分组交换附加了建立和释放连接的开销,适合于两个站之间传输的分组较多的情况。

虚电路分组交换方式提供面向连接的网络服务,数据报分组交换方式提供无连接的网络服务,应该说,面向连接的虚电路分组交换方式比无连接的数据报分组交换方式能提供更好的服务质量(QoS),但这是以额外的连接开销为代价的。数据报分组交换方式在传输分组数较少的信息时更简便高效。

9-3 叙述广域网的分组转发机制。什么是源站无关性?

解答:广域网中交换机分组转发是基于路由表的下一跳转发机制。每一个结点交换机中都有一个路由表,路由表中最重要的两项内容是分组发往的目的站以及分组路径上的下一跳(next hop)。如果目的站是直接连接同一个交换机上的其他主机,则不需要别的交换机转发,因此表中的下一跳注明的是本交换机。交换机以转发分组的目的站的地

址为索引,查询路由表,得到转发路径上的下一跳,将报文转发出去。

路由表中没有源站地址,这是因为路由选择中的下一跳只取决于分组的目的站地址,而与源站地址无关,这称为源站无关性。

9-4 什么是静态路由和动态路由?最优路径可以有哪些度量指标?

解答:静态路由/动态路由指用静态/动态的方式构造路由表。交换机启动时设置路由,此后不再改变,若网络发生变化,必须由人工更新,称为静态路由(static routing)。交换机启动时设置初始路由,然后相邻交换机之间不断交换路由信息,运行路由算法,使路由随时自动更新,称为动态路由(dynamic routing)。动态路由比静态路由有更好的转发性能,能适应网络拓扑和负载的变化,其代价是交换机更大的处理开销。

最优路径指路径的某种度量指标最优,可以有不同的度量指标:

跳数 指路径所经过的交换机数目;

时延 指分组由源站到达目的站所花费的时间;

费用 借助电信等部门的通信线路需交纳费用;

可靠性 指链路的误码率。

度量指标在通用算法研究中常常统称为“距离”。度量指标可以用数字来表示。

9-5 拥塞如何产生?什么是拥塞崩溃和死锁?

解答:拥塞是分组交换网络共同的问题,主要是分组转发结点超载引起。在分组交换网中,交换结点用存储转发的方式转发分组。试想,若出现大量的分组从几个输入链路同时涌入同一交换结点而又由同一个链路输出,交换结点来不及处理,该链路输出队列的增长速度高于帧输出的速度,分组将会在交换结点的这个输出缓冲队列中排队等候,使传输时延增大,出现拥塞现象。严重的情况下,交换结点的缓冲队列溢出,必须丢弃分组。对于带有差错控制的可靠传输,丢弃分组会引起发送方的超时重发,这又增加了网上的分组数量,使拥塞更加严重。

当网络负载增大到一定程度,此时随着网络负载的增加,吞吐量不但不增加反而下降,传输时延急剧增加,说明网络已经出现了严重拥塞现象。最终,吐量趋于零,称为拥塞崩溃。当吞吐量降为零,网络完全失去传输能力,称为死锁。

9-6 简单描述拥塞控制的闭环控制策略。

解答:闭环控制也称反馈控制,它包括两个环节:反馈机制和控制机制。反馈机制把当前网络的状态,如有无拥塞及拥塞程度等通知发送结点。交换结点负责监视和反馈拥塞信息,拥塞程度可以根据缓冲队列长度来确定。交换结点可以利用分组头部中的拥塞信息位向端结点通告拥塞,或者向发送结点发送特殊的控制分组通告拥塞信息,这样的反馈是直接的。反馈也可以是间接的,由发送结点从本地观察到的分组延迟或丢失情况来推断拥塞是否发生。发送结点在收到拥塞信息后应减少它输出给网络的分组流量,拥塞控制的基本手段是降低发送主机的输出分组流,即源抑制。

9-7 不同的交换方式具有不同的性能。为了使数据在网络中的传输延迟最小,首选的交换方式是__(1)___。与电路交换相比,分组交换的一个重要优点是__(2)___,最大的缺点是__(3)___。分组交换对报文交换的主要改进是 ____(4)___,这种改进产生的直接结果是 ____(5)___。

- (1) A . 电路交换
C . 分组交换
 - (2) A . 延迟时间小
C . 缓冲区易于管理
 - (3) A . 增大了延迟
C . 不能实现速率转换
 - (4) A . 传输单位更小长度有限
C . 可进行差错控制
 - (5) A . 降低误码率
C . 减少延迟
- B . 报文交换
D . 信元交换
 - B . 可充分利用通信线路
D . 便于标准化
 - B . 不能实现链路共享
D . 不能满足实时应用要求
 - B . 传输单位更大
D . 路由算法更简单
 - B . 提高数据率
D . 增加延迟

答案: A, B, A, A, C

9-8 设待传送数据总长度为 L 比特, 分组长度为 P 比特, 其中头部开销长度为 H 比特, 源结点到目的结点之间的链路数为 h , 每个链路上的延迟时间为 D 秒, 数据传输率为 Bb/s , 电路交换和虚电路建立连接的时间都为 S 秒, 在分组交换方式下每个中间结点产生 d 比特的延迟时间, 则传送所有数据, 电路交换需时间为 (1) 秒, 虚电路分组交换所需时间为 (2) 秒, 数据报分组交换所需时间为 (3) 秒。 ($[X]$ 表示对 X 向上取整)

- $$\begin{aligned}
(1) \quad & A \cdot hD + L \cdot B & B \cdot S + hD + L \cdot P \\
& C \cdot S + hD + L \cdot B & D \cdot S + L \cdot B \\
(2) \quad & A \cdot S + (hd \cdot B + P \cdot B) \times [L \cdot (P - H)] \\
& B \cdot S + (hD + P \cdot B) \times [L \cdot (P - H)] \\
& C \cdot S + ((h - 1)D + P \cdot B) \times [L \cdot (P - H)] \\
& D \cdot S + ((h - 1)d \cdot B + hD + P \cdot B) \times [L \cdot (P - H)] \\
(3) \quad & A \cdot (hd \cdot B + P \cdot B) \times [L \cdot (P - H)] \\
& B \cdot (hD + P \cdot B) \times [L \cdot (P - H)] \\
& C \cdot ((h - 1)d \cdot B + hD + P \cdot B) \times [L \cdot (P - H)] \\
& D \cdot ((h - 1)d \cdot B + hD + P \cdot B) \times [L \cdot P]
\end{aligned}$$

答案：C, D, C

第 10 章

广域网实例

10-1 和 X.25 对照,简述帧中继技术的特点。

解答: X.25 分组交换网的传输线路基本上是借助于电话网,它容易受到各种干扰,误码率较高。为了保证可靠的信息传输,X.25 分组交换网分为物理层、数据链路层和分组层,在数据链路层和分组层进行两级的差错控制。帧中继传输采用光缆,大幅度地提高了信息传输速率,而且它不受电磁干扰,误码率大大降低。帧中继协议进行了简化,帧中继只有数据链路层和物理层,而且数据链路层只有简单的差错控制,只是检测到错误帧时就简单地丢弃。

和 X.25 一样,帧中继也采用面向连接的虚电路交换方式,虚电路也分为交换虚电路 SVC 和永久虚电路 PVC 两种,但帧中继主要是为长距离用户提供 PVC 链路,为局域网提供互连服务。

另外,帧中继采用了快速分组交换技术,交换机接收到一帧时,只要读出帧的目的地址,就立即转发此帧。

10-2 帧中继包括哪些方式拥塞控制措施?请简单介绍。

解答: 帧中继包括以下三种拥塞控制措施:接纳控制、通信量管制和拥塞通知。

1. 接纳控制

接纳控制是帧中继根据新的连接请求的通信量和网络剩余带宽的容量确定是否接纳这一新的连接建立。新的连接请求若被接受,它对通信量的需求应得到某种保证。通信量描述包括以下 3 个参数,它们在用户和帧中继服务商为每一条虚电路达成的合约中约定。

承诺信息速率 CIR 网络承诺该连接的数据传输平均速率,实际上交换机是在某一约定的时间间隔 T_c 内对通信量进行测量;

承诺突发量 B_c 网络承诺该连接在 T_c 内可传输的最大信息量, $B_c = CIR \times T_c$;

超额突发量 B_e 描述在时间间隔 T_c 网络将试图为连接传输的、非承诺的最大超额信息量。

2. 通信量管制

一旦某连接被允许进入网络,与数据源连接的帧中继的边界交换机必须监控该连接的通信量,使其对网络资源的实际使用不超建立连接时所限定的数值。网络对连接的通信量管制基于在 T_c 内收到的帧的总比特数的多少,设为 N ,则通信量管制方式如下:

当 N 未超过 B_c 时,帧将被传输;

当 N 介于 B_c 和 $B_c + B_e$ 之间时, 网络将超过 B_c 的那些帧的 DE 标志置 1, DE 置 1 的帧也提交给网络, 但若无资源可用时它有可能被丢弃;

当 N 超过 $B_c + B_e$ 时, 帧将立即被丢弃。

3. 拥塞通知

帧中继交换结点使用帧首部的 FECN 和 BECN 比特进行显式的拥塞通知, 链路两端主机的高层协议根据帧中继的拥塞通知执行拥塞控制。当收到 BECN 拥塞通知时, 高层协议可以直接降低自己的发送速率。当收到 FECN 拥塞通知时, 接收端高层协议可以采取适当的流量控制措施。

10-3 解释异步传输模式(ATM)一词中“异步”的含义。

解答: ATM 是和同步传输模式 STM 相对应的。STM 采用时分多路复用(TDM)技术, TDM 将一条通信线路按一定周期将时间分成一个个时间片, 称为帧, 每一个帧又分成若干个时隙, 每个时隙携带一个用户的信号。STM 在传输中每个用户信息所占用的时隙在帧内的相对位置是固定不变的, 为每个用户提供了周期性的固定长度的传输时间。

STM 的这种时隙的利用方式简化了控制, 但也存在一些问题。当某个用户暂无信息发送时, 它所占用的时隙就闲置, 而另一用户有大量突发性数据要传送, 也只好在它固定的时隙内等待传送, 信号产生时延。

ATM 采用统计时分多路复用(STDM)方式, 用户信息在每个帧中所占用时隙的位置不是固定不变的, 而且还可以根据需要在在一个帧中分配多个时隙。在 ATM 中, 只要帧中有空闲时隙, 信息就可占用, ATM 这种时隙的利用方式, 使得来自一个特定用户的信息在信道中的传输没有周期性, 因而称为异步传输模式。

目前 ATM 物理层主要使用 SDH, 因此 ATM 中的“异步”实用中就是 ATM 信元异步插入到 SDH 帧中。

10-4 从数据交换技术上讲, 信元交换的特点是什么?

解答: 从数据交换技术上讲, 信元交换有如下特点:

信元交换属于面向连接的虚电路分组交换技术;

信元交换属于快速分组交换 FPS, 当交换结点收到 5 个字节的信头就开始转发信元;

信元交换的分组是只有 53 个字节的定长的信元, 长度固定而且很短的信元使得交换结点只用硬件电路就可以进行信元处理, 大大缩短了处理时间。

10-5 什么是虚通路(VP)和虚通道(VC)? 叙述它们的作用和特点。

解答: VP 和 VC 用来表示 ATM 连接。一个 VC 表示传送 ATM 信元的一条通道, 用虚通道标识(VCI)来标识。一个 VP 包含一组 VC, 可达 65 536 个, VP 用虚通路标识(VPI)来标识, 这组虚通道有同样的 VPI 和不同的 VCI。两个不同的 VP 中的 VC 可以有相同的 VCI, 因此 VPI 和 VCI 一起(记为 VPI/VCI)才能完全识别一个虚通道。

VP 和 VC 是单向的, 但在建立连接时可以同时建立起两个端点之间的一对虚电路, 它们可以使用相同的标识符, 但两个方向上, 信道的特性可以不同。

VPI/VCI 只有局部意义。一个 VPI/VCI 只标识相邻两个结点之间的虚通道。在两个端用户的 ATM 连接上, 可能经过多个交换结点, 所有相邻两个结点之间的虚通道都有

自己的 VPI/VCI。ATM 信元的传输根据信元的 VPI/VCI 标识和交换机的 VPI/VCI 转换表进行。

VP 和 VC 是逻辑概念,一条实际的物理线路可以建立多条虚通路和虚通道。

10-6 说明 ATM 层如何转发信元。

解答: ATM 层根据信元头部的 VPI/VCI 和 ATM 交换机的 VPI/VCI 转换表转发信元。VPI/VCI 转换表是在建立连接时由信令协议在交换结点上建立的。转换表包含有入口端口号和入口 VPI/VCI 以及出口端口号和出口 VPI/VCI,从而指示了信元传输路径 VCC 上的下一个结点。

在交换结点,从某一输入端口接收到一个信元后,查找转换表,根据端口号和信元头部的 VPI/VCI 得到出口的 VPI/VCI 和端口号,将出口的 VPI/VCI 填入信元头部,更新 VPI/VCI 字段,并将信元由查到的出口端口输出。这样利用 VPI/VCI 沿 VCC 逐结点转发信元,直至到达目的端。

10-7 在 ATM 网络的协议结构中,AAL 层在什么位置出现? ATM 交换机包含什么层次?

解答: 在 ATM 网络的协议结构中,AAL 层仅在 ATM 网络的端点(如主机、IP 路由器等)实现,而在网络的中间交换结点,即 ATM 交换机,只有 ATM 层和物理层。

10-8 ATM 规定了哪几种服务类型?它们的特点是什么?

解答: ATM 论坛依据 ATM 所提供的通信量特性规定了 5 种服务类型:

(1) 恒定比特率(CBR) 这类服务包括 PCM 编码的话音和未经压缩的视频信号的传输等,在整个连接期间信元的传输速率不变。

(2) 实时可变比特率(rt-VBR) 用于具有严格实时要求的可变速率通信量,如实时电视会议一类的服务。这种应用中,屏幕上的画面时而相对静止时而很快变化,当采用 MPEG 标准对视频信号进行压缩时,传输的比特率也随着屏幕的变化而有很大的变化。

(3) 非实时可变比特率(nrt-VBR) 用于没有严格实时要求的可变速率通信量,如多媒体电子邮件和存放在媒体上的视像信息。

(4) 不指明比特率(UBR) 用来支持“尽最大努力服务”的非实时应用,它们可以使用网络的剩余带宽,对时延不敏感。这类服务的例子是数据传输业务,如文件传输等。

(5) 可用比特率(ABR) 这类服务是对 UBR 的改进。ABR 的设计目的是使非实时的数据业务能够动态地充分利用其他高优先级业务(CBR 和 VBR)剩下的可用带宽,并试图使所有的 ABR 用户公平合理地共享网络的可用带宽,而不影响 CBR 和 VBR 连接的服务质量。ABR 服务根据网络的当前负荷情况依靠反馈机制调整源端点的发送速率,因而可获得较小的信元丢失率 CLR,而 UBR 不进行调整。

10-9 为了保证网络服务质量(QoS),ATM 规定了哪些说明用户通信量和网络服务质量的参数?

解答: 下面的 3 个参数用来描述网络提供的服务质量:

信元丢失率(CLR): CLR 等于丢失的信元数与传送的信元数之比。每个信元的头部有一比特的信元丢弃优先级 CLP 字段,在网络拥塞时,首先丢弃 CLP=1 的信元。应用中 CLR 可用于 CLP=0 的守约信元或 CLP=0 和 1 的总信元。

信元传送时延(CTD):信元离开源 UNI 到达目的 UNI 所经历的时延,包括传播时延、在各个中间交换机的排队时延和在交换机的交换时延等。

信元时延偏差(CDV):时延偏差也称时延抖动,指 CTD 变化量的最大值,也称为峰峰 CDV。

以下 5 个参数用来描述用户的通信量,ATM 应该监视用户发送的数据流:

峰值信元速率(PCR)(信元数/s):用户计划发送信元的最大速率,PCR 的倒数即最小信元间隔。

最小信元速率(MCR):用户能够接受的信元最小速率。

持续信元速率(SCR):信元在一段时间 T 内的平均速率。SCR 并不是在任意长一段时间内的平均信元速率。在突发数据时,SCR 大于长时间的平均信元速率。

最大突发量 MBS:在 PCR 下可连续发送的最大信元数。

信元时延偏差容差 CDVT:信元之间间隔的偏差即信元时延的抖动的范围。对于 PCR 和 SCR,它是要被指定的。

10-10 叙述 ATM 对于 ABR 类服务的拥塞控制方式。

解答:ATM 对于 ABR 类服务的拥塞控制方式是一种闭环控制方式,它是一种基于速率的方法,发方依据网络反馈的拥塞状况的信息,计算出信元发送速率。

ABR 拥塞控制设计了一种特殊的资源管理(RM)信元,其负荷类型 PT=110,发送端在 n 个数据信元(默认值为 32)之后发出一个 RM 信元,它由连接上的交换机特殊处理,携带连接上的拥塞信息。当 RM 信元到达目的端后再返回发送端,发送端根据 RM 信元的拥塞信息调整信元发送速率。ABR 有两种机制可以从连接上的交换机得到拥塞状况的反馈信息:

简单的拥塞指示 每个数据信元的 PT 字段都会有一个显式前向拥塞指示 EFCI 比特,一个发生拥塞的交换机可以将该比特置 1,目的端对接收到的所有信元的 EFCI 进行检测。当一个 RM 信元到达时,如果最近收到的信元的 EFCI 为 1,则将 RM 信元的拥塞指示 CI 比特由初始值 0 变为 1,并将 RM 信元发回发送端。

显式的速率反馈 RM 单元还包含一个 2 字节的显式速率 ER 字段,ER 的初值置为 PCR。在 RM 信元的往返传输过程中,路径上的拥塞的交换机会将 RM 信元的 ER 值降为它所能支持的值,但不能增加。这样,(ER)字段将被修改为源端到目的端路径上所有交换机的最小支持速率。

当 RM 信元返回发送端后,发送端会根据 CI 和 ER 值调整信元发送速率。如果 RM 信元丢失,发送端也要降低信元发送速率,因为 RM 信元丢失可能是网络拥塞而致。

10-11 什么是非对称数字用户线 ADSL 技术?为什么称为非对称?它在一根电话线上划分几个信道?

解答:模拟电话线路的传输带宽可达到 1.1MHz 以上,而普通老式电话业务(POTS)只使用 0~4kHz 这一段,数字用户线(DSL)技术利用传统电话线路的高频段传输数据,它使用 FDM 方式充分挖掘了传统电话线路的带宽资源。

ADSL 是 DSL 中的一种,之所以称为“非对称”是指 ADSL 的技术提供下行大于上行的非对称传输速率,因为它一般多用于个人或家庭用户 Internet 浏览应用,通常下载网页

或文件的机会较多,而上传数据的机会相对较少。

当使用 ADSL 上网的时候,ADSL 调制解调器使用 FDM 技术在一根电话线上产生三个信道;一个为标准电话服务的话音信道,一个是中速上行信道,另一个是高速下行信道,并且这三个信道可以同时工作。

10-12 典型 ADSL Internet 接入网络主要包括什么设备?它们的作用是什么?

解答:典型 ADSL Internet 接入网络主要有两部分设备:一部分是用户端设备,主要是 ADSL modem 和语音分离器;另一部分是中心结点设备,主要是语音分离器和数字用户线接入复用器(DSLAM)。

ADSL modem 将用户设备送来的数据信息(如 IP 报文)封装成 PPP 帧格式,经 ADSL 调制电路调制成适合在铜质双绞线上远距离传输的模拟信号后,送到双绞线进行传输。在相反方向,ADSL modem 将通过双绞线送来的模拟信号解调为二进制比特流,由 PPP 帧中分离出 IP 报文,送给用户设备。

语音分离器用于合成或分离电话机的话音信号和 ADSL modem/ DSLAM 调制的信号。用户端的话音分离器将来自 ADSL modem 的模拟信号和来自电话机的话音信号合成在一起,通过双绞线进行传输。在相反方向,语音分离器将双绞线上的信号分离为话音信号和 ADSL modem 调制的模拟信号,分别送给电话机和 ADSL modem。中心结点的话音分离器的作用类似。

DSLAM 主要有两个功能,一是 ADSL 接入,DSLAM 一般都内嵌多个 ADSL modem,可以同时接入多个 ADSL 访问;二是多路接入复用,将同时接入的多个 ADSL 访问复用到公共数据网络,接入 Internet。

10-13 什么是混合光纤同轴电缆网(HFC)?简述 HFC 网络结构。

解答:HFC 网是在有线电视网 CATV 的基础上发展起来的,HFC 是混合有光纤和同轴电缆的网络,是双向的,除了提供原来的 CATV 电视播送业务外,还能提供数据业务,进行 Internet 宽带接入。

HFC 是混合光纤同轴电缆网,光纤部分是星型网络拓扑,同轴电缆部分是树型网络拓扑。由电缆调制解调器终端系统 CMTS 到各服务区的光纤结点使用光纤,构成星型网,CMTS 与光纤结点的典型距离为 25km。服务区内使用同轴电缆,由光纤结点连接到各个住宅。一个光纤结点下可接 1~6 根同轴电缆,再使用分线器将同轴电缆引入各个住宅用户,组成一个服务区。一个光纤结点下的 HFC 同轴电缆系统构成一个树型结构的网络拓扑。同轴电缆网络虽然形式上是树型结构,但实质上是共享媒体的总线型结构。光纤结点到用户一般不超过 2~3km。为了补偿同轴电缆中信号传播的衰减,每 600m 左右要加入一个放大器。

10-14 电缆调制解调器(cable modem)工作在 OSI 模型中的什么层次?简述 cable modem 在 HFC 网络中的作用。

解答:cable modem 工作在 OSI 的物理层和数据链路层。

cable modem 是放在用户家中的端接设备,连接用户主机和 HFC 网络,提供用户双向数据接口。cable modem 一般使用 10BaseT 接口连接用户主机。

在上行方向 cable modem 从计算机接收数字数据,把它们调制成模拟信号,通过

HFC 传送到前端 CMTS。一个用户群共享上行信道,可能会产生冲突,因此在 cable modem 的媒体接入控制 MAC 子层要类似以太网采用 MAC 协议。在下行方向, cable modem 接收 HFC 网上的模拟信号, cable modem 将其解调为数字数据传送给用户计算机。下行方向采用广播方式,每个 cable modem 都监听下行信道广播的数据,只有地址与之匹配的 cable modem 才接收数据,因此下行信道没有冲突的问题。

10-15 帧中继网的虚电路建立在__(1)__,在用户平面采用的协议是__(2)__.这种网络没有流量控制功能,但增加了拥塞控制功能。如果沿着帧传送方向出现了拥塞,则把帧地址字段中的__(3)__位设置为 1,这样接收方就可通过__(4)__协议要求发送方降低数据速率。

- (1) A . 数据链路层 B . 网络层 C . 传输层 D . 会话层
- (2) A . X.28 B . HDLC C . LAP-D D . LAPF
- (3) A . BECN B . FECN C . DECN D . TECN
- (4) A . 网络层 B . 数据链路层 C . 传输层 D . 高层

答案: A, D, B, D

10-16 ATM 网络中使用信元作为传输数据的单位,当信元从用户端进入网络中第一个交换机后,信元头中修改的部分是__(1)__.信元传输采用__(2)__.当进行 VP 交换时,VPI 和 VCI 的变化情况是__(3)__.当需要传输压缩的视频流数据时,采用的服务类别最好是__(4)__。

- (1) A . VCI B . GFC C . CLP D . PT
- (2) A . TDM B . FDM C . WDM D . STDM
- (3) A . VPI 变化,VCI 不变 B . VPI 不变,VCI 变化
- C . VPI 变化,VCI 变化 D . VPI 不变,VCI 不变
- (4) A . CBR B . ABR C . UBR D . rt-VBR

答案: B, D, A, D, D

10-17 ATM 网络采用__(1)__多路复用技术传送信元,典型的数据速率为 155.5Mb/s,这样每秒大约可以传送__(2)__万个信元。采用短的、固定长度的信元,为使用硬件进行高速,数据交换创造了条件。ATM 网络采用了许多通信量管理技术以避免拥塞的出现,其中__(3)__是防止网络过载的第一道防线。

- (1) A . 统计时分 B . 同步时分 C . 频分 D . 码分
- (2) A . 24 B . 36 C . 56 D . 64
- (3) A . 接纳控制 B . 选择性信元丢弃
- C . 通信量整形 D . 使用参数控制

答案: A, B, A

10-18 N-ISDN 定义的基本速率接口中,B 信道的数据速率是__(1)__kb/s,D 信道的数据速率是__(2)__kb/s,用来传输话音和数据的信道是__(3)__.在一条 64kb/s 的理想信道上,传送一个 100KB 的文件需要的时间是__(4)__s。

- (1) A . 16 B . 32 C . 64 D . 128
- (2) A . 16 B . 32 C . 64 D . 128

- (3) A . A 信道 B . B 信道 C . C 信道 D . D 信道
- (4) A . 1 .56 B . 1 .6 C . 12 .5 D . 12 .8

答案: C, A, B, D

10-19 非对称数字用户线 ADSL 是采用__ (1) __调制通过双绞线向用户提供宽带业务、交互式数据业务和普通电话服务的接入技术, 其上行速率为 640kb/s ~ 1Mb/s, 下行速率为 1Mb/s ~ __ (2) __, 有效传输距离为 3 ~ 5km。cable modem 又叫线缆调制解调器, 它可以连接用户家中的 PC 和 __ (3) __网络。cable modem 的最高上行速率可达 __ (4) __, 下行速率则更高, 彻底解决了由于声音/ 图像传输而引起的阻塞。

- (1) A . TDM B . FDM C . WDM D . CDM
- (2) A . 8Mb/s B . 4Mb/s C . 2Mb/s D . 1 .5Mb/s
- (3) A . ATM B . PSTN C . HFC D . FR
- (4) A . 10Mb/s B . 2Mb/s C . 1 .5Mb/s D . 1Mb/s

答案: B, A, C, A

10-20 阅读以下有关网络接入方案的说明并回答问题。

某单位已完成了主干网络的建设任务, 现在需要对其住宅区的部分用户接入主干网的技术方案作选型设计。职工住宅已有的通信条件是: (1) 电话线和 (2) 电视铜缆。在不重新布线的前提下, 以下 4 种技术方案可供选择: (1) 异步拨号, (2) ISDN, (3) ADSL, (4) cable modem。请回答:

(1) 采用电话线方式上网, 并按要求在计算机连入网络的同时能通电话, 连网速率高于 500kb/s, 可以选用哪种技术方案? 其最高通信速率为多少?

(2) 采用电视铜缆接入计算机主干网络, 用户端需增添什么设备? 理论上网络提供的最高通信速率为多少? 实际的速率大约是多少?

解答: (1) 采用 ADSL, 上行、下行速度分别为 1Mb/s、8Mb/s。

(2) 用户端需增添 cable modem, 上行、下行速度最高速率分别可达 10Mb/s 和 36Mb/s, 但实际的上行、下行速率分别为 0.2 ~ 2Mb/s 和 3 ~ 10Mb/s。

第 11 章

网 际 层

11-1 用一句话概述网际层提供什么样的网络服务。

解答：网际层负责将数据报从源主机传送到目的主机，提供无连接的、不可靠的但尽力而为的数据报传送服务。

11-2 IPv4 的地址包括哪几个字段？分为几类？用户使用哪几类？画图表示它们的结构。它们各适用于什么规模的网络？IP 地址使用什么记法表示？你们单位的 IP 地址网络号字段是什么？是几类的？

解答：IPv4 定义的 IP 地址是 32 比特长度的二级地址，包括 3 个字段：

- 类别字段；
- 网络号字段 net-id；
- 主机号字段 host-id。

IP 地址分为 A、B、C、D、E 5 类，其中 D 类为多播地址，E 类保留，今后使用；用户使用的是 A、B、C 3 类，称为基本类。IP 地址的字段结构如图 1-11-1 所示。

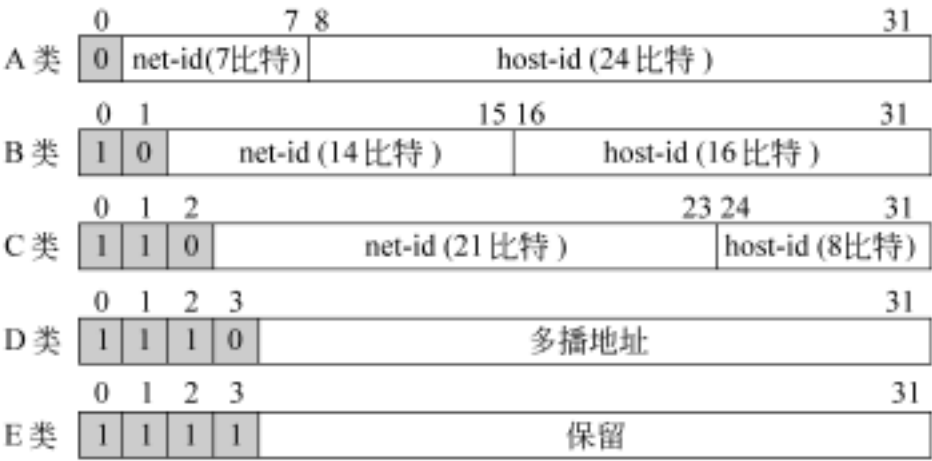


图 1-11-1 IP 地址的字段结构

A、B、C 3 类 IPv4 地址分别适用于大、中和小规模的网络，它们分别可包含 1 677 万、65 534 和 254 台主机。

IPv4 地址使用点分十进制记法表示，32 比特的 IP 地址常记为用点相连的 4 个十进制数，每个十进制数对应 8 比特的二进制。采用点分十进制记法读写方便，易于记忆。

11-3 说出特殊形式的 IP 地址及其意义。

解答：全 0 或全 1 的网络号和主机号的 IP 地址有特殊用途，一般不使用，汇总于表 1-11-1：

表 1-11-1 特殊形式的 IP 地址及其用途

特殊 IP 地址		用 途
网络号	主机号	
全为 0	全为 0	表示本主机,只作源地址,启动时用,之后获得了 IP 地址不再使用
全为 0	host-id	本地网络上主机号为 host-id 的主机,只作源地址
全为 1	全为 1	有限广播(本地网络),只作目的地址,各路由器都不转发
net-id	全为 1	定向广播(net-id 标识的网络),只作目的地址
net-id	全为 0	标识一个网络
127	任意	本地软件回送测试(loopback test),Internet 上不能出现这种地址

11-4 如果没有进行子网划分,A、B 和 C 类 IP 地址的子网掩码各是什么?

解答:如果没有进行子网划分,A、B 和 C 类 IP 地址的子网掩码分别是 255 .0 .0 .0, 255 .255 .0 .0 和 255 .255 .255 .0。

11-5 某单位的网络使用 B 类 IP 地址 166 .111 .0 .0,如果将网络上的计算机划分为 30 个子网,subnet-id 应该取几位?子网掩码应该是什么?每个子网最多可包含多少台计算机?试用二进制和点分十进制记法对应地写出 subnet-id 最小的子网上 host-id 最小和最大的主机的 IP 地址。

解答:如果将该单位的 B 类网络划分为 30 个子网,subnet-id 应该取 5 位,子网掩码应该是 255 .255 .248 .0,每个子网最多可包含 $2^{11} - 2 = 2\,046$ 台主机。

subnet-id 最小的子网上 host-id 最小的主机的 IP 地址:
10100110 01101111 00001000 00000001, 166 .111 .8 .1。

subnet-id 最小的子网上 host-id 最大的主机的 IP 地址:
10100110 01101111 00001111 11111110, 166 .111 .15 .254。

11-6 一个 A 类 IP 网络 17 .0 .0 .0,欲划分为 6 个子网,子网掩码应该是什么?给出每个子网的 IP 地址的范围。

解答:子网掩码是:255 .224 .0 .0

子网 1:17 .32 .0 .1 ~ 17 .63 .255 .254

子网 2:17 .64 .0 .1 ~ 17 .95 .255 .254

子网 3:17 .96 .0 .1 ~ 17 .127 .255 .254

子网 4:17 .128 .0 .1 ~ 17 .159 .255 .254

子网 5:17 .160 .0 .1 ~ 17 .191 .255 .254

子网 6:17 .192 .0 .1 ~ 17 .223 .255 .254

11-7 ARP 进行的是哪两种地址的转换?ARP 如何进行地址的转换?它采取了哪些措施提高地址转换的效率?

解答:ARP 用于从 IP 地址到物理地址的转换。

ARP 使用动态绑定的方式进行 IP 地址到物理地址的转换。动态绑定是在同一个物理网络上进行的,网络应该支持广播方式。ARP 的操作过程如下:在某一物理网络上,一

个主机 a 欲解析另一个主机 b 的 IP 地址 IP_b 。a 先在网络上广播一个 ARP 请求报文,请求 IP 地址为 IP_b 的主机回答其物理地址 PHY_b 。网上所有主机都将收到该 ARP 请求,但只有 b 识别出自己的 IP_b 地址,并做出应答,向 a 发回一个 ARP 响应报文,回答自己的物理地址 PHY_b 。应答不再使用广播方式。

ARP 采取如下措施提高地址转换的效率:

使用高速缓存。每台 ARP 的主机保留了一个专用的 ARP 缓存区存放最近获得的 IP 地址和物理地址的映射,ARP 先在缓存中查找 IP 地址对应的物理地址。

在 ARP 请求报文中放入源站的 IP 地址和物理地址的映射,以免目标机紧接着为解析源站的物理地址而再进行一次动态绑定操作。

源站在广播自己的地址映射时,网上所有主机都将它存入自己的高速缓存。

新的主机入网时,主动广播自己的地址映射。

11-8 IP 数据报首部的定长域的长度是多少?最大首部长度是多少?IP 数据报可携带的数据长度最多是多少?

解答:IP 数据报首部的定长域的长度是 20 字节。最大首部长度是 60 个字节,除定长域长度 20 字节,选项的最大长度为 40 个字节。IP 数据报的总长字段指示整个 IP 数据报的长度,包括报头长及数据区长,单位为字节。总长字段为 16 比特,所以 IP 数据报最长可达 65 535 个字节。IP 数据报可携带的数据长度最大是 65 535 减去 (20 ~ 60) 字节的首部长度。

11-9 IP 对数据报的什么部分进行差错校验?其优、缺点是什么?IP 在什么结点进行差错校验?为什么?

解答:IP 只对数据报的首部进行校验,而不对数据区进行校验。这种做法的优点是可以节约路由器处理每一个数据报的时间,提高 IP 层的处理效率。但缺点是它给高层软件遗留下了数据不可靠的问题,增加了高层协议的处理负担。不同的高层协议可以根据具体情况,选择自己的数据校验方法,也可以不再校验。

在传输的路径上,数据报每经过一个结点都要重新计算报头校验和,因为据报的首部的生存时间、标志、片偏移等字段在转发过程中可能发生变化。

11-10 IP 如何进行数据报传输延迟监控?

解答:IP 主要使用数据报的生存时间(TTL)字段进行数据报的延迟监控。TTL 最大值为 120s,传送过程中,路由器要从该字段减去已经历的时间。一旦 TTL 小于等于 0,生存时间结束,便将该数据报从网中删除,并向源站报告出错信息。

一般 TTL 是一个粗略的数值,可以采用简单的处理办法。路径上的路由器处理报头时,简单地将 TTL 减 1,如果数据报在路由器中因等待服务被延迟,再减去延迟的时间。

在接收端的内存中还设置了另一种监控数据报传输延迟的重组定时器。接收端收到某个数据报的第一个分片之后,启动一个重组定时器开始计时,如果在规定时间限制之内还未收到全部分片,则放弃整个数据报,并向源站报告出错信息。

11-11 什么是最大传输单元(MTU)?IP 数据报传输中为什么要进行分片与重组?分片在何处进行?重组在何处进行?

解答：各种物理网络对可传输的数据量的上限有自己的规定,叫做最大传输单元(MTU)。不同物理网络的 MTU 一般是不相同的,如以太网为 1 500 字节。与 MTU 不同,IP 数据报的大小可在一定范围内选择,比如 IPv4 协议规定每一 IP 数据报最大不能超过 65 535 个字节。因为不同物理网络的 MTU 不同,无法选择一个合适的 IP 数据报长度来适应路径中的所有物理网络。为此,IP 协议提供一种 IP 数据报分片机制,在路径中 MTU 较小的网络,将数据报分成若干较小的片进行传输,到达目的站后再将所分的片进行重组,恢复原数据报。

分片在物理网络的交界处进行,即由路由器负责,而片重组是在目的站完成。

11-12 无选项 IP 数据报携带 5 000 字节数据,它下一步经由 MTU 为 1 500 字节的以太网,数据报如何分片?用图形表示分片的情况,并标明每个分片的片头中“片偏移”字段的数值。

解答：分片的方法及片的格式如图 1-11-2 所示,片头中相关字段的值也示于图中,其中 x 代表源站赋予数据报的标识符。

数据区大小为 5 000 字节的原数据报：

报头(标识= x ,标志=000,偏移 0)	数据(3 600 字节)
--------------------------	--------------

在 MTU = 1 500 字节网络上的 4 个分片

片 1 头(标识= x ,标志=001,偏移 0)	片 1 数据(1 480 字节)
片 2 头(标识= x ,标志=001,偏移 185)	片 1 数据(1 480 字节)
片 3 头(标识= x ,标志=001,偏移 370)	片 2 数据(1 480 字节)
片 4 头(标识= x ,标志=000,偏移 555)	片 3 数据(560 字节)

图 1-11-2 题 11-12 的 IP 数据报分片

11-13 什么是直接交付和间接交付？

解答：直接交付是指在同 一个物理网络上,把 IP 数据报从源站或路由器直接传送到目的站,数据报传送中间不涉及路由器。当源站与目的站在一个物理网络上时,才能进行直接交付。数据报路径上的最后一个路由器总是和目的站连在同一个物理网络上,因此使用的是直接交付形式。

当目的站与源站不在一个直接连接的物理网络上时,就必须进行间接交付,源站需要把数据报发给某一个与它连接在同一个物理网络上的路由器,由它进行转发。显然,除最后一个将数据报直接交付给目的站的路由器之外,所有传送路径上的其他路由器也都使用间接交付。

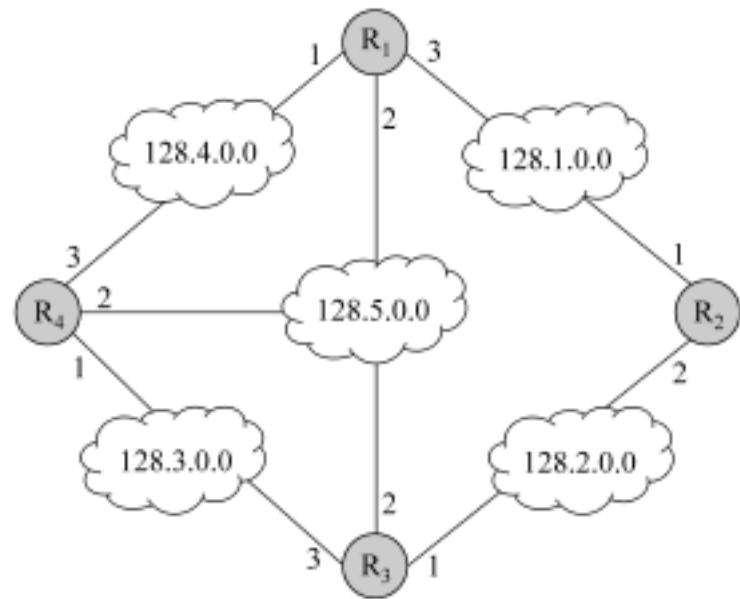
11-14 最基本的路由表包含什么信息?IP 采用什么样的数据报转发机制?叙述基本的数据报转发流程。

解答：最基本的路由表包含许多(目的网络 IP 地址,下一跳 IP 地址)序偶,其中目的网络 IP 地址中 host-id 部分置为 0,下一跳 IP 地址是到目的网络路径上的下一跳或称下一站(next hop)的 IP 地址。

IP 的数据报转发机制是路由表驱动的下一跳转发，从源到目的结点的整个传送过程是逐跳(hop by hop)进行的。路由表为每个目的网络指明路径上的下一跳,IP 根据数据报的目的网络地址去查找路由表,由匹配的表项得到下一跳的 IP 地址,每个结点负责转发到自己的下一跳。

```
基本的 IP 数据报转发流程如下：
从数据报中提取目的站 IP 地址 D,并计算其网络前缀 N,查找路由表
if N 与任何直接相连的网络的地址匹配
    then 通过该网络把数据报交付到目的地 D(其中涉及到把 D 转换成一个物理地址、封装数据报并发送该帧)
else if 路由表中包含一个到 D 的指定主机路由
    then 把数据报发送到表中指定的下一跳
else if 路由表中包含到网络 N 的一个路由
    then 把数据报发送到表中指定的下一跳
else if 路由表中包含一个默认路由
    then 把数据报发送到表中指定的默认路由器
else 宣布数据报转发出错
```

11-15 对于图 1-11-3(a)所示的网络图和图 1-11-3(b)所示的路由器端口和 IP 地址的对应关系,请给出路由器 R₂和网络 128.3.0.0 上的某一计算机的基本路由表(表中只包含目的网络和下一跳地址)。如果有多种选择,只要给出一种跳数最小的就可以。



(a) 网络图

路由器	端口 1 对应 IP 地址	端口 2 对应 IP 地址	端口 3 对应 IP 地址
R ₁	128.4.0.1	128.5.0.1	128.1.0.1
R ₂	128.1.0.2	128.2.0.1	无
R ₃	128.2.0.2	128.5.0.2	128.3.0.1
R ₄	128.3.0.2	128.5.0.3	128.4.0.2

(b) 路由器端口和 IP 地址的对应关系

图 1-11-3 题 11-15 的图示

解答：路由器 R₂ 的路由表见表 1-11-2：

表 1-11-2 路由器 R₂ 的路由表

目的主机所在网络	下一跳地址
128 .1 .0 .0	直接交付,端口 1
128 .2 .0 .0	直接交付,端口 2
128 .3 .0 .0	128 .2 .0 .2
128 .4 .0 .0	128 .1 .0 .1
128 .5 .0 .0	128 .1 .0 .1

网络 128 .3 .0 .0 上某一主机的路由表见表 1-11-3：

表 1-11-3 网络 128. 3. 0. 0 上某一主机的路由表

目的主机所在网络	下一跳地址
128 .1 .0 .0	128 .3 .0 .1
128 .2 .0 .0	128 .3 .0 .1
128 .3 .0 .0	直接交付
128 .4 .0 .0	128 .3 .0 .2
128 .5 .0 .0	128 .3 .0 .1

11-16 设路由器 R 的不完整的路由表见表 1-11-4：

表 1-11-4 路由器 R 的不完整路由表

序号	目的网络	子网掩码	下一跳	转发端口
1	166 .111 .64 .0	255 .255 .240 .0	R ₁ 端口 1	Port-2
2	166 .111 .16 .0	255 .255 .240 .0	直接交付	Port-1
3	166 .111 .32 .0	255 .255 .240 .0	直接交付	Port-2
4	166 .111 .48 .0	255 .255 .240 .0	直接交付	Port-3
5	0 .0 .0 .0 (默认路由)	0 .0 .0 .0	R ₂ 端口 2	Port-1

现路由器 R 收到下述分别发往 6 个目的主机的数据报：

H₁：20 .134 .245 .78， H₂：166 .111 .64 .129， H₃：166 .111 .35 .72，

H₄：166 .111 .31 .168， H₅：166 .111 .60 .239， H₆：192 .36 .8 .73。

请回答下列问题：

- (1) 路由表中序号 1～4 的目的网络属于哪类网络？它们是由什么网络划分出来的？
- (2) 假如 R₁ 端口 1 和 R₂ 端口 2 的 IP 地址的 host-id 均为 5(十进制), 请给出它们的 IP 地址。
- (3) 到目的主机 H₁ ～ H₆的下一跳是什么？(如果是直接交付写出转发端口)

解答：(1) 路由表中序号 1~4 的目的网络属于 B 类网络,它们是由 166 .111 .0 .0 划分的子网。

(2) R₁ 端口 1 和 R₂ 端口 2 的 IP 地址分别连接在网络 166 .111 .32 .0 和 166 .111 .16 .0 上,它们的 IP 地址分别为:166 .111 .32 .5 和 166 .111 .16 .5。

(3) 到目的主机 H₁ ~ H₆的下一跳分别是:

H₁ : 166 .111 .16 .5

H₂ : 166 .111 .32 .5

H₃ : 直接交付,R 的 Port-2

H₄ : 直接交付,R 的 Port-1

H₅ : 直接交付,R 的 Port-3

H₆ : 166 .111 .16 .5

11-17 ICMP 报文如何传输?简述 ICMP 在 TCP/ IP 体系中的地位。

解答: ICMP 报文是封装在 IP 数据报的数据部分中进行传输的,包含 ICMP 报文的 IP 数据报报头的“协议”域标记为“1”,指明是 ICMP 报文。

虽然 ICMP 报文像 TCP 和 UDP 一样,是由 IP 数据报传输的,但 ICMP 并不是比 IP 更高层的协议,ICMP 软件只是作为整个 IP 软件的一个模块而存在。在协议层次结构中,ICMP 的差错和控制信息传输只是解决网际层中的一类特殊问题,它不能构成上层协议赖以存在的基础,在概念上并不能构成一个独立的层次,它只作为 IP 的一部分,每个 IP 实现中都应该包含它。

11-18 ICMP 差错报告的特点是什么?简要介绍主要差错报告报文。

解答: 差错报告具有以下特点:

(1) ICMP 差错报文的基本的功能是提供差错报告,但并不严格规定对差错应采取什么样的处理方式。

(2) ICMP 的差错报告都是路由器或目的站向源站报告的方式,即发现差错的路由器或目的站向源站发出报告。

(3) ICMP 差错报告是伴随着抛弃出错的数据报而产生的。IP 软件一旦发现传输错误,它首先抛弃出错的数据报,然后调用 ICMP 向源站报告出错信息。

ICMP 差错报告包括目的不可到达报告、超时报告和参数出错报告:

(1) 目的不可到达报告

所谓的目的有四个层次的不同概念,从大到小依次为:网络、主机、协议和端口,因此目的不可达中有网络不可达、主机不可达、协议不可达和端口不可达。

(2) 超时报告

一旦 TTL 值减到 0 或重组定时器定时时间到,路由器或目的站立即抛弃该数据报,并向源站发送 ICMP 超时报告。

(3) 参数出错报告

参数出错报文报告数据报报头和数据报选项有错误的参数。代码域有 0 和 1 两种情况:0 码值报告一个出错参数;1 码值报文报告缺少必要的选项。

11-19 ICMP 主要有哪些控制报文?它们的功能是什么?

解答：ICMP 提供的控制报文主要有源抑制报文和重定向报文。

TCP/ IP 采用源抑制技术进行拥塞控制,源抑制必须使发送数据的源站知道传输路径上有拥塞发生。源抑制报文用于通知源站传输中发生了拥塞。

重定向报文用于主机路由表的动态优化。主机启动时根据一个配置文件对其路由表进行初始化,初始的路由表一般都是比较小的,例如可能只有一个默认路由器地址。初始路由器一旦检测到某数据报经过了非优的路径传输,一方面继续将该数据报转发出去,另一方面向主机发送一个路由重定向报文,其中包含了重定向的最优路径上的下一个路由器的 IP 地址。这样主机开机后经过不断积累,就掌握了越来越多的最优路径信息。

11-20 路由协议的作用是什么？有哪两类路由协议？

解答：路由协议用于路由器之间不断地交换路由信息,并根据接集到的信息,运行路由算法,优化更新路由,维持路由器有一个动态的优化的路由表。

基于自治系统的定义和划分,TCP/ IP 把路由协议分为如下两大类：

内部网关协议(IGP)是在一个自治系统(AS)内部使用的路由协议,由 AS 自主决定,与互联网中其他 AS 选用什么路由协议无关。这类协议常用的有 RIP 和 OSPF 协议等。

外部网关协议(EGP)用于多个 AS 之间的路由信息交换。在外部网关协议中,目前常用的是边界网关协议 BGP-4。

11-21 对于图 1-11-4,如果目的结点为结点 D,列表表示用距离矢量路由算法求各结点到目的结点的最短路径的迭代过程,并画出以 D 为根的最短路径树。

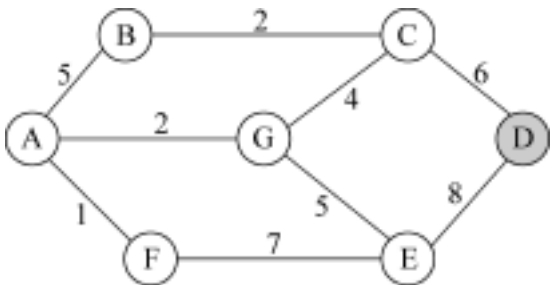


图 1-11-4 题 11-21 的图示

解答：对于图 1-11-4 所示的网络,在表 1-11-5 中给出了距离矢量算法计算各个结点到目的结点 D 的距离,表中 $(k, D(i))$ 表示计算结果,其中 k 为当前最短路径的下一跳,初始化时下一跳置为 no, $D(i)$ 为结点 i 到目的结点 D 的最短距离。

表 1-11-5 各个结点到目的结点 D 的距离

迭代	结点 A	结点 B	结点 C	结点 E	结点 F	结点 G
初始化	(no,)	(no,)	(no,)	(no,)	(no,)	(no,)
1	(no,)	(no,)	(D, 6)	(D, 8)	(no,)	(no,)
2	(no,)	(C, 8)	(D, 6)	(D, 8)	(E, 15)	(C, 10)
3	(G, 12)	(C, 8)	(D, 6)	(D, 8)	(E, 15)	(C, 10)
4	(G, 12)	(C, 8)	(D, 6)	(D, 8)	(A, 13)	(C, 10)
5	(G, 12)	(C, 8)	(D, 6)	(D, 8)	(A, 13)	(C, 10)

图 1-11-5 是最后计算得到的以目的结点 D 为树根的最小距离树。

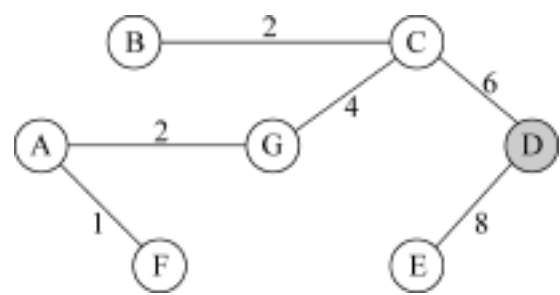


图 1-11-5 以目的结点 D 为树根的最小距离树

11-22 图 1-11-6(a)和(b)分别给出了路由器 B 原有的路由表和从邻接的路由器 A 传来的更新报文,据此给出路由器 B 更新后的路由表,用箭头指明为引起更新的表项。

目的站	距离	下一跳	目的站	距离	目的站	距离	下一跳
网络 1	1	直接	网络 1	2	网络 1	1	直接
网络 3	1	直接	网络 7	5	网络 3	1	直接
网络 7	8	路由器 D	网络 8	6	网络 7	6 (5+1)	路由器 A
网络 8	5	路由器 E	网络 22	7	网络 8	5	路由器 E
网络 14	7	路由器 C	网络 14	10	网络 22	8 (7+1)	路由器 A
网络 45	13	路由器 F	网络 45	14	网络 14	7	路由器 C
网络 78	6	路由器 A	网络 78	9	网络 45	13	路由器 F
					网络 78	10 (9+1)	路由器 A

(a) (b) (c)

图 1-11-6 题 11-22 的路由表

解答：图 1-11-6(c)即为路由器 B 更新后的路由表,箭头指明了引起更新的表项。当路由器 B 根据来自邻接的路由器 A 的报文添加或更新某个表项时,它把路由器 A 作为该表项的下一跳。如果 A 报告到某目的网络距离是 n ,那么 B 中更新过的表项中距离就是 $n + 1$ 。

11-23 已知网络拓扑和各链路长度如图 1-11-7 所示,请用 Dijkstra 算法计算由源结点 A 到网络的其他各结点的最短路径,用表格表示出计算过程,并画出最短路径树。

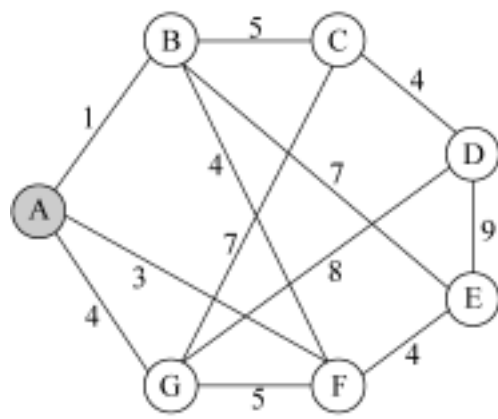


图 1-11-7 网络拓扑图

解答：表 1-11-6 是对图 1-11-7 网络求解的全部过程,上述步骤共执行了 6 次,因为网络有 7 个结点。表中的带“*”的数字是得到的最短路径值。

表 1-11-6 求解图 1-11-7 的过程

迭代	集合 N	结点 B	结点 C	结点 D	结点 E	结点 F	结点 G
初始化	{ A }	(B, 1)	(no,)	(no,)	(no,)	(F, 3)	(G, 4)
1	{ A, B }	(B, 1) [*]	(B, 6)	(no,)	(B, 8)	(F, 3)	(G, 4)
2	{ A, B, F }		(B, 6)	(no,)	(F, 7)	(F, 3) [*]	(G, 4)
3	{ A, B, F, G }		(B, 6)	(G, 12)	(F, 7)		(G, 4) [*]
4	{ A, B, F, G , C }		(B, 6) [*]	(C, 10)	(F, 7)		
5	{ A, B, F, G , C, E }			(C, 10)	(F, 7) [*]		
6	{ A, B, F, G , C, E, D }			(C, 10) [*]			

经过上述计算,就可得到以 A 为根的最短路径树,如图 1-11-8 所示。由最短路径树可以清楚地看到由源结点 A 到网络中任意一个结点的最短路径。

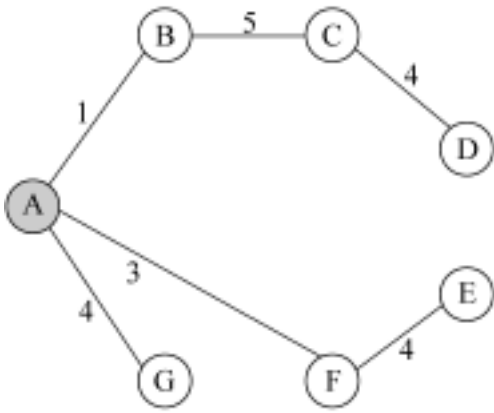


图 1-11-8 以 A 为根的最短路径树

11-24 什么是自治系统(AS)？AS 内部使用哪类路由协议？目前主要有什么协议？

解答：一个自治系统(AS)是一个包含一定范围的互连网络,其最重要的特点是它自己有权决定在本自治系统内部采用哪种路由协议。一般情况下,一个自治系统内部的所有网络属于某一个行政单位或一个 ISP 来管辖。

AS 内部使用内部网关协议 IGP,IGP 前面主要有 RIP 和 OSPF 协议。

11-25 IP 如何表示多播组地址？以太网如何表示组地址？用于多播的以太网地址范围是什么？

解答：IP 使用 D 类地址用作多播组地址。IPv4 的 D 类地址的前缀是 1110,占 4 个比特,其余 28 个比特用来标识多播组地址,共可以标识超过 2.68 亿个组。

以太网的物理地址为 48 比特,其中第 1 字节的最低位表示单地址或组地址,为 0 为单地址;为 1 则为组地址,支持多播。IANA 拥有高 24 位为 0x00005E 的以太网物理地址块,其中用于多播的以太网地址范围是 0x01005E000000 ~ 0x01005E7FFFFFFF,共有 2^{23} 个地址,有 800 多万个。

11-26 画图说明 IP 组地址如何影射为以太网物理地址。影射是一对一的吗？为什么？试举出一个例子。如何解决不惟一性的问题？

解答：当 IP 多播数据报交到底层以太网进行传送时,IP 组地址要转换(映射)为以太

网物理地址,映射关系如图 1-11-9 所示。

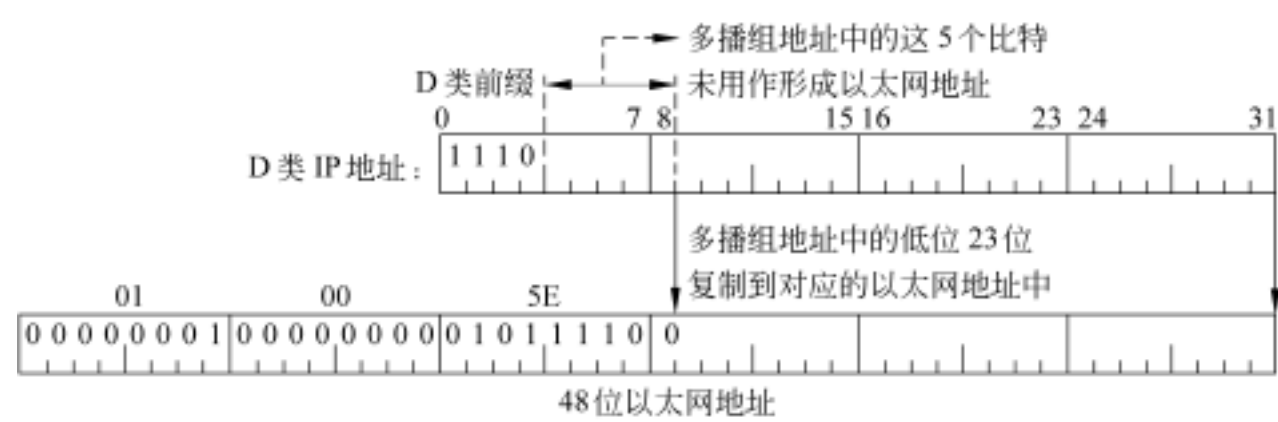


图 1-11-9 IP 组地址转换为以太网物理地址的映射关系

由于 28 比特 D 类 IP 地址中的 23 比特才和以太网组地址中的 23 比特有一一对应关系,28 比特的前 5 比特不能用来构成以太网硬件地址。这就导致这种映射不是一一对应的,而是多对一的。D 类 IP 地址中前 5 比特不同而后 23 比特相同的多个地址会映射为同一个以太网地址。例如:多播 IP 地址 224 .0 .65 .33 (即 0xE0004121)和 232 .128 .65 .33 (即 0xE8804121)转换成以太网多播物理地址均为 0x01005E004121。

由于这种映射的不惟一性,因此数据报到了 IP 层还需进行过滤,将不是本机接收的数据报丢弃。过滤的方法可以比较数据报的目的 IP 地址与本机的地址是否相同。由于组地址空间足够大,冲突的概率是很低的。

11-27 叙述 IGMP 的工作机制。为了提高效率,IGMP 又采用了一些措施,试举出两种。

解答:多播路由器有多个端口,分别连接不同的物理网络,对每个端口它都动态地维护一张组地址表,表中记录了与该端口连接的物理网络上的主机当前所加入的多播组地址。路由器根据这个表进行多播。

IGMP 多播路由器通过轮询本地网络上的主机,建立和维护这个组地址表。多播路由器周期性地(典型是 125s)轮询本地网络上的主机,以便确定目前各个多播组中有哪些主机。轮询是用组地址 224 .0 .0 .1 作为目的地址对本地主机发送查询报文,每个实现多播的主机必须加入永久多播组 224 .0 .0 .1。源地址是轮询的多播路由器的地址,组地址设置为 0,其 TTL = 1。

主机通过发送 IGMP 报告报文来响应多播路由器的查询,报告报文的地址使用欲加入的或已加入并继续保持的多播组的 IP 地址,报文中的组地址也填入这个地址,源地址为主机的 IP 地址, TTL = 1。一个主机中可能有一个或多个进程加入不同的组,对每个组都要发回 IGMP 报告。主机中应该维护一个表,它包含了所有参与多播的进程和它们所加入的多播组的 IP 地址。进程也可以随时离开一个组,当主机检测到参加某个组的进程全部都退出后,对于这个组,就不再发去 IGMP 响应报文。多播路由器也就知道现在这个主机已经退出了该多播组。

为了提高效率,IGMP 进一步采用了一些措施,如:

当一台主机上有多个进程要求加入同一个多播组时,则只有一个进程发出声明成员关系的报告报文。多播路由器并不关心一台主机上有多少个进程加入同一组。

当主机收到查询后,并不立即响应,而是延迟一个随机时间再响应,延迟时间在 0~10s,间隔为 0.1s。由于响应报文的目的地址是多播组的组地址,因此,后发送响应的主机在等待发送过程中就可能收到其他同组主机相同的 IGMP 响应报告,它们就不必再发送自己的响应报文了。因为多播路由器并不关心同一端口上连接有多少台主机属于同一组,不管有一台或多台主机属于该组,它都会对这个端口转发该组的数据报。

11-28 说明 RPF 的逆向路径转发处理方式,并以图 1-11-10 的路由器 R₁ 和 R₃ 转发源站 H₀ 的多播数据报为例进行说明。

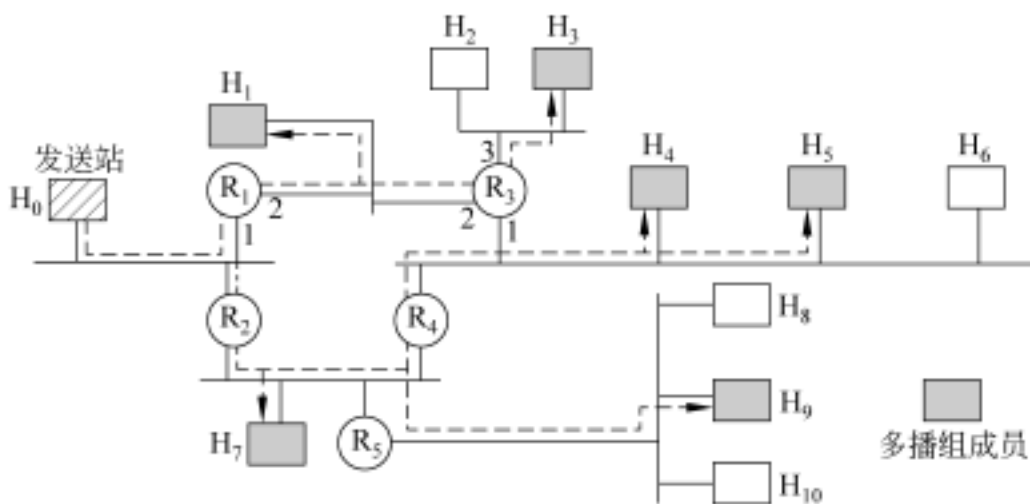


图 1-11-10 题 11-28 多播网络图

解答: RPF 的逆向路径转发处理方法是:当多播数据报到达时,记住其输入端口,然后路由器将提取多播数据报的源网络地址,反过来把它作为目的网络地址在单播路由表中查找,在匹配的表项中找到对应的转发端口,如果这个端口与数据报的输入端口一致,路由器就由除外该端口的所有其他端口都转发一个多播数据报副本;如果不一致,则丢弃该数据报。

下面以图 1-11-10 为例说明 RPF 算法。图中源站 H₀ 发送多播数据报。R₁ 接收到由 H₀ 发来的数据报后,记住其输入端口是连接了 H₀ 和 R₂ 的端口 1,然后将 H₀ 的网络地址反过来作为目的地址在本地单播路由表中进行查找,找到了对应的转发端口也是端口 1,与输入端口一致,它就从除外该端口 1 的另一个端口 2 转发一个多播数据报副本。R₃ 接收到由 R₁ 转发的数据报后,记住其输入端口为连接 R₁ 和 H₁ 的端口 2,然后将 H₀ 的网络地址反过来作为目的地址在本地单播路由表中进行查找,找到它对应的端口也是端口 2,与输入端口一致。R₃ 就从除外该端口的其他的两个端口即端口 1 和 3 都转发一个多播数据报副本。如果 R₃ 接收到由 R₄ 转发的 H₀ 的数据报,那么在单播路由表中查找到的到 H₀ 的转发端口与数据报的实际到达端口就不一致,R₃ 将丢弃该多播数据报。

11-29 IPv6 和 IPv4 兼容吗? IPv6 和 Internet 上层的 TCP、UDP 兼容吗? IPv6 和 IPv4 相比,主要的改进是什么?

解答: IPv6 和 IPv4 不兼容,但它与上层的 TCP、UDP 协议兼容。

IPv6 和 IPv4 相比,主要的改进如下:

大大地扩充了地址空间,多级地址结构,无类别地址。IPv6 地址增大到了 128 比

特,增加了地址的层次。

新的简化的首部格式。IPv6 使用一种新的数据报格式,首部由 IPv4 的 13 个字段减少到 8 个字段,使用了固定长度的首部和扩展首部。

简化了协议,加快了数据报的转发的速度。例如,取消了首部检验和字段,改进了分片机制,只在源站进行分片。

对流的支持。流是特定源和目的之间的数据报序列,IPv6 报头中有专门的流标签域。路由器根据流标签对流中的数据报进行同样的处理,加快了数据报的处理速度。IPv6 同时定义了流的优先级,以支持不同种类的业务需求,提供 QoS 支持。

安全功能。IPv6 将 IP 安全(IPsec)的认证首部 AH 和封装安全净荷 ESP 作为标准配置,规定了身份认证扩展首部和封装安全净荷扩展首部,来保证信息在传输中的安全。

即插即用功能。计算机接入 Internet 时可自动获取 IP 地址。

- 11-30 IPv6 的地址长度是多少?地址空间有多大?
- 解答: IPv6 的地址长度是 128 比特,IPv6 的地址空间可包容 3.4×10^{38} 个地址。粗略地算,可以让地球上每个人都拥有大约 6.3×10^{28} 个 IP 地址,比全部的 IPv4 地址空间还要大 1.4×10^{19} 倍。可见,IPv6 的地址空间是何等之巨大。
- 11-31 IPv6 聚集全球单播地址的用途是什么?它的结构如何?说明各字段的意义。
- 解答: IPv6 聚集全球单播地址用来给全世界接于 Internet 上的主机分配单播地址,其结构如图 1-11-11 所示。

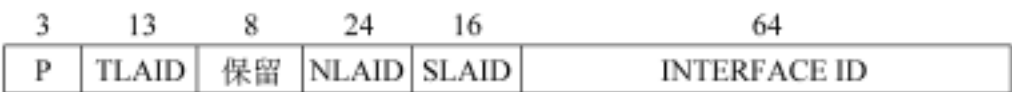


图 1-11-11 IPv6 聚集全球单播地址结构

如图所示,聚集全球单播地址包含 6 个字段,除 8 比特的保留字段外,分别是:

- P:前缀(prefix),3 比特,001,表示是聚集全球单播地址;
- TLA ID:顶级聚集(Top-Level Aggregation)标识,13 比特;
- NLA ID:次级聚集(Next-Level Aggregation)标识,24 比特;
- SLA ID:地点级聚集(Site-Level Aggregation)标识,16 比特;
- INTERFACE ID:接口标识,64 比特。

IPv6 将聚集全球单播地址划分了 TLA、NLA 和 SLA 三个段来标识网络。

TLA 一般是一个全球顶级 ISP,13 比特的 TLA ID 限制它们不超过 8 192 个。一个 TLA 连接一组二级 ISP。

TLA 之下的 NLA 可以由顶级 ISP 再进一步划分层次。比如一个顶级 ISP 可以拿出 NLA 中前面的若干比特标识其网络的下面一层或多层编号(二级或多级 ISP)。NLA 的最后一个层次标识用户地点(site),一个地点可以包含用路由器连接的众多的子网。

16 比特 SLA ID 一般是分配给用户地点中的子网。用户也可以在 SLA 上创建层次结构,比如拿出前面的 n 比特作为前缀标识子网群组,而剩余的 $16-n$ 比特标识群组中的

各个特定子网。

IPv6 单播地址的低位 64 比特标识特定的网络接口。64 比特的 IPv6 地址后缀足以适应物理地址的直接编码。选择 64 比特的原因是基于 IEEE802.1-64 地址格式规范。

11-32 IPv6 地址使用什么记法表示？该记法中还采用了什么规定使它更为简便和实用？试举例说明。

解答：IPv6 使用冒分十六进制记法(简称为 colon hex) 标记地址,它把每 16 比特的量用十六进制值表示,各量之间用冒号分隔。例如: 691E: 8032: FAF0: 3FC0: 0: 5180: 960A: 22, 其中 0000 和 0022 简记为 0 和 22,前面的 0 省略了。为进一步简化和方便使用,冒分十六进制记法还采用以下两种技术:

零压缩,即多个连续的零可以用一对冒号来代替,例如: F506: 0: 0: 0: 0: 0: 0: B61 可以写成如下简洁形式: F506:: B61。IPv6 规定,在一个 IPv6 地址中只能使用一次零压缩。

冒号十六进制记法可以和点分十进制记法后缀联合使用。这种结合表示方法在 IPv4 向 IPv6 的过渡阶段特别有用。例如,下面是一个合法的冒分十六进制记法: 0: 0: 0: 0: 0: 0: 0: 192 . 54 . 12 . 67。再使用零压缩即可得出: :: 192 . 54 . 12 . 67。

另外,CIDR 斜线表示法在 IPv6 地址表示中仍然适用。

11-33 IPv4 数据报首部中的“协议”字段的作用是什么？

解答：IPv4 数据报首部中的协议字段表示创建数据报数据区数据的高级协议的类型,比如 TCP 为“6”、UDP 为“17”、ICMP 为“1”等。IP 数据报中的协议号将 IP 层协议与上面的传输层及使用它的本层协议绑定在一起,以复用 IP 协议,其作用类似于 DIX 以太网帧的类型字段,它将数据链路层的以太网和网络层的协议绑定在一起。协议类型代码是由一个中央管理机构管理的,在整个 Internet 范围内全局一致。

11-34 为了简化 IPv6 地址的表达,可采用什么技术？写出下列 IPv6 地址的简洁形式:

(1) 211B: 0052: 0000: 0000: 0000: 0000: 03DE: AF45

(2) 15CB: 0000: 0000: CD76: 0000: 0000: 0000: 0000

(3) 0000: 0000: 0000: 0000: 192 . 124 . 36 . 1

解答: (1) 211B: 0052:: 03DE: AF45

(2) 15CB: 0000: 0000: CD76:: 或 15CB:: CD76: 0000: 0000: 0000: 0000

(3) :: 192 . 124 . 36 . 1

11-35 试说明 IPv4 向 IPv6 过渡使用的双协议栈技术及存在的问题。

解答：双协议栈在 IP 层同时安装 IPv6 和 IPv4 协议,具有 IPv6 和 IPv4 两种地址,结点既可以转发 IPv6 分组也可以转发 IPv4 分组。双协议栈结点和 IPv6 结点通信时使用 IPv6 数据报和 IPv6 地址,而和 IPv4 结点通信时使用 IPv4 数据报和 IPv4 地址。双协议栈主机如何知道目的主机是采用哪一种地址呢？这可通过 DNS 域名解析系统来查询,若 DNS 返回的是 IPv6 地址,双协议栈源主机就使用 IPv6 地址,若 DNS 返回的是 IPv4 地址,双协议栈源主机就使用 IPv4 地址。

双协议栈技术中,当 IPv6 数据报就由源结点最终传输到目的结点,中间经过了

IPv6 到 IPv4 的格式转换。但数据报格式转换的过程中,却丢失了部分信息,IPv6 数据报首部的某些字段如流标签等在中间的 IPv6 到 IPv4 双协议栈结点将 IPv6 格式转换为 IPv4 格式时丢失,在逆向转换时也无法恢复,这是双协议栈技术无法避免的。

11-36 试说明 IPv4 向 IPv6 过渡使用的隧道技术。

解答:隧道技术是实现端对端的 IPv6 over IPv4 的 IPv6 数据报传输的一种可行的方法。在隧道两端使用 IPv6 到 IPv4 双协议栈结点,它们将 IPv6 数据报作为无结构无意义的数据,封装于 IPv4 数据报的净荷部分,同时将 IPv4 数据报首部“协议”字段的值置为“41”(表示净荷为 IPv6 数据报),源地址和目的地址分别置为隧道首末端结点的地址。这种数据报的封装方式即 IPv6-in-IPv4。携带了 IPv6 数据报的 IPv4 数据报,将穿过若干 IPv4 路由器组成的隧道,到达隧道的末端。在隧道的末端,进行 IPv4 数据报的解封,将 IPv6 数据报从 IPv4 数据报中剥离出来,通过 IPv6 并送往目的结点。

11-37 列表写出 / 13、/ 14、...、/ 24 CIDR 地址块的:

(1) 掩码(点分十进制形式), (2) 包含的地址数, (3) 包含的 B/ C 类网络数。

解答:/ 13、/ 14、...、/ 24 CIDR 地址块如表 1-11-7 所示,表中,包含的地址数未将全 0 和全 1 的地址除外, K = 1024。

表 1-11-7 地址块表

地址前缀长度	掩码	包含的地址数	包含的 B/ C 类网络数
/ 13	255 .248 .0 .0	512K	B 类:8 或 C 类:2 048
/ 14	255 .252 .0 .0	256K	B 类:4 或 C 类:1 024
/ 15	255 .254 .0 .0	128K	B 类:2 或 C 类:512
/ 16	255 .255 .0 .0	64K	B 类:1 或 C 类:256
/ 17	255 .255 .128 .0	32K	C 类:128
/ 18	255 .255 .192 .0	16K	C 类:64
/ 19	255 .255 .224 .0	8 K	C 类:32
/ 20	255 .255 .240 .0	4 K	C 类:16
/ 21	255 .255 .248 .0	2 K	C 类:8
/ 22	255 .255 .252 .0	1 K	C 类:4
/ 23	255 .255 .254 .0	512	C 类:2
/ 24	255 .255 .255 .0	256	C 类:1

11-38 (a) 一个单位有下面的 6 个 / 24 CIDR 地址块,试进行最大程度的路由聚合,写出聚合后的 CIDR 地址块。

- (1) 211 .98 .136 .0 / 24 (2) 211 .98 .137 .0 / 24 (3) 211 .98 .138 .0 / 24
(4) 211 .98 .139 .0 / 24 (5) 211 .98 .140 .0 / 24 (6) 211.98 .141 .0 / 24

(b) 如果这个单位再增加下面 2 个 / 24 CIDR 地址块,进行最大程度的路由聚合,写出聚合后的 CIDR 地址块。

- (7) 211 .98 .142 .0 / 24 (8) 211 .98 .143 .0 / 24

解答: (a) 这 6 个 / 24 CIDR 地址块, 聚合为两个 CIDR 地址块, 一个是: 211 .98 .136 .0/ 22, 可包含 4 个 C 类网络数, 另一个是: 211 .98 .140 .0/ 23, 可包含 2 个 C 类网络数。

(b) 增加这 2 个 / 24 CIDR 地址块后, 聚合为一个 CIDR 地址块: 211 .98 .136 .0/ 21, 可包含 8 个 C 类网络数。

11-39 描述 IP 数据报如何通过 IPOA 网络(入口路由器、ATM 网络和出口路由器所做的主要工作)。

解答: 当 IP 数据报通过 IPOA 网络, 要先后经过入口路由器、ATM 网络和出口路由器, 它们所做的主要工作如下:

(1) 首先入口路由器需要做如下处理:

根据 IP 数据报的目的地址从 IP 路由表中查找出下一站路由器的 IP 地址, 也就是 ATM 主干网边缘转发 IP 数据报的某出口路由器的 IP 地址。

入口路由器将 ATM 主干网看成是 IP 层下面的数据链路, 根据查找到的出口路由器的 IP 地址, 从 ATM 的 ARP 表中, 解析出该出口路由器的 ATM 地址。

入口路由器将得到的出口路由器的 ATM 地址与 IP 数据报一起交给 ATM 主干网。

(2) 下面由 ATM 网络进行处理:

确定通向该 ATM 目的地址的虚通道的标识符 VCI, 查表就可得到, 在发送端维持了一个从 ATM 地址到 VCI 的映射表。一般使用的是永久虚电路, 此映射表是静态的。

在该虚通道的发送端(即入口路由器)将 IP 数据报封装在 AAL5 的 PDU 中, 经 AAL 层的处理分割成 48 字节的数据单元, 再交给 ATM 层形成 53 字节的信元, 通过 ATM 主干网传输到出口路由器。

(3) 最后, 出口路由器的 AAL5 将 ATM 信元恢复为 AAL5 PDU, 取出 IP 数据报, 输出到 IP 网络。

入/ 出口路由器都是双协议栈, 它们与 ATM 主干通信使用 ATM 协议, 与 IP 网络通信使用 IP 协议。

11-40 画图并简要描述 MPLS 网络结构和 IP 分组通过 MPLS 网络的过程。

解答: 图 1-11-12 是 MPLS 网络结构和 IP 分组穿过 MPLS 网络的示意图。

图 1-11-12 中间部分为 MPLS 网络。组成 MPLS 网络的主要设备称为标记交换路由器 LSR, 它分为两类: 位于 MPLS 网络内部的为核心 LSR, 位于 MPLS 网络边缘的为边缘(LSR), 又称为标记边缘路由器(LER)。LER 对内与核心 LSR 连接, 对外与普通的 IP 路由器连接, 以便将 MPLS 网络嵌入到 Internet 之中。核心 LSR 集成了第 3 层的路由功能和第 2 层的交换功能, 路由功能使用路由协议与其他路由器交换路由信息进行路由选择, 交换功能根据 MPLS 转发表将打上标记的分组进行快速转发。

IP 分组从一侧 IP 的网络通过 MPLS 网络传送到另一侧。IP 分组在 IP 路由器 R 和 LER 之间传送使用通常的 IP 协议, 基于 IP 地址进行转发, 涉及到第 3 层。当 IP 数据报进入 MPLS 网络内部, 核心 LSR 使用标记基于 MPLS 转发表进行转发, 只涉及到第 2

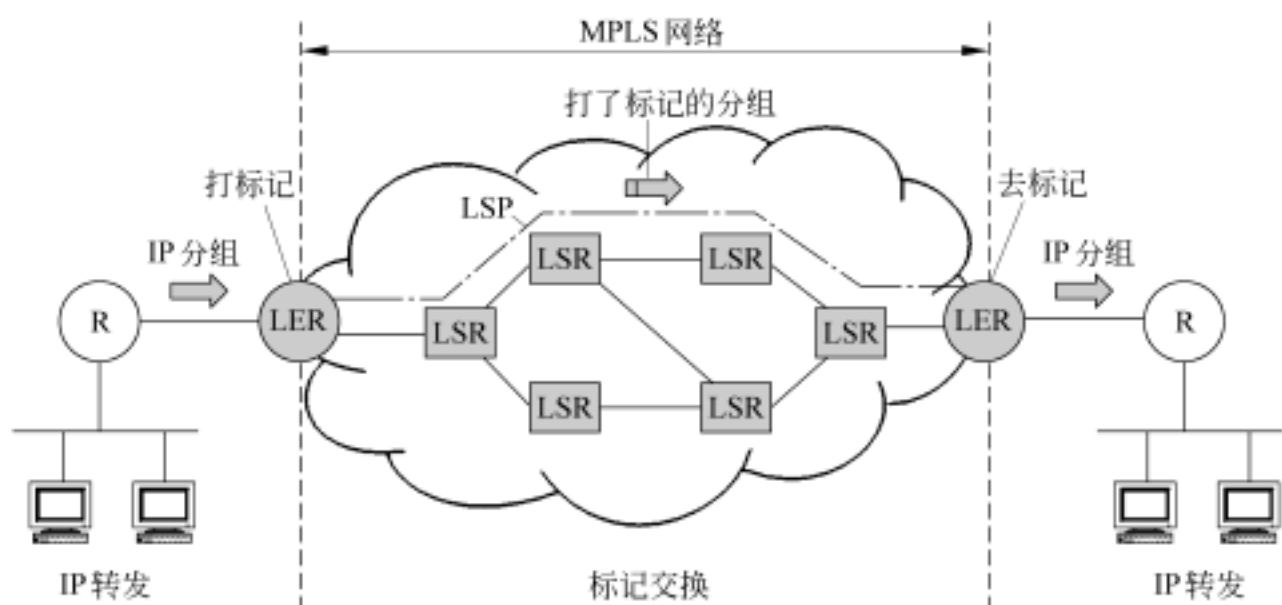


图 1-11-12 MPLS 网络结构和 IP 分组穿过 MPLS 网络示意图

层。MPLS 的标记转发方式使用 MPLS 转发表进行直接检索,确定相应的下一跳,在 LSR 输出端口用新的标记替换原标记,这样携带新标记的报文便逐跳地向目的地转发。

为了实现基于标记的转发,核心 LSR 中有一个 MPLS 转发表,它含有输入端口、输入标记和输出标记、输出端口的映射。MPLS 转发表的表项数目较一般第 3 层的路由表的表项数目少,可以通过硬件来处理,因此速度快得多。根据初始的标记和 MPLS 转发表,IP 报文就确定了在 MPLS 网络端点之间的传输路径,这种路径被称为标记交换路径(LSP)。在 MPLS 网络内部,打标记的 IP 分组沿着 LSP 从入口 LER 传输到出口 LER。

11-41 试总结路由器转发 IP 数据报时执行的主要操作。

解答:路由器在 IP 数据报转发过程中进行的处理主要包括:

- (1) 数据链路层接收帧,解封 IP 数据报,提交 IP 层软件处理。
- (2) IP 数据报首部合法性验证。根据首部提供的协议控制信息,对数据报进行验证,例如,非法的源地址或目的地址的数据报将被丢弃。首部校验和应该正确,否则数据报也将被丢弃。
- (3) IP 数据报选项处理。如果有记录路由选项、源站路由选项和时间戳选项,路由器都安作出相应的处理。
- (4) 转发路由选择。根据数据报的目的地址,查找路由表,选择数据报的下一跳(next hop)IP 地址。可能是本地交付,即直接发给与路由器直接连接在同一物理网络上的目的主机,也可能间接交付,转发给下一个路由器。对于广播和多播,要通过多个端口转发。
- (5) TTL 处理。将 IP 数据报首部中的生存时间 TTL 字段的值减 1。若 TTL 减到 0,IP 数据报将被丢弃,ICMP 协议还将向源站发出 ICMP 超时报告。
- (6) 数据报分片处理。当转发的 IP 数据报大于输出的物理网络的最大传输单元 MTU 时,路由器将进行分片处理,并修改 IP 数据报首部中的标志和片偏移两个相关字段。
- (7) 重新计算头校验和。这是因为 TTL 字段发生了变化,标志和片偏移字段也可能发生变化。

(8) 使用 ARP 得到目的站的 MAC 地址, IP 数据报封装到 MAC 帧中, MAC 寻址并将数据发出。一个 IP 数据报最终将通过物理网络接收和发出, 因此上述第 1 和第 8 项需要数据链路层和物理层的软件硬件的支持。

11-42 IP 地址由 32 个二进制位构成, 其组成结构为: 网络地址 + 主机地址。分为五类, 其中提供作为组播地址的是 (1), A 类地址用前 8 位作为网络地址, 后 24 位作为主机地址, A 类网络个数为 (2); B 类地址用前 16 位作为网络地址, 后 16 位作为主机地址, 可以实际分配的属于 B 类全部 IP 地址共有 (3) 个。采取子网划分后, IP 地址的组成结构为 (4), 子网划分导致实际可分配 IP 地址数目减少, 一个 C 类网络采用主机地址的前两位进行子网划分时, 该 C 类网络减少的地址数目为 (5)。

- (1) A . A 类地址 B . C 类地址 C . D 类地址 D . E 类地址
 (2) A . 127 B . 126 C . 255 D . 128
 (3) A . $16\,384 \times 65\,536$ B . $16\,384 \times 65\,534$
 C . $163\,828 \times 65\,534$ D . $16\,382 \times 65\,536$
 (4) A . 网络地址 + 子网地址 + 主机地址
 B . 网络地址 + 子网络接口地址 + 主机地址
 C . 网络地址 + 主机地址 + 子网络接口地址
 D . 网络地址 + 主机地址 + 子网地址
 (5) A . 6 B . 8 C . 62 D . 130

答案: C, B, C, A, D

11-43 IPv4 地址可以划分为{网络号, 主机号}两部分。在下面的地址标记中, 用 0 表示所有比特为 0, 用 1 表示所有比特为 1。以下选项中, (1) 不能作为目标地址, (2) 不能作为源地址, (3) 只能用于本机测试。

- (1) A . {0, 0} B . {127, 主机号} C . {10, 主机号} D . {网络号, 1}
 (2) A . {0, 0} B . (127, 主机号) C . {10, 主机号} D . {网络号, 1}
 (3) A . {0, 0} B . {127, 主机号} C . {10, 主机号} D . {192, 1}

答案: A, D, B

11-44 路由器是一种常用的网络互连设备, 它工作在 OSI RM 的 (1) 上, 在网络中它能够根据网络通信的情况 (2), 并识别 (3)。相互分离的网络经路由器互连后 (4)。

- (1) A . 物理层 B . 数据链路层 C . 网络层 D . 传输层
 (2) A . 动态选择路由 B . 控制数据流量
 C . 调节数据传输率 D . 改变路由结构
 (3) A . MAC 地址 B . 网络地址
 C . MAC 地址和网络地址
 D . MAC 地址和网络地址的共同逻辑地址
 (4) A . 形成了一个更大的物理网络 B . 仍然还是原来的网络
 C . 形成了一个逻辑上单一的网络 D . 成为若干个互连的子网

答案: C, A, B, D

11-45 在使用路由器 R 的 TCP/ IP 网络中,两主机 A 和 B 通过一路由器 R 互联,为主机 A 和主机 B 应用层之间提供通信服务的层是__(1)__,提供机器之间通信的层是__(2)__,具有 IP 层和网络接口层的设备__(3)__;在 A 与 R 和 R 与 B 使用不同物理网络的情况下,主机 A 和路由器 R 之间传送的数据帧与路由器 R 和主机 B 之间传送的数据帧__(4)__,A 与 R 之间传送的 IP 数据报和 R 与 B 之间传送的 IP 数据报__(5)__。

- | | | | |
|-------------------------|-----------------|------------------|-----------|
| (1) A . 应用层 | B . 传输层 | C . IP 层 | D . 网络接口层 |
| (2) A . 应用层 | B . 传输层 | C . IP 层 | D . 网络接口层 |
| (3) A . 包括主机 A、B 和路由器 R | B . 仅有主机 A、B | | |
| | C . 仅有路由器 R | D . 也应具有应用层和传输层 | |
| (4) A . 是不同的 | B . 是相同的 | | |
| | C . 有相同的 MAC 地址 | D . 有相同的介质访问控制方法 | |
| (5) A . 是不同的 | B . 有相同的 IP 地址 | | |
| | C . 有不同的 IP 地址 | D . 有不同的路由选择协议 | |

答案: B, C, A, A, B

11-46 在自治系统内部的各个路由器之间,运行的是内部网关协议 IGP。早期的 IGP 一般是__(1)__,它执行__(2)__。后来又出现了执行最短路径优先算法的 IGP。按照这种协议,每个路由器向网络中的其他路由器发布__(3)__,当路由信息改变后,路由器按照__(4)__算法更新路由表。在不同自治系统的路由器之间,运行外部网关协议 EGP,典型的 EGP 是__(5)__。

- | | | | |
|-----------------------|--------------------|-----------------|----------|
| (1) A . RIP | B . GGP | C . BGP | D . OSPF |
| (2) A . 路由选择算法 | B . 距离矢量算法 | | |
| | C . 链路状态算法 | D . 内部网关算法 | |
| (3) A . 它连接的所有链路的状态信息 | B . 它的路由表 | | |
| | C . 与它相邻的路由器的地址 | D . 所有目标结点的 URL | |
| (4) A . Diikstra | B . Ford-Fulkerson | | |
| | C . Floyd | D . Warshah | |
| (5) A . RIP | B . GGP | C . BGP | D . OSPF |

答案: A, B, A, A, C

11-47 路由信息协议 RIP 是内部网关协议 IGP 中使用得最广泛的一种基于__(1)__的协议,其最大优点是__(2)__。RIP 规定数据每经过一个路由器,跳数增加 1,实际使用中,一个通路上最多可包含的路由器数量是__(3)__,更新路由表的原则是使到各目的网络的__(4)__。更新路由表的依据如下。

若相邻路由器 A 说:“我到目的网络 Y 的距离为 N”,则收到此信息的路由器 B 就知道:“若将路由器 A 选为到网络 Y 的下一跳,则我到网络 Y 的距离为__(5)__”。

- | | | | |
|------------------|--------------|------------|---------|
| (1) A . 链路状态路由算法 | B . 距离矢量路由算法 | | |
| | C . 集中式路由算法 | D . 固定路由算法 | |
| (2) A . 简单 | B . 可靠性高 | C . 速度快 | D . 功能强 |
| (3) A . 1 个 | B . 16 个 | C . 15 个 | D . 无数个 |

- (4) A . 距离最短 B . 时延最小 C . 路由最少 D . 路径最空闲
(5) A . N B . N - 1 C . 1 D . N + 1

答案: B, A, C, A, D

11-48 ICMP 协议属于 TCP/ IP 网络中的 (1) 协议, ICMP 报文封装在 (2) 协议数据单元中传送, 在网络中起着差错报告和拥塞控制的作用。ICMP 的 ping 程序中使用 (3) 报文, 以探测目标主机是否可以到达。如果在 IP 数据报传送过程中, 发现生命期(TTL)字段为零, 则路由器发出 (4) 报文。如果网络中出现拥塞, 则路由器产生一个 (5) 报文。

- (1) A . 数据链路层 B . 网际层 C . 传输层 D . 会话层
(2) A . IP B . TCP C . UDP D . PPP
(3) A . 地址掩码请求/ 响应 B . 回应请求/ 应答
 C . 信息请求/ 响应 D . 时间戳请求/ 响应
(4) A . 超时 B . 路由重定向 C . 源端抑制 D . 目标不可到达
(5) A . 超时 B . 路由重定向 C . 源抑制 D . 目标不可到达

答案: B, A, B, A, C

11-49 IPv6 是下一代 IP 协议。IPv6 的基本报头包含 (1) 个字节。基本报头中的 (2) 字段指明了一个特定的源站向一个特定目的发送的分组序列, 各个路由器要对该分组序列进行特殊的资源分配, 以满足应用程序的特殊传输需求。一个数据流由 (3) 指定。在 IPv6 中, 地址被扩充为 128 位, 并且为 IPv4 保留了一部分地址空间。按照 IPv6 的地址表示方法, 以下地址中属于 IPv4 地址的是 (4)。

- (1) A . 16 B . 32 C . 40 D . 60
(2) A . 净荷长度 B . 流标号 C . 下一个报头 D . 跳数限制
(3) A . 源地址、目标地址和流名称 B . 源地址、目标地址和流标号
 C . 源地址、端口号和流标号 D . MAC 地址、端口号和流标号
(4) A . 0000:0000:0000:0000:0000:FFFF:1234:1180
 B . 0000:0000:0000:1111:1111:FFFF:1234:1180
 C . 0000:0000:FFFF:FFFF:FFFF:FFFF:1234:1180
 D . FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:1234:1180

答案: C, B, B, A

11-50 给定的 IP 地址为 192 . 55 . 12 . 120, 子网掩码是: 255 . 255 . 255 . 240, 那么子网号是 (1), 子网的广播地址是 (2)。如果主机地址的前十位用于子网, 那么 184 . 231 . 138 . 239 的子网掩码是 (3)。如果子网掩码是 255 . 255 . 192 . 0, 那么下面主机 (4) 必须通过路由器才能与主机 129 . 23 . 144 . 16 通信。

- (1) A . 192 . 55 . 12 . 112 B . 192 . 55 . 12 . 120
 C . 192 . 55 . 12 . 120 D . 192 . 55 . 12 . 0
(2) A . 255 . 255 . 255 . 255 B . 192 . 55 . 12 . 127
 C . 192 . 55 . 12 . 120 D . 192 . 55 . 12 . 112
(3) A . 255 . 255 . 192 . 0 B . 255 . 255 . 224 . 0

- C . 255 .255 .255 .224

(4) A . 129 .23 .191 .21

C . 129 .23 .130 .33
- D . 255 .255 .255 .192

B . 129 .23 .127 .222

D . 129 .23 .148 .127

答案: A, B, D, B

11-51 网络地址为 192 .168 .35 .0,掩码为 / 28,这个网络中可用的子网数和主机数是_____。

- A . 6 个子网/ 64 台主机

C . 14 个子网/ 14 台主机
- B . 14 个子网/ 32 台主机

D . 30 个子网/ 64 台主机

答案: C

11-52 如图 1-11-13 所示为某公司网络分布,公司获得的网段为 168 .111 .0 .0 。如何确定子网掩码,才能满足目前需求而又使得公司能够进一步划分出最多的子网 ?

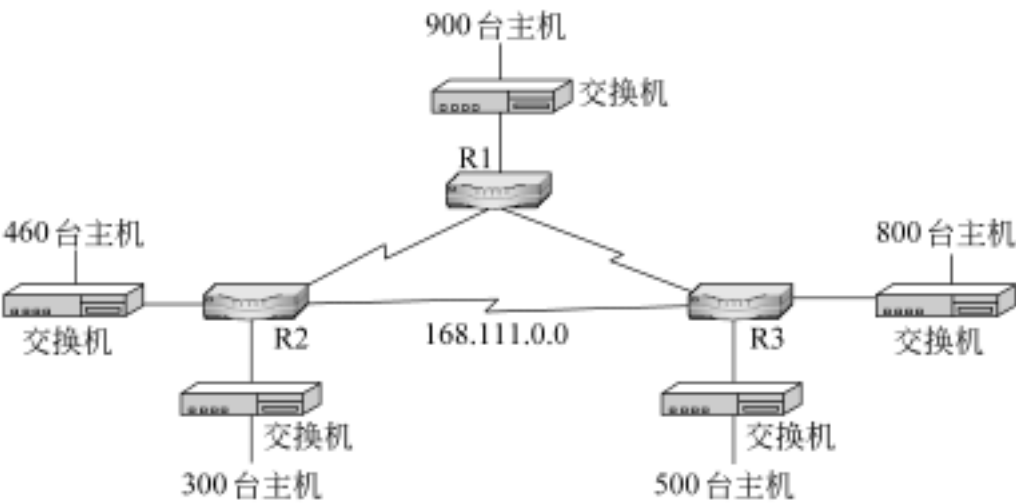


图 1-11-13 某公司网络分布图

- A . 255 .255 .224 .0

B . 255 .255 .240 .0

C . 255 .255 .248 .0
- D . 255 .255 .252 .0

E . 255 .255 .254 .0

F . 255 .255 .255 .0

答案: D

11-53 如图 1-11-14 所示,如何配置主机 B 方可与主机 C 通信 ?

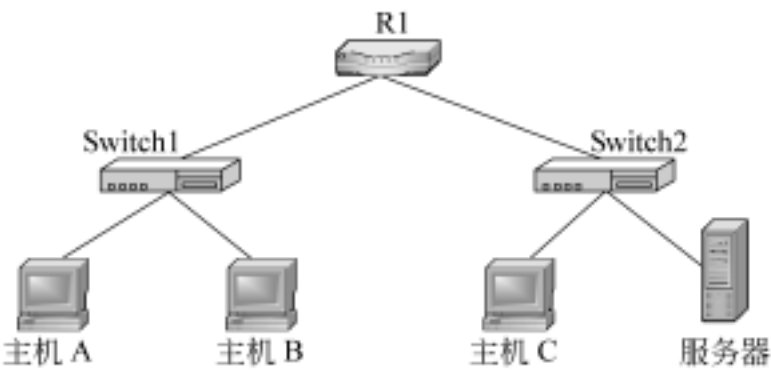


图 1-11-14 题 11-53 问题图

- A . 与 Switch 1 相连的 RTA 路由器的 MAC 地址

B . 一个惟一的 IP 地址

D . 默认路由地址

F . 局域网的子网掩码
- C . Switch 1 的 IP 地址

E . Host C 的 MAC 地址

答案: B, D, F

11-54 设有 A,B,C,D 四台主机都处在同一个物理网络中,A 主机的 IP 地址是 193 .155 .12 .112,B 主机的 IP 地址是 193 .155 .12 .120,C 主机的 IP 地址是 193 .155 .12 .176,D 主机的 IP 地址是 193 .155 .12 .222。共同的子网掩码是 255 .255 .255 .224。请回答:

- (1) A,B,C,D 四台主机之间哪些可以直接通信? 哪些需要通过设置路由器才能通信? 请画出网络连接示意图,并注明各子网地址。
- (2) 若要加入第五台主机 E,使它能与 D 主机直接通信,其 IP 地址的设定范围应是多少?
- (3) 不改变 A 主机的物理位置,将其 IP 地址改为 192 .155 .12 .168,试问它的定向广播地址和本地广播地址各是多少? 若使用本地广播地址发送信息,请问哪些主机能够收到?
- (4) 若要使主机 A,B,C,D 在这个网上都能直接相互通信,可采取什么办法?

解答: (1) 如图 1-11-15 所示:

- A、B 两台主机之间可以直接通信。
- A、B 与 C 之间通过路由器方能通信。
- A、B 与 D 之间通过路由器方能通信。
- C 与 D 之间通过路由器方能通信。

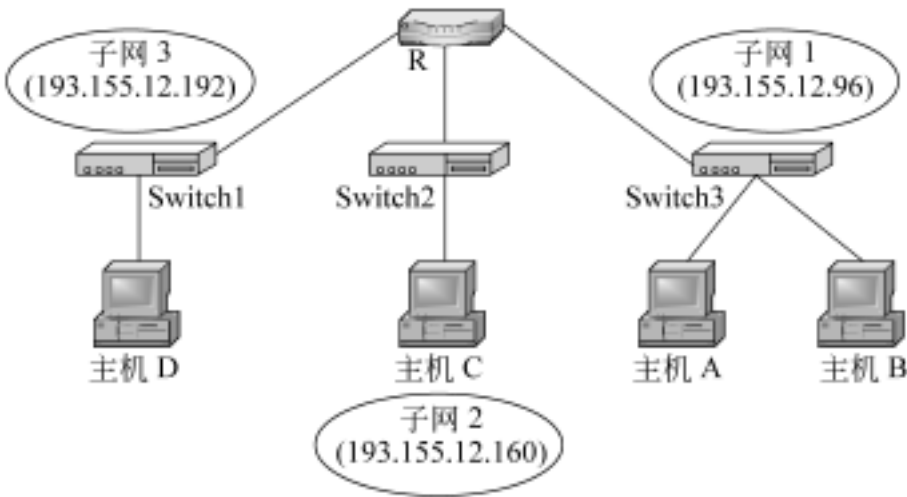


图 1-11-15 题 11-54 解答图

- (2) IP 地址的范围是 193 .155 .12 .193 至 193 .155 .12 .221。
- (3) 定向广播地址是 193 .155 .12 .191,本地广播地址是 255 .255 .255 .255,若使用本地广播地址 255 .255 .255 .255 发送信息,B 主机可以接收。
- (4) 将子网掩码改为 255 .255 .255 .0(即 C 类地址的默认值)。

11-55 某学校拟组建一个小型校园网,具体设计如下:

1. 设计要求

- (1) 终端用户包括: 48 个校园网普通用户;一个有 20 个多媒体用户的办公室;一个有 45 个用户的多媒体教室(性能要求办公室)。
- (2) 服务器提供 Web、DNS、E-mail 服务。

- (3) 支持远程教学,可以接入互联网,具有广域网访问的安全机制和网络管理功能。
 - (4) 各楼之间的距离为 550m。
- 2 . 可选设备(见表 1-11-8)

表 1-11-8 可选设备表

设备名称	数量	特 性
交换机 Switch1	1 台	具有两个 100BaseTX 端口和 24 个 10BaseT 端口
交换机 Switch2	2 台	各具有两个 100M 快速以太网端口(其中一个 100BaseTX、一个 100BaseFX)和 24 个 10BaseT 端口
交换机 Switch3	2 台	各配置 2 端口 100BaseFX 模块、24 个 100 BaseTX 快速以太网端口
交换机 Switch4	1 台	配置 4 端口 100BaseFX 模块、24 个 100BaseTX 快速以太网端口,具有 MIB 管理模块。
路由器 Router1	1 台	提供了对内的 10/ 100M 局域网接口,对外的 128K 的 ISDN 或专线连接,同时具有防火墙功能。

- 3 . 可选介质
- 3 类双绞线、5 类双绞线、多模光纤。
- 该校网络设计方案如图 1-11-16 所示。

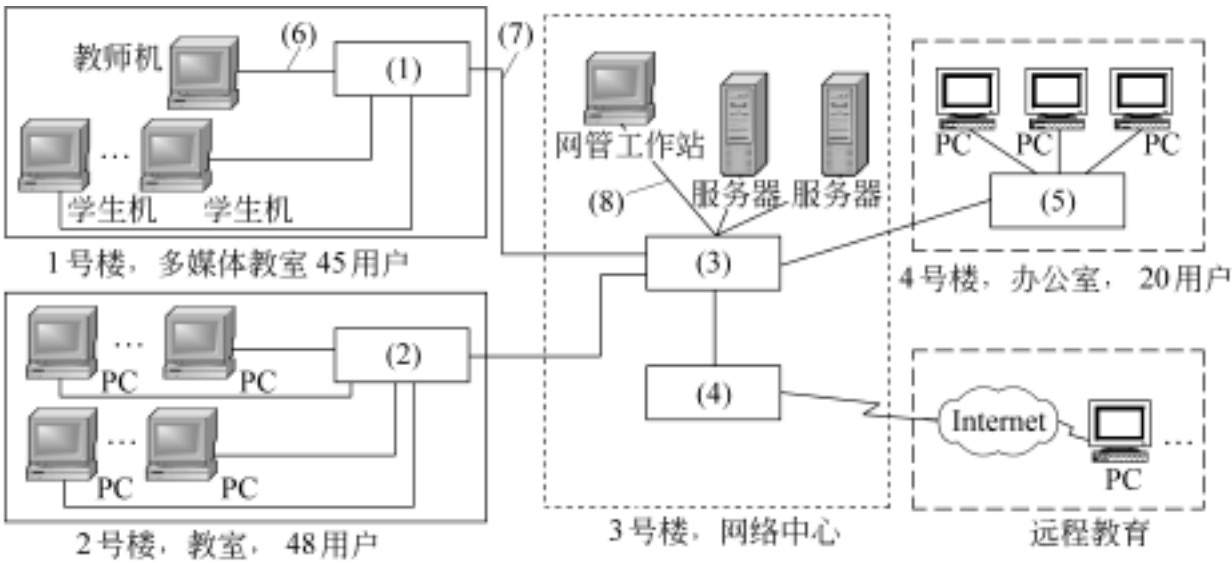


图 1-11-16 题 11-55 网络设计方案

- 问题 1: 依据给出的可选设备进行选型,将(1) ~ (5)处空缺的设备名称填写在答题纸相应位置(每处可选一台或多台设备)。
- 问题 2: 填写(6) ~ (8)处空缺的介质(所给介质可重复选择)。
- 解答: 问题 1:
- (1) 两台交换机 Switch3。
 - (2) 一台交换机 Switch1 和一台交换机 Switch2。
 - (3) 一台交换机 Switch4。
 - (4) 一台路由器 Router1。

(5) 一台交换机 Switch2。

问题 2:

(6) 5 类双绞线

(7) 多模光纤

(8) 5 类双绞线

11-56 某网络结构如图 1-11-17 所示,如果路由器 A 与网络 1 之间的线路突然中断,按照 RIP 路由协议的实现方法,路由表的更新时间间隔为 30s,中断 30s 后路由器 B 的路由表 1(见表 1-11-9)和中断 500s 后路由器 B 的路由表 2(见表 1-11-10)如下。

注: 若到达目的网络不需转发或目的网络不可达,用“ - ”来表示“下一站地址”;
当目的网络不可达时,“跳数”为 16。

请填充中断 30s 后路由器 B 的路由表 1 和中断 500s 后路由器 B 的路由表 2。



图 1-11-17 题 11-56 网络结构图

表 1-11-9 路由器 B 的路由表 1

目的网络	下一站地址	跳数
10 0 0 .0	(1)	(2)
20 0 0 .0	-	0
30 0 0 .0	-	0
40 0 0 .0	(3)	(4)

表 1-11-10 路由器 B 的路由表 2

目的网络	下一站地址	跳数
10 0 0 .0	(5)	(6)
20 0 0 .0	(7)	(8)
30 0 0 .0	(9)	(10)
40 0 0 .0	30 0 0 .1	1

答案:

- (1) 30 0 0 .1
- (2) 3
- (3) 30 0 0 .1
- (4) 1
- (5) -
- (6) 16
- (7) -
- (8) 0
- (9) -
- (10) 0

第 12 章

传输层

12-1 简要说明 TCP/ IP 传输层的作用。它主要包含哪两个协议？它们的主要特点是什么？

解答：TCP/ IP 传输层为应用进程提供一条端到端的逻辑信道，为应用进程提供数据传输服务。传输层的一个重要目的是进一步加强底层网络的数据传输服务，传输层在不可靠的 IP 服务基础上，提高传输的可靠性。

TCP/ IP 传输层有两个并列的协议：传输控制协议(TCP)和用户数据报协议(UDP)。一般，TCP 和 UDP 共存于互联网的传输层。

TCP 使用 IP 提供面向连接的可靠的传输服务。TCP 在传输前要建立连接。一般 TCP 用于一次传输要交换大量报文的情形。为了提供可靠的传输服务，TCP 采取了诸多措施，如差错控制、流量控制和拥塞控制等。

UDP 使用 IP 提供无连接的不可靠但效率高的传输服务。UDP 比 TCP 简单得多。UDP 适用于一次传输少量信息的情况。它的可靠性由上层的应用程序提供。UDP 的价值在于其效率高，当底层通信子网相当可靠时，就更为适宜。

12-2 简述协议端口及其作用。有哪两类协议端口？它们如何分配和管理？

解答：和 OSI 类比，协议端口(简称端口)相当于传输层与上面应用层接口处的服务访问点 TSAP。端口是一种抽象的软件结构，包括一些数据结构和输入、输出缓冲队列，容纳传输层和该端口所对应的应用进程之间交换的数据。为了标识不同的端口，每个端口都拥有一个叫做端口号的整数标识符。

TCP/ UDP 使用端口与上层的应用进程交互，端口标识了应用层中不同的进程。传输层的 TCP/ UDP 要和应用层的多个进程交互，通过端口机制提供了复用和解复用的功能。

TCP/ UDP 将端口分为两大类：一类是保留端口，一类是自由端口。周知端口，也称保留端口，以全局方式进行统一分配，并公之于众。保留端口保留给服务器进程使用，每一种标准的服务器都分配有一个全局公认的端口号，号码为 0 ~ 1023 的端口才能作为保留端口，由 Internet 名字和号码分配公司 ICANN 管理。自由端口以本地方式进行分配，用户可自由使用。当某一进程与远地的进程通信之前，首先要在本地申请一个自由端口，然后使用周知端口与远地服务器进行通信。号码为 1024 及以上的端口都能作为保留端口。

12-3 UDP 用户数据报报头共几个字节？哪几个字段？为什么不包含目的地址和

源地址？

解答：UDP 用户数据报格式非常简单，报头只有 8 个字节，包含 4 个字段：

源端口 发送端 UDP 端口，当不需要返回数据时，该域为 0；

目的端口 接收端 UDP 端口；

长度 UDP 数据报总长度，以字节为单位，最小值为 8(报头长)；

校验和 UDP 校验和是一个可选域，如果此域为“0”就表示不计算校验和。

UDP 数据报中不指定源站和目的站的 IP 地址，因为传输层只需识别端口，不用识别主机，识别主机的任务由网际层完成。

12-4 UDP 用户数据报的伪报头的作用是什么？为什么称为伪报头？UDP 提供了什么样的可靠性措施？

解答：伪报头是 UDP 计算校验和使用的，计算校验和时，除 UDP 用户数据报本身进行计算外，伪报头也参与计算，它补充了目的站 IP 地址和源站 IP 地址。伪报头参与校验和的计算是为了验证 UDP 数据报是否传到正确的目的地(IP 地址加端口号)。

伪报头并不是 UDP 数据报的有效成分，只是计算校验和时临时与 UDP 用户数据报组合在一起，校验和计算之后就丢弃，并不被传送，所以称为伪报头。

UDP 校验和是 UDP 提供的传输可靠性的唯一手段，而且它还是可选的。当选择进行 UDP 校验和计算时，若校验和出现差错，UDP 也没有超时重传等差错控制机制，而只是交与上层处理。另外，UDP 是无连接的，也没有流量控制和拥塞控制等可靠性措施。

12-5 什么是 TCP 的数据流和报文段？TCP 对什么进行编号？TCP 采用什么确认的方式？TCP 的确认序号是什么意思？

解答：TCP 的数据流，指的是字节的无结构的序列，TCP 提供的是面向连接的可靠的流传输。为了便于每次的传输，又把数据流划分为若干个段，称为报文段，每个报文段作为 TCP 的协议数据单元 PDU 封装到一个 IP 数据报中在网上传输，报文段到达目的站后，TCP 再将它们组装为原来的数据流。

TCP 对数据流按字节编上序号，而不是按报文段编序号。TCP 将传输的报文段所携带数据的第一个字节的序号放在报文段首部的序号字段中。

TCP 采用累计确认方式，收方确认已正确收到的、积累的连续数据流。在确认报文段首部的确认序号字段中，收方写入的确认序号比正确收到的字节序列的最高序号多 1，表明了它前面的数据流已正确收到，指示了所期望接收的下一个报文段的起始序号。

12-6 设 TCP 的最大报文段生存时间 MSL 分别为 120s 和 60s，均使用 32 比特的序号空间。问：同一 TCP 连接中在 MSL 内不出现相同序号的最大信息传输速率分别是多少？TCP 采取什么措施避免同一连接上在 MSL 内出现相同的序号？

解答：32 比特的序号的空间，序号循环一周要发送 2^{32} 个字节，若 TCP 的最大报文段生存时间 MSL 为 120s，则同一 TCP 连接上在 MSL 内不出现相同序号的最大信息传输速率是： $(2^{32} \times 8)\text{b} \div 120\text{s} = 286\text{Mb/s}$ 。

同样方法可得：若 TCP 的最大报文段生存时间 MSL 为 60s，则同一 TCP 连接中在 MSL 内不出现相同序号的最大信息传输速率是 572Mb/s 。

序号空间不变时，数据传输速度越高序号循环一周的时间越小，就可能小于 TCP 规

定的 MSL。为了同一 TCP 连接上在 MSL 内不产生相同的序号, TCP 使用时间戳选项, 发方 TCP 在每个发送的报文段首部插入 32 比特的时间戳, 收方将收到的时间戳也插入到 ACK 报文段中作为确认。这样, 32 比特的时间戳和 32 比特的序号组合在一起就可以避免序号循环产生的问题。

12-7 理论上光纤可以达到 75Tb/s 的信息传输速率。如果 TCP 的最大报文段生存时间 MSL 仍取 120s , 问: 为避免出现相同序号的问题而扩大序号空间, TCP 应该使用至少多少的比特的序号空间? 对于光纤的这一速率, 如果仍使用 32 比特的序号空间, MSL 最大有多大?

解答: 由 $(2^n \times 8)\text{b} \div 120\text{s} = 75\text{Tb/s}$, 得 $2^n = (75 \times 10^9 \times 120) \div 8 = 1.125 \times 10^{12}$, n 约等于 40, 为避免出现相同序号的问题, TCP 应该使用至少 40 比特的序号空间。

如果仍使用 32 比特的序号空间, MSL 最大只有 $(2^{32} \times 8)\text{b} \div 75\text{Tb/s} = 0.46\text{s}$ 。

12-8 在 TCP 连接上, 主机的发送窗口 64K 字节, 线路的往返时间是 50ms。问:

(1) 主机能达到的最大信息传输速率是多少?

(2) 若在此线路上使用窗口比例因子选项实现 155Mb/s 的信息传输速率, 窗口比例因子至少应该选多大? 扩展后的窗口可达多少字节?

解答: 在 TCP 连接上, 发方只有经过一个往返时间 RTT 才能发出数据并收到确认, 之后才能向前滑动发送窗口并继续发送; 又因为主机的发送窗口最大值为 64K (65 536) 字节, 因此, TCP 最多只能在 RTT 时间内发送 64K 字节的数据, 能达到的最大信息传输速率是: $(65\,536 \times 8)\text{b} \div 50\text{ms} = 10.5\text{Mb/s}$ 。

若在此线路上使用窗口比例因子选项实现 155Mb/s 的信息传输速率, 设窗口比例因子为 n , 则:

$(65\,536 \times 2^n \times 8)\text{b} \div 50\text{ms} = 155\text{Mb/s}$, 因此, $2^n = 14.8$, 取窗口比例因子 $n = 4$ 。扩展后的窗口可达: $64\text{K} \times 2^4 = 1024\text{K}$ 字节。

12-9 通告窗口设置于何处? 它表示什么意思? 它反映了什么信息? 在 TCP 起流量控制中它起什么作用?

解答: 通告窗口设置于收方报文段的窗口字段, 单位为字节。

通告窗口告诉发方: 在收到收方的下一次确认之前, 发方能够发送的数据的长度不能超过此窗口的大小。如果通告窗口为 n , 则发方能够发送的数据流是从确认序号开始的 n 个字节。

通告窗口实际上反映了收方目前可用的接收缓冲区的大小, 即它的接收能力。

通告窗口在 TCP 流量控制中反馈了收方当前的接收能力, 发方根据通告窗口反馈的值调节自己的发送窗口的大小, 从而实现流量控制。

12-10 在 TCP 连接上, 主机 A 向主机 B 传输 1 100 字节的数据, 双方 TCP 协商的 MSS 为 300 字节, 主机 B 通告的窗口 WIS 为 1 200 字节, 又设主机 A 和 B 的初始序号 ISN 分别为 1 000 和 2 000, 参照主教材图 12.7 和图 12.13(b) 画出主机 A 和主机 B 建立连接—传输数据(A → B)—关闭连接的全过程示意图, 图中标明重要的协议参数。

解答: 见图 1-12-1。

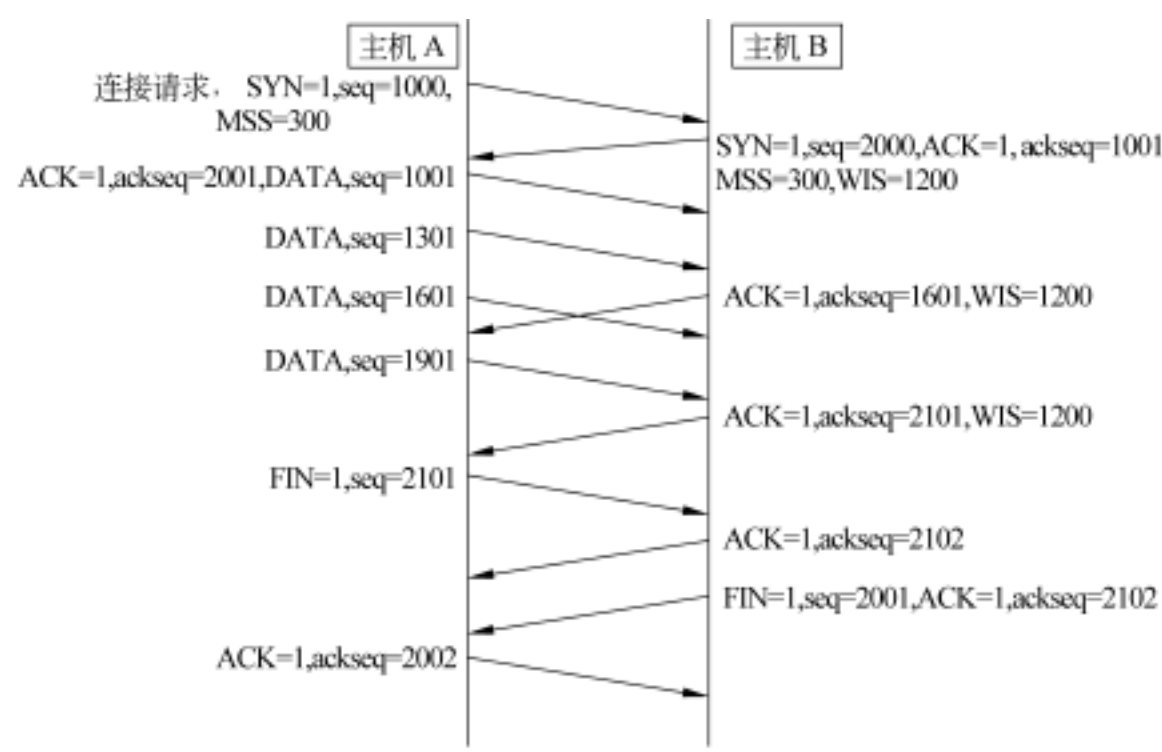


图 1-12-1 题 12-10 解答图

12-11 TCP 为什么使用坚持定时器？

解答：当收方接收缓冲区满时 TCP 使用 0 通告窗口值停止连接上的通信流量。但使用中,滑动窗口的 0 通告值可能带来一个问题。考虑下述情况:收方发出了一个 0 通告窗口,发方将发送窗口调整为 0,暂时停发送并等待。之后,收方应用程序从缓冲区取走了数据,收方发送一个非 0 的窗口通告,通知发方又可以发送数据了。但这一非 0 通告的报文丢失了,发方和收方都等待对方的动作,因而造成了死锁。

为此,TCP 使用坚持定时器解决这种死锁现象。当接收到 0 通告值的确认后,发方启动坚持定时器,当定时器设定的时间到,发方发送一个探测报文段。收方对探测报文段的响应包含了通告窗口的通告值。如通告值不为 0,则发方调整发送窗口进行发送;若通告值为 0,则重新设定坚持定时器重复上述过程。

12-12 简述拥塞控制与流量控制产生的原因和所解决的问题。它们解决问题的根本途径是什么？

解答：如果收方的接收缓冲区小和处理能力低都会造发方的数据流“淹没”收方的接收缓冲区,使数据丢失,流量控制用来保证发送数据在任何情况下都不会“淹没”收方的接收缓冲区。TCP 的流量控制是端到端的,不涉及中间路由器。

拥塞是分组交换网络共同的问题。产生拥塞的原因是网络中一个或若干个路由器的数据报负载相对它的处理能力过重,路由器不得不将过多的数据报放在缓存队列中排队等待转发,造成严重的传输时延。路由器的缓存能力总是有限的,严重情况下,数据报将充满缓存,于是路由器不得不丢弃数据报。TCP 的拥塞控制要涉及到中间的路由器。

TCP 流量控制和拥塞控制的根本的措施是减慢源发站的发送速率,即源抑制。

12-13 TCP 发现拥塞的途径是什么？

TCP 可以通过以下途径发现拥塞发生：

报文段的超时重传；

来自 ICMP 的源抑制报文；

在快速重传算法中,收到第 3 个重复的确认而不必等到重传定时器到时。

12-14 TCP 拥塞控制主要采用哪几种技术？简要解释这些技术的特点。（解释拥塞窗口和慢启动门限。）

解答：为了避免拥塞,TCP 推荐使用以下几种技术:慢启动、拥塞避免、快速重传和快速恢复。

慢启动指每出现一次拥塞,拥塞窗口都要降到 1 个报文段长度的起点,然后增加,使报文段从最小的流量开始注入到网络之中。

拥塞避免在慢启动算法之后执行,是指当拥塞窗口增大到慢启动门限值之后,就将拥塞窗口增长速率由指数增长变为加性增长,以避免再次出现拥塞。

快速重传算法中,当收到第 3 个重复的确认时,就认为报文丢失而重传报文段,而不必等到重传定时器到时,故称快速重传。

快速恢复在快速重传算法之后执行,而不是执行慢启动,TCP 不把拥塞窗口降到 1,而只降到报文段丢失时拥塞窗口的一半加 3。

拥塞窗口用于发送方的流量控制。发送窗口按下取值:发送窗口 = min(拥塞窗口,通告窗口)。当发生拥塞时,拥塞窗口将数据流量限制为小于接收方的接收能力。在未发生拥塞的稳定运行情况下,拥塞窗口和通告窗口是一致的。

慢启动门限用来分界慢启动和拥塞避免策略。用变量 ssthresh 和 cwnd 分别表示慢启动门限和拥塞窗口,则:

- 当 $cwnd < ssthresh$, 使用慢启动策略;
- 当 $cwnd > ssthresh$, 使用拥塞避免策略;
- 当 $cwnd = ssthresh$, 即可使用慢启动策略也可使用拥塞避免策略。

12-15 图 1-12-2 是采用慢启动和拥塞避免的拥塞控制策略的传输过程的例子。现假设,当进行到第 11 次传输和第 19 次传输时发生拥塞,重发定时器出现超时,其他条件和参数与图中相同。发生拥塞后,慢启动门限变为多少？参照图 1-12-2 画出采用慢启动和拥塞避免的拥塞控制策略的传输过程中拥塞窗口和慢启动门限的变化曲线。

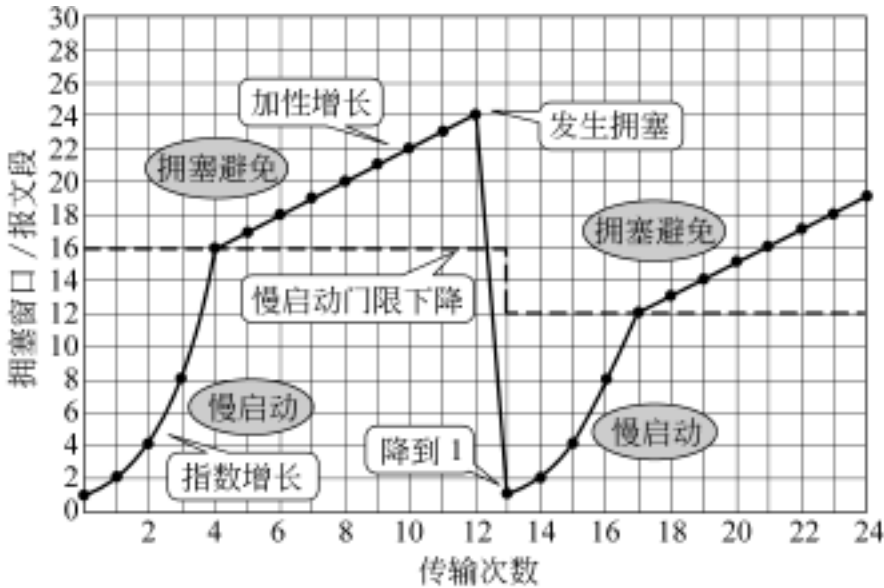


图 1-12-2 题 12-15 问题图

解答：第 11 次传输发生拥塞后,慢启动门限变为 11 个报文段。第 19 次传输发生拥塞后,慢启动门限变为 7 个报文段。拥塞窗口和慢启动门限的变化曲线如图 1-12-3 所示。

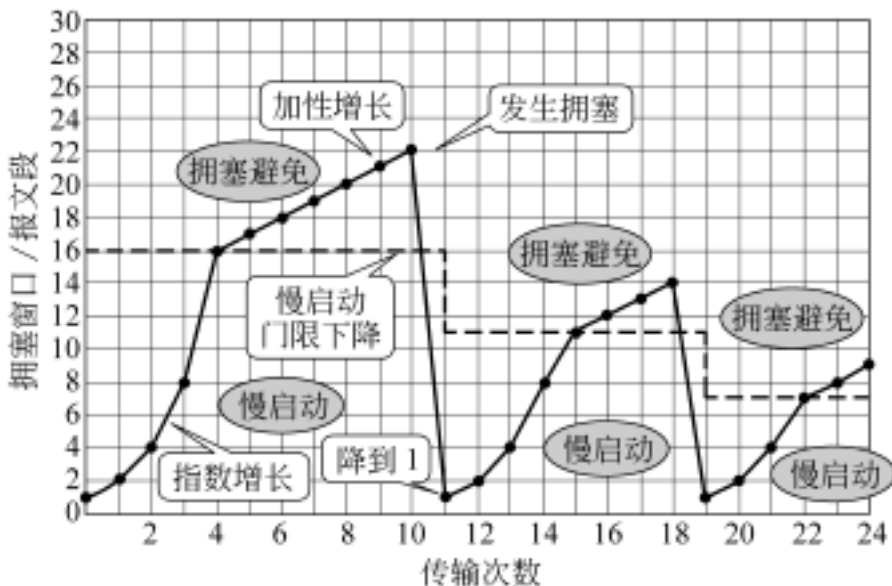


图 1-12-3 拥塞窗口和慢启动门限的变化曲线

12-16 TCP 的重传机制是保证什么性能的重要措施？UDP 具有重传机制吗？

解答：TCP 的重传机制是保证可靠性的重要措施, TCP 为应用层提供可靠的传输服务,它是 TCP 可靠性的一个重要措施。UDP 为应用层提供的是不可靠的传输服务,UDP 没有定义重传机制。

12-17 TCP 为什么要用自适应算法计算重传定时器定时时限？

解答：在 Internet 环境下,超时重传时限 RTO 不能简单地设置。Internet 环境比单纯的局域网要复杂得多。首先,同一个源站发送的报文段到不同的目的站的路径不同,报文段可能只经过一个小时延的单跳网络,也可能要经过大时延的由许多路由器连接的多跳网络,因而所需要的时间大不相同;其次,每个路由器产生的时延与网络负荷密切相关,互联网的负荷经常发生变化,网络负荷的变化使报文段在不同时间经过相同的路径所需要的时间也不同。可见,在 Internet 环境中,传输层数据报的往返时延的变化很大。因此,TCP 采用自适应算法计算重传定时器定时时限,以适应这些变化。

12-18 Karn 算法提出的原因是什么？简述 Karn 算法。

解答：在出现超时重传时,存在确认的二义性,TCP 计算样本往返时间 RTT 存在问题。发方 TCP 生成了一个报文段发送出去,由于重传定时器到时没有收到确认,又重传了一次,之后收到了确认。由于这两个报文段完全相同,确认报文也相同,发送方无法分辨出确认是对原报文段还是对重传报文段。此即确认的二义性,它可能引起错误地计算 RTT。为此提出了 Karn 算法。

Karn 算法不使用重传报文段的样本而只使用发送一次的报文段的样本计算 RTT,因此避免了确认二义性带来的问题。但这种简单的 Karn 算法也带来了新问题,因为它忽略了重传对往返时间的影响。出现重传意味着网络传输延时加大了,应该加大往返时间估计值。Karn 算法使用定时器补偿策略把超时重传的影响估计在内。

12-19 什么是最大报文段长度 MSS？选择合适的 MSS 的困难何在？如何选择？

解答：最大报文段长度 MSS 指的是 TCP 报文段所携带数据的最大长度，单位为字节，不能超过此限制。MSS 可以在 TCP 建立连接时商定。

在互联网环境中，选择合适的 MSS 是很困难的，取值过大或过小都可能会造成网络的性能变坏。选择过小的 MSS 值会造成短数据报的传输，降低网络利用率。选择大的 MSS 传输会引起 IP 软件不得不进行分片，增加了路由器的负担，而且分片越多，丢失或出错的可能就越大，因而增加了数据报重传的概率，也降低了网络的性能。

从理论上讲，TCP 报文段的最佳长度 MSS^* 可以这样得到：在 IP 数据报在从源站到目的站的路径上不被分片的前提下，它所封装的 TCP 报文段携带尽量长的数据，这个长度的最大值就是 MSS^* 。但实际上确定 MSS^* 是很困难的。这是因为互联网上的路由是动态的，随着网络拓扑和网络负载等因素的变化，一对计算机之间传输的路径可能变化，因此 MSS^* 也会随之改变。此外，最佳长度 MSS^* 还取决于低层协议数据单元首部的长度，它们也不是固定的。例如，IP 数据报有选项时， MSS^* 的长度就要减小。

TCP 选择最佳报文段长度的简单做法是选取建立连接时双方声明的 MSS 的较小者。如果一方没有声明 MSS，MSS 取默认值 536 字节。

12-20 为适应网络技术的发展，TCP 提出了新的窗口比例因子选项，原因是什么？窗口比例因子选项如何扩大窗口值？

解答：计算机网络技术的飞速发展使得当年 TCP 协议的某些规定不能适应今天的需要，TCP 仅 16 比特的通告窗口字段就限制了连接上的传输带宽。为此，TCP 规定了窗口比例因子选项，扩大通告窗口的数值。窗口比例因子双方在建立连接时商定。

16 比特的窗口字段只能通告最大 64K 字节 (65 536 字节) 的发送窗口值，发方至少经过一个往返时间 RTT 才能发出数据、收到确认，之后才能向前滑动发送窗口并继续发送。因此，TCP 在 RTT 时间内最多发送 64K 字节的数据。TCP 连接上的最大容量为数据速率 (b/s) 与 RTT(s) 的乘积，即往返时延带宽积，显然，它的值不能超过通告窗口。

当初 TCP 面对的是 56kb/s 的线路，假如 RTT 为 100ms，那么往返时延带宽积只有 $(56 \times 10^3 \times 0.1) / 8 = 700$ 字节，对于 1.544Mb/s 的 T1 线路，往返时延带宽积为 19.3K 字节，它们都小于当初 64K 字节的窗口值。现在网络带宽大大提高，比如对于带宽为 622Mb/s 的 OC-12 线路，在 100ms RTT 的假定下，其往返时延带宽积则有 $118.6 \times 64K$ 字节。这样，当初设计的 64K 字节的窗口就远不够用了，所以 TCP 对 16 比特的窗口必须进行扩展。

TCP 用窗口比例因子选项扩展窗口值。窗口比例因子表示原来 16 位的窗口值向左移位的次数，每移 1 次，窗口值翻 1 番。窗口比例因子的最大值为 14，窗口最大可扩大 $2^{14} = 16\,384$ 倍，所以扩展后的窗口可达 $16\,384 \times 64K$ 字节 = 2^{30} 字节。

12-21 在 TCP 建立连接的过程中，通信双方可以为数据传输做哪些准备工作？

解答：在三次握手建立连接的过程中，可以完成以下传输准备工作：

使每一方都确知对方存在，知道对方已准备就绪；

双方确商定了初始传输序号，确定了双方发送数据流的其始序号；

双方还可以协商一些其他通信参数，如通告窗口大小，最大报文段长度 MSS 和窗口比例因子等。

12-22 设 TCP 连接上报文段的往返时间 RTT 的初始值 $rtt(0) = 24\text{ms}$, 随后的值分别是 32, 16, 40, 28, 36ms 和 22ms。根据 TCP 的重传策略, 计算报文段的平滑往返时间 $srtt(k)$ 和重传定时时限 $rto(k) (k = 1, 2, 3, 4, 5, 6)$ 。计算中, 假设 SRTT 的初始值 $srtt(0) = rtt(0)$, RTT 和 SRTT 偏差的平滑值的初始值 $d(0) = rtt(0)/3$ 。

解答: 使用下述 3 个公式计算:

$$srtt(k) = srtt(k - 1) + 0.125(rtt(k) - srtt(k - 1)) \tag{1}$$

$$d(k) = d(k - 1) + 0.25(|rtt(k) - srtt(k)| - d(k - 1)) \tag{2}$$

$$rto(k) = srtt(k) + 4d(k) \tag{3}$$

初值, $k = 0$: $srtt(0) = rtt(0) = 24\text{ms}$, $d(0) = rtt(0)/3 = 8\text{ms}$ 。

第 1 步, $k = 1$: $rtt(1) = 32\text{ms}$,

由式(1), $srtt(1) = srtt(0) + 0.125(rtt(1) - srtt(0)) = 24 + 0.125(32 - 24) = 25$

由式(2), $d(1) = d(0) + 0.25(|rtt(1) - srtt(1)| - d(0)) = 8 + 0.25(|32 - 25| - 8) = 7.75$

由式(3), $rto(1) = srtt(1) + 4d(1) = 25 + 31 = 56$

以下各步计算方法相同, 计算结果如表 1-12-1 所示。

表 1-12-1 计算结果

步数 k	$rtt(k)$	$srtt(k)$	$d(k)$	$rto(k)$
0(初值)	24	24	8	56
1	32	25	7.75	56
2	16	23.88	7.78	55
3	40	25.90	9.36	63.34
4	28	26.16	7.48	56.08
5	36	27.39	7.76	58.43
6	22	26.72	7	54.72

12-23 下面对于 TCP 协议特征的描述哪些是正确的?

- A . 在 UDP 层之下。
- B . 用于传输 IP 错误信息。
- C . 强制重传没有被送达的数据包。
- D . 提供面向连接的传输服务。
- E . 在 TCP 头中包含目标主机的 IP 地址信息。
- F . 分割数据成为 segments 发送并在目的地重组。

答案: C, D, F

12-24 两台对等主机正在通过 UDP 协议进行通信, 在传输过程中, 一个数据报没有到达目的地。下面哪些关于数据报重传的描述是正确的?

- A . 源端的重传计时器到期之后就开始重新传输。
- B . 目的端的重传计时器到期之后就开始重新传输。

C . 是否重传数据由应用层协议控制。

D . 只有当目前数据序列号等于或高于确认序号时才重新传输。

答案: C

12-25 TCP 是互联网中的__(1)__协议,使用__(2)__次握手协议建立连接。当主动方发出 SYN 连接请求后,等待对方回答__(3)___。这种建立连接的方法可以防止__(4)___。TCP 使用的流量控制协议是__(5)___。

- | | | | |
|---------------------|-----------------|-----------------|--------------|
| (1) A . 传输层 | B . 网络层 | C . 会话层 | D . 应用层 |
| (2) A . 1 | B . 2 | C . 3 | D . 4 |
| (3) A . SYN, ACK | B . FIN, ACK | C . PSH, ACK | D . RST, ACK |
| (4) A . 出现半连接 | B . 无法连接 | C . 假冒的连接 | D . 产生错误的连接 |
| (5) A . 固定大小的滑动窗口协议 | B . 可变大小的滑动窗口协议 | | |
| C . 后退 N 帧 ARQ 协议 | | D . 选择重发 ARQ 协议 | |

答案: A , C , A, D, B

12-26 TCP 是一个面向连接的协议,它提供连接的功能是__(1)___的,采用__(2)___技术来实现可靠数据流的传送。为了提高效率,TCP 引入了滑动窗口协议,如果窗口中有的报文段丢失,重传报文段的数量最多可以__(3)___,TCP 协议采用滑动窗口协议解决了__(4)___。

- | | | | |
|----------------------|---------------|---------------|---------|
| (1) A . 全双工 | B . 半双工 | C . 单工 | D . 单方向 |
| (2) A . 超时重传 | B . 确认机制 | | |
| C . 超时重传和确认机制 | | D . 丢失重传和重复确认 | |
| (3) A . 是任意的 | B . 1 个 | | |
| C . 大于滑动窗口的大小 | | D . 等于滑动窗口的大小 | |
| (4) A . 端到端的流量控制 | B . 整个网络的拥塞控制 | | |
| C . 端到端的流量控制和网络的拥塞控制 | | | |
| D . 整个网络的差错控制 | | | |

答案: A , C, D, A

12-27 基于 TCP/IP 的互联网服务中,IP 协议提供主机之间的__(1)___分组传输服务。TCP 协议提供端到端的__(2)___报文传输服务;为了实现可靠的服务,采用超时重传和累计确认技术,并规定,确认序号为__(3)___。TCP 使用三次握手协议来建立连接,设甲乙双方发送报文的初始序号分别为 X 和 Y,甲方发送__(4)___的报文给乙方,乙方接收报文后发送__(5)___的报文给甲方,然后甲方发送一个确认报文给乙方便建立了连接。

- | | |
|--------------------------|---------------|
| (1) A . 可靠的面向连接的 | B . 不可靠的面向连接的 |
| C . 可靠的无连接的 | D . 不可靠的无连接的 |
| (2) A . 可靠的面向连接的 | B . 不可靠的面向连接的 |
| C . 可靠的无连接的 | D . 不可靠的无连接的 |
| (3) A . 上一个已接收的报文段的末字节序号 | |
| B . 下一个希望接收的报文段的首字节序号 | |

C.下一个将要发送的报文段的末字节序号

D.下一个将要发送的报文段的首字节序号

(4) A. $\text{SYN} = 1$, 序号 = X

B. $\text{SYN} = 1$, 序号 = $X + 1$

C. $\text{SYN} = 1$, 序号 = Y

D. $\text{SYN} = 1$, 序号 = $Y + 1$

(5) A. $\text{SYN} = 0$, 序号 = Y; $\text{ACK} = 1$, 确认序号 = $X + 1$

B. $\text{SYN} = 1$, 序号 = Y; $\text{ACK} = 0$, 确认序号 = $X + 1$

C. $\text{SYN} = 1$, 序号 = Y; $\text{ACK} = 1$, 确认序号 = $X + 1$

D. $\text{SYN} = 1$, 序号 = Y; $\text{ACK} = 1$, 确认序号 = X

答案: D, A, B, A, C

第 13 章

应用层

13-1 什么是 C/S 模式？什么是 B/S 模式？为什么采用 C/S 模式作为互联网应用程序间相互作用的最主要形式？

解答：C/S 模式即客户-服务器模式，客户(client)和服务器(server)分别是两个应用进程，可以位于互联网的两台不同主机上。服务器被动地等待服务请求，客户向服务器主动发出服务请求，服务器做出响应，并返回服务结果给客户，这就是 C/S 模式。

B/S 模式即浏览器-服务器模式，是一种基于 Web 的 C/S 模式。B/S 模式中，客户是浏览器，服务器是 Web 服务器。客户向服务器发出信息浏览请求，服务器向客户送回客户所要的万维网文档，以页面的形式显示在客户的屏幕上。B/S 模式的一个重要特点是平台无关性，Browser、Web Server 及主流语言 Java 和 HTML 等都可以做到与硬件平台无关。另外，B/S 模式的客户端变瘦，其功能主要是一个多媒体浏览器。

采用 C/S 模式作为互联网应用程序间相互作用的最主要形式的原因如下：

从技术方面讲，互联网上不同主机进程之间进行通信，其重要特点是主机发起通信完全是随机的。因此需要一种机制，能够适应这种随机性。C/S 模式很好地解决了上述技术问题，每次通信过程都由客户进程主动发起，而且是随机的，服务器进程从开机起就处于等待状态，随时准备对客户的请求做出及时的响应。

从实际应用方面讲，C/S 模式的重要特点是非对等性相互作用，客户请求服务，服务器提供服务。一般提供服务的计算机要比请求服务的计算机拥有更好更多的硬、软件资源和更强的处理能力。C/S 模式很好地适应了 Internet 上资源分布不均的客观现实。

C/S 模式优化了网络计算，提高了网络的利用率。客户可以请求服务器进行大型计算，比如数据库查询等，客户接收用户的查询请求，形成查询报文传给服务器，服务器执行大型数据库的查询，之后将查询结果传回给客户，客户进行结果显示，提供友好的人机界面。因此，客户和服务器分工合作，协同完成计算，网络上传输的只是简短的查询请求和结果。

13-2 什么是域名？叙述 Internet 的域名结构。什么是域名系统 DNS？

解答：域名即主机名，它用来惟一地标识连接在 Internet 上的主机，它采用层次结构，在应用层使用。

域名为层次结构，分为若干级，各级域名之间用小数点连接：

..... 三级域名 二级域名 .顶级域名

每一级域名均由英文字母和阿拉伯数字组成,不超过 63 个字符,不区分字母大小写。各级域名自左向右级别越来越高,顶级域名 TLD 在最右边。一个完整的域名总字符数目不能超过 255 个。域名系统不规定一个域名必须包含多少个级别。这样,整个 Internet 层次结构的名称空间就构成一棵命名树,根结点是无名的,根下面就是顶级域结点。

DNS 负责主机名和 IP 地址之间的转换,它是一个联机分布式数据库系统,采用客户-服务器模式。进行域名查询的机器称为域名解析器,需要时主动发起域名解析请求,域名服务器则随时准备作出响应。域名服务器的数据库中存放着它所管辖范围的主机名和 IP 地址之间的映射表,域名服务器之间又可以相互联络和协作,以便分布在 Internet 各个域名服务器数据库中的域名都能被有效地搜索。

13-3 叙述域名服务器系统的组织方式。

解答:域名服务器系统基本上是按照域名的层次进行组织的,但域名服务器系统的层次并不与域名系统的层次严格对应。

Internet 允许根据具体情况将某一域名空间划分为一个或多个域名服务器管辖区。在每个管辖区设置相应的授权域名服务器。管辖区内的主机必须在授权域名服务器处注册登记,授权域名服务器的 DNS 数据库中记录了辖区内主机的域名和 IP 地址的映射表,负责对本管辖区内的主机进行域名解析工作。

有两种授权域名服务器有特殊的名称。一种是本地域名服务器或默认域名服务器。对每个管辖区内的所有主机来说,该管辖区内的授权域名服务器称为本地域名服务器,辖区内的所有主机都知道它的 IP 地址。另一种是根域名服务器,是负责顶级域的授权域名服务器。

分散在世界各地的域名服务器形成了一个联合协作的系统,需要时域名服务器之间可以协作完成解析,为此:每个域名服务器都知道所有的根域名服务器的 IP 地址,根域名服务器知道其下属的二级域名服务器的 IP 地址,每个域名服务器又知道其下一级域名服务器的 IP 地址。

13-4 描述域名解析方式。

解答:域名解析分为两步进行:

第一步 访问本地域名服务器。当某一个应用需要将主机名映射为 IP 地址时,该应用使用域名解析器,首先请求本地域名服务器进行解析。本地域名服务器查找 DNS 数据库,如果能找到对应的 IP 地址,就放在应答报文中返回。如果本地域名服务器中不包含该域名和 IP 地址的映射,则要转入第二步;

第二步 访问非本地的其他域名服务器。先访问顶级域名对应的根服务器,根服务器不能解析时,再请求其下一级服务器,下一级服务器不能解析时,再请求下下一级服务器,……,如此进行一次自顶向下的搜索,最后找到其授权域名服务器,实现域名解析。

其中第二步域名解析又有两种方式:第一种方式称为递归解析,此时,域名服务器又是解析器,它不能解析时,就变为解析器请求其他域名服务器解析,如此递归,直至得到解析结果。第二种方式称为反复解析,由客户自己每次请求一个服务器,服务器不能解析则返回下一个服务器的 IP 地址给客户,客户反复进行解析,直至得到解析结果。

13-5 为提高域名解析的效率,DNS 采取了什么措施?

解答：为了提高解析效率，域名解析中使用了域名缓存技术。域名缓存技术是在服务器中设置一个专用的内存缓冲区，用来存放近期解析过的域名及其对应的 IP 地址的映射。于是，在服务器域名解析过程中，如果在数据库中搜索不到相关记录，则可使用域名缓存进行解析，如果域名缓存也解析不到，再访问非本地的其他域名服务器。这显然提高了解析效率。

域名缓存机制不仅用于域名服务器，也用于主机。许多主机运行一种功能很强的解析器软件，系统启动时这种解析器软件从本地域名服务器获取一个完整的域名-IP 地址映射数据库的副本，并维护一个近期使用的域名-IP 地址映射的缓冲区，这样主机缓冲区中既有本地的域名映射也有非本地的部分域名映射。

13-6 主机名(域名)和计算机名有何不同？它们各来自什么体系？WINS 的作用是什么？与 DNS 有何不同？

解答：主机名和计算机名都用于标识网络中的一台计算机，但来自不同的规定，用于不同场合。主机名是 Internet 中使用的层次结构的名称，而计算机名是网络基本输入输出系统 NetBIOS 规范的名称，它是一个不超过 15 个字符长度的名字，没有层次结构。主机名和计算机名分别来自 TCP/IP 和 Microsoft Windows 两个最有影响的体系。

WINS 用于 Microsoft TCP/IP 网络中计算机名到 IP 地址的解析，而 DNS 用于 TCP/IP 网络中主机名到 IP 地址的解析。

13-7 Telnet 为用户提供什么应用服务？Telnet 运行使用什么模式？Telnet 采用什么样的服务器方案？

解答：Telnet 为用户提供访问远程系统的资源的服务，就像远地主机的本地用户一样使用这台主机的软、硬件资源。例如，远在异国就可以通过 Telnet 连接到华盛顿的国会图书馆，访问它的资源。

Telnet 运行使用客户-服务器模式。在本地系统运行 Telnet 客户进程，而在远地主机则运行 Telnet 服务器进程。当用户在本地调用 Telnet 时，本地主机上的应用程序成为客户，Telnet 客户通过操作系统内核的键盘驱动程序接收输入的信息并传送到远地的服务器，服务器发回的信息并显示在本地用户屏幕上。

Telnet 的服务器方案是并发服务器，用主从服务器的方式解决并发请求的问题。先于客户启动的 Telnet 服务器用周知端口 23 监听并接受来自客户的 TCP 连接请求，每有一个来自客户的 TCP 连接请求，它就产生一个从服务器来处理这一连接，而原来的主服务器继续等待新的请求。

13-8 FTP 为用户提供什么应用服务？什么是匿名 FTP？FTP 运行采用什么模式？

解答：文件传输协议 FTP 为用户提供文件传输服务，通过网络进行文件的全文拷贝。

匿名 FTP 给用户提供了一种方便的访问方式，它是一种非严格访问控制，但服务器常常将匿名访问限制在某一个目录下的公共文件，如 `usr/ftp`。客户在支持匿名 FTP 的服务器上访问公共文件时，只需使用下述公开的账号：

登录名：`anonymous`

口令：`guest`

就可以与服务器建立会话。guest 是早期系统的匿名访问口令,如今许多 FTP 版本常常要求用户使用其电子邮件地址作为口令,这样,当发生问题时远程 FTP 程序可发送电子邮件通知用户。

FTP 是基于客户-服务器模型而设计的,客户和服务器之间利用 TCP 连接传输信息。但与一般客户-服务器模型有所不同的是,FTP 的客户与服务器之间要建立双重连接,一个是控制连接,负责传输控制信息,一个是数据连接,负责传输文件。FTP 服务器采用并发服务器方式,以满足多个客户的并发请求。

13-9 电子邮件系统中,用户代理(UA)和报文传送代理(MTA)的功能是什么?

解答:UA 包含一个在本地运行的用户接口,用户通过一个友好的接口来交付、读取和处理邮件,其主要功能如下:

发件撰写 给用户提供方便的编辑信件的环境;

收件显示 在计算机屏幕上显示来信内容,包括来信附上的声音和图像等;

收件处理 收信人应能根据情况按不同方式对来信进行处理,例如,删除、存盘、打印等;

交付和读取邮件 用户撰写好邮件后,UA 使用 SMTP 将用户的邮件传送到它的邮件服务器。相反方向上,UA 使用 POP(或 IMAP)从邮件服务器读取邮件到用户主机进行处理。

MTA 运行在 ISP 的邮件服务器上,其主要功能如下:

邮件发送 接收本地用户发送的邮件,存于邮件缓存区待发,MTA 定期(通常每 30 分钟)进行扫描并发送。如果到一定时间(比如几天)某个邮件仍发不出去,就将其从发送邮件缓存区删除,并通知发件人。

邮件接收 MTA 接收发到本地用户的邮件,并将邮件存放在收信人的邮箱中。邮件发送和接收使用 SMTP 协议,另外,MTA 还运行 POP 服务器协议,供用户随时读取邮箱中的邮件。可见,邮件服务器需要昼夜不停地运行,为用户转发和接收邮件。

邮件传输情况报告 将邮件传送的情况向发件人报告。

13-10 简述 RFC822 定义的电子邮件的格式,其信息使用什么编码?

解答:电子邮件信息包括两个部分,中间用一个空行分隔。第一部分是一个首部,包括有关发送方、接收方、发送日期和信息格式等。第二部分是主体,包括信息主体的文本。

电子邮件首部保持标准形式。首部的每一行首先是一个关键字,接着是一个冒号,然后是附加的信息。有些关键字在电子邮件首部是必须的,另一些是可选的。每个首部必须包含以 To 开头的行,引出一个接收方的列表,可以包含一个或多个电子邮件地址。电子邮件的首部有一个以 From 开头的行,其后是发送方的电子邮件地址。以下列出主要的关键字。

To: 接收方邮件地址;

From: 发送方邮件地址;

Cc: 发送副本的邮件地址;

Date: 发送的日期和时间;

Subject: 邮件的主题;
X-Charset: 使用的字符集;
Reply-To: 回复邮件的地址。
RFC822 电子邮件使用可打印的 ASCII 码。

13-11 IETF 定义 MIME 的目的上什么 ?MIME 主要包括那几部分的内容 ?

解答: 早期的电子邮件只能传输 ASCII 码信息。随着时代的发展,电子邮件中广泛需要传输声音、图像等多媒体信息以及非英语的文本。为了能通过电子邮件发送各种非 ASCII 码信息,IETF 定义了多用途 Internet 邮件扩充 MIME。

MIME 主要包含以下三部分内容:

- (1) 扩充了邮件首部,增加了有关 MIME 的 5 个关键字。
- (2) 定义了邮件内容的数据类型,即关键字 Content-Type 所包含的类型。MIME 标准定义了 7 种基本类型以及每种类型的子类型。
- (3) 规定了针对不同数据类型的编码方式,称为内容传输编码。经过内容传输编码后,非 ASCII 码信息转换为 RFC822 规定的 ASCII 码格式,仍使用 SMTP 协议进行 MIME 电子邮件的传输。

13-12 对于如下 3 个字节数据 01001000 10111100 00110101,请给出其 quoted-printable 编码,并用二进制、十六进制、十进制和打印形式表示。

这 3 个字节数据的各种形式为:

二进制: 01001000 10111100 00110101
十六进制: 48 BC 35
十进制: 72 188 53
打印形式: “ H ” 非 ASCII 码 “ 5 ”

解答: 这 3 个字节 quoted-printable 编码的各种形式为:

二进制: 01001000 00111101 01000010 01000011 00110101
十六进制: 48 3D 42 43 35
十进制: 72 61 66 67 53
打印字符: “ H ” “ = ” “ B ” “ C ” “ 5 ”

这 3 个字节都转换成了可打印的 ASCII 码,打印字符串为“ H = BC5 ”。

13-13 对于 13-12 题的 3 个字节数据,请给出其 base64 编码,并用打印形式、二进制、十六进制和十进制表示。对另外 3 个字节数据 00001101 10100001 01111101,重复上述过程。

解答: 对于 13-15 题的 3 个字节数据进行 base64 编码,过程如下:

二进制: 01001000 10111100 00110101
6 比特单位: 010010 001011 110000 110101
base64 编码: “ S ” “ L ” “ w ” “ 1 ” (“ SLw1 ”)
二进制: 01010011 01001100 01110111 00110001
十六进制: 53 4C 77 31
十进制: 83 76 119 49

对 3 个字节数据 00001101 10100001 01111101 进行 base64 编码,过程如下:

二进制:	00001101	10100001	01111101	
6 比特单位:	000011	011010	000101	111101
base64 编码:	“ D ”	“ a ”	“ F ”	“ 9 ” (“ DaF9 ”)
二进制:	01000100	01100001	01000110	00111001
十六进制:	44	61	46	39
十进制:	68	97	70	57

13-14 SMTP 工作于什么模式?它使用传输层的什么协议?它传输的信息使用什么编码?

解答:SMTP 工作于客户-服务器模式,负责发送邮件的 SMTP 进程是 SMTP 客户,负责接收邮件的 SMTP 进程是 SMTP 服务器。SMTP 客户使用周知端口 25 与目的主机的 SMTP 服务器建立 TCP 连接。SMTP 使用传输层的 TCP 协议。SMTP 传输的邮件使用 ASCII 码。

13-15 使用 POP 协议的原因是什么?邮箱访问协议 IMAP 与 POP 有什么不同之处?

解答:SMTP 服务器程序必须昼夜不间断地运行并且始终连通网络,才能随时接收外面发来的邮件,否则就可能使很多发来的邮件丢失,用户的计算机很难做到这一点,电子邮件系统中使用设置有用户信箱的邮件服务器负责这一工作。为了从信箱中读取邮件,TCP/ IP 专门设计了一个对邮件信箱进行远程访问的协议,通过它用户从信箱中读取自己的邮件。信箱访问协议使用最多的是邮局协议 POP3。

邮箱访问协议 IMAP 和 POP 一样,也是基于客户-服务器模式工作,但它们有一定的差别。IMAP 是一个联机处理协议,IMAP 的用户可以在远地操纵服务器的邮箱,就像在本地操纵一样,用户可以在不同的地方使用不同的计算机随时上网阅读和处理自己的邮件。但这需要每次都要与邮件服务器建立连接,因而要付上网费。而 POP 邮件在下载 to 用户主机之后,对邮件的所有处理都在用户的主机上进行,不需要网络继续连接。

13-16 万维网是一种网络吗?它是一个什么样的系统?采用什么模式工作?使用什么传输协议?

解答:万维网并不是某一种类型的计算机网络,万维网是 Internet 上的一种应用系统,一个大规模的分布式信息系统,提供海量的信息存储和交互式超媒体信息服务的应用系统。用链接的方法可以非常方便地从 Internet 上的一个 Web 站点访问另一个 Web 站点,从整个 Internet 上获取丰富的信息。

万维网用客户-服务器模式工作。浏览器就是在用户计算机上的客户端程序,万维网文档所驻留的计算机运行服务器程序,即万维网服务器(Web server),万维网的这种客户-服务器模式也称为基于 Web 的客户-服务器模式,或浏览器-服务器 B/ S(browser/ server)模式。

为了使万维网文档在 Internet 上传输,万维网客户和服务程序之间的交互使用超文本传输协议 HTTP,HTTP 在 TCP/ IP 体系中是一个应用层协议,基于传输层的 TCP 协议进行可靠的传输。

13-17 什么是超媒体？什么是超链？

解答：超媒体(hypermedia)是超文本(hypertext)的多媒体化扩充,Hypermedia 这个词的后缀 media 意思是信息的载体除了文本外,还可以是声音、图形、图像、动画以及视频图像等多种表示方式;Hypermedia 这个词的前缀 Hyper 意思是一个超媒体是使用超链(hyperlink)将多个信息源链接而成。超链是包含在每一个页面中能够链接到其他万维网页面的链接信息。利用一个链接可以由一个文档找到一个新的文档,由这个新文档又可链接到其他的文档,……,如此链接下去,可以在全世界范围内连接于 Internet 上的超文本系统中漫游。

13-18 描述用户鼠标单击万维网页面上某一个链接后万维网产生的处理过程。

解答：如果浏览器的用户用鼠标单击了网页上的某一个链接,它对应一个指向另外一个页面的超链,假设该超链的 URL 是 `http://www.uinversity.edu.cn/chn/zsxx/index.htm`,那么,万维网的处理过程如下:

浏览器分析页面的 URL;

浏览器向 DNS 请求解析服务器的域名 `www.uinversity.edu.cn` 的 IP 地址,DNS 解析出 IP 地址并作出应答;

浏览器使用服务器的 IP 地址和周知端口 80 与服务器建立 TCP 连接;

浏览器发出取文件 HTTP 命令:`GET /chn/zsxx/index.htm`;

服务器响应,将文件 `index.htm` 发送给浏览器;

双方释放 TCP 连接;

浏览器显示文件 `index.htm` 的页面。

13-19 浏览器主要由哪几个部分组成？它们的作用是什么？浏览器设置缓存的目的是什么？

解答：一个浏览器主要包括一组客户、一组解释程序以及一个控制程序。

控制程序是核心部件,它管理调度客户和解释程序,解释鼠标的点击和键盘的输入,调用有关的程序来执行相应的操作。例如,当用户用鼠标单击一个超链的起点时,控制程序就调用一个客户从远地服务器上取回该文档,并调用相应解释程序进行解释,最终由显示驱动程序驱动,显示该文档的页面。

浏览器可以包含 HTTP 客户、FTP 客户和电子邮件客户等。浏览器必须包含 HTTP 客户,HTTP 客户用来与服务器建立连接和交换数据。浏览器还可以包含一个 FTP 可选客户,用来获取文件传送服务。一些浏览器还包含一个电子邮件可选客户,使浏览器也能够发送和接收电子邮件。

HTML 解释程序是必需的,而其他的解释程序则是可选的。解释程序对 HTTP 客户从服务器得到的 HTML 文档进行解释并转换为适合用户显示硬件的命令来处理版面的细节,显示驱动程序将页面在显示器上展现出来。

浏览器中还可设有一个缓存。浏览器将它取回的页面副本都存入本地磁盘的缓存中。当用户浏览某个页面时,浏览器首先检查本地的缓存,若缓存中保存了该页面,浏览器就直接从缓存中读取该页面而不必通过网络得到,因而明显地改善了浏览器的运行速度。但问题的另一面是,如果缓存中保存的是用户今后不再浏览的页面,反而会因为增加

无意义的磁盘操作而降低了浏览器的性能,因此许多浏览器允许用户调整缓存策略。比如,用户可以设置页面缓存时间的时限等。

13-20 叙述 Web 代理技术。

解答:万维网代理可以提高万维网访问的效率。Web 代理一般是运行于本地 LAN 上的一台主机上的一个进程,它代理用户的万维网的访问,许多 ISP 也运行万维网代理。运行万维网代理的主机的磁盘上存储了大量的它近期访问所得到的网页的备份,它们可以在后来的同样访问中使用,这种技术称为缓存可以减轻网络负载。

为了使用 Web 代理技术,浏览器也要做相应的配置,使得所有的页面访问请求都发送给代理。使用 Web 代理的工作过程如下:浏览器访问万维网时,先向代理发出 HTTP 请求报文。如果运行代理的主机的磁盘中已经存储了该请求的对象,则将此对象放到 HTTP 响应报文中返回给浏览器;否则,代理就代表该浏览器向 Internet 上的源头服务器发出 HTTP 请求报文。代理从源头服务器收到这个请求的对象后,先复制在自己的磁盘中(以便今后使用),再放在 HTTP 响应报文中发送给原请求该对象的浏览器。可见,Web 代理即作为客户也作为服务器。

13-21 HTTP 在 TCP/IP 体系结构中处于什么层次?它使用传输层的什么协议? HTTP 监听连接请求使用的周知端口是多少?什么是持续连接和非持续连接? HTTP 协议定义了几类报文?

解答:HTTP 是 TCP/IP 体系中应用层的协议,它一般基于传输层的 TCP 协议,HTTP 服务器通过 TCP 的周知端口 80 监听客户向它发出连接请求。HTTP1.0 为每次请求都要建立一次 TCP 连接,服务器发回响应后 TCP 连接就被释放,这是一种非持续连接。HTTP1.1 支持持续连接(persistent connection)并把它作为默认选择,对于用户连续的多个访问请求,TCP 连接不被释放,这可减少开销,提高效率。

HTTP 定义了两类报文:HTTP 客户的请求报文和服务器的响应报文,HTTP 客户和服务器交互的是 ASCII 码文本的请求和类似于 MIME(MIME-like)的响应。

13-22 HTML 的超链的起点和终点表示什么?如何定义一个超链?什么是远程链接和本地链接?

解答:每个超链都有一个起点和终点,起点表示一个超链在万维网页面中从何处引出,它可以是一个页面中的一个字符串或一幅图等,单击它们,就从该处出发链接到一个新的页面,即终点。在 HTML 的语法中,终点用这个新页面的 URL 表示,而起点用单击的字符串或一幅图的文件名表示。

HTML 定义一个超链的语法是:

$$A \text{ HREF} = \text{terminal-URL} \text{ start} / A$$

式中,start 是超链的起点,如果起点是字符串,start 就是该字符串,如果起点是一幅图,start 还要使用图像文件的标签 `IMG SRC = ...`,图的文件名放在引号中。terminal-URL 是超链终点的统一资源定位符,放在 `HREF = " ... "`的引号中。HREF 与字符 A 中间应有一个空格。

如果超链的终点不是在本网站上,而是其他网站上的页面,这种链接方式称为远程链接。如果超链指向本主机中的某一个文件,这种链接方式则属于本地链接。

13-23 什么是命名锚？如何定义一个命名锚？

解答：命名锚(named anchor)是 HTML 链接到同一个文件中某个位置的一种链接方法。式(1)用来定义一个命名锚：

$$A \text{ NAME} = \text{named anchor terminal-characters} / A \quad (1)$$

其中 NAME 后面引号中的 named anchor 写入命名锚的名字,terminal-characters 具体指明该链接终点位置,它是这个位置开始的一个字符串。

链接到一个命名锚的语法是：

$$A \text{ HREF} = \# \text{ named anchor start} / A \quad (2)$$

其中字符 # 后面的 named anchor 就是命名锚的名字,式(2)指明了一个超链的起点 start 和终点的名字 named anchor,但终点的名字和具体位置 terminal-characters 还要由式(1)来定义。因此式(1)和式(2)应联合使用,缺一不可。

使用命名锚也可链接到本地的其他 HTML 文件上,这时式(2)中的字符 # 前应加上该文件的名字,但命名锚不能链接到其他地点的文件上。

13-24 Web 文档可以分为几类？它们的特点是什么？

解答：Web 文档可以划分为以下三类：

静态文档(static document) 静态文档是最基本的万维网文档。静态文档创作完毕后存放在万维网服务器中,在用户浏览的过程中,页面内容不会改变,只有程序员修改了存放在万维网服务器中的静态文档,显示页面才可能改变,因而是静态的。

动态文档(dynamic document) 与静态文档不同,动态文档所看到的页面内容可以反映当时的情况而经常变化。动态文档是在浏览器访问万维网服务器的时候,才由服务器上的应用程序动态创建。当浏览器请求到达服务器时,它运行另一个应用程序,该应用程序对浏览器发来的数据进行处理并生成一个 HTML 格式的文档。即使浏览器发出同样的请求,但每次生成的动态文档可以不同。

活动文档(active document) 活动文档则有更快的刷新能力,可以连续快速地进行屏幕刷新。动态文档进行显示屏幕的刷新是由服务器完成,连续刷新的能力是有限的,不能满足像动画一类的应用需要。活动文档技术的屏幕刷新的工作是由浏览器实现。当浏览器请求一个活动文档时,服务器的响应中返回一段程序,该程序在浏览器上运行,它负责屏幕刷新的工作,可以连续快速地进行屏幕刷新。

13-25 为实现动态文档,CGI 对 Web 服务器作了什么改进？

解答：为实现动态文档,CGI 从两个方面对万维网服务器进行了改进：

一方面,增加了一个应用程序,称作 CGI 程序,用来处理浏览器发来的数据并创建动态文档。浏览器访问万维网服务器时可以启动 CGI 程序,CGI 程序对浏览器发来的数据进行处理并即时生成 HTML 格式的文档,万维网服务器将此文档作为对浏览器的响应发回浏览器。由于对浏览器每次请求的响应都是即时生成的,因此通过动态文档所看到的页面内容可以反映当时的情况而不断地变化,报告变化中的当前最新信息。例如动态文档可用来报告股市行情或民航铁路售票情况等经常变化的内容。

另一方面,增加了一个机制,通过它万维网服务器和 CGI 程序进行交互,增加的这个

机制就是 CGI。CGI 是一种标准,它规定了万维网服务器如何与 CGI 程序交互。名称中出现“网关”二字是因为 CGI 程序还可以访问其他的服务器资源,如数据库等,CGI 程序的作用有点像一个网关。前面提到的利用动态文档可用来报告股市行情或民航铁路售票情况,它们的数据就可以放在数据库中。

13-26 HTML 中表单的功能是什么?如何定义一个表单?

解答:表单(form)用来将用户数据从浏览器传递给服务器,这在创建动态文档时是很有用的。表单和 CGI、PHP、JSP 和 ASP 程序配合使用来创建动态文档。表单在浏览器的屏幕出现时,可以有一些选择框和按钮,可供用户选择和单击,有的方框可让用户录入数据,这样浏览器就可以收集不同用户的不同数据,传递给服务器。

在 HTML 文档的主体中使用表单标签 FORM 和 / FORM 定义一个表单,在它们中间要插入一些标签,来指明表单中所包含项目的细节。在 FORM 标签中首先要说明一个 ACTION 参数,ACTION 参数后面的引号中指出在万维网服务器中的 CGI 程序的位置,一般就是一个 URL。

13-27 RTP/ RTCP 本身对多媒体数据传输能够提供 QoS 保证吗?为什么说它们适合传输多媒体数据?

解答:RTP/ RTCP 本身并不对多媒体数据块做任何处理,并不提供任何 QoS 保证。但 RTP/ RTCP 包含了实时应用的一些共同性的信息,提供给应用层,使应用层有依据进行必要的 QoS 处理。RTP/ RTCP 为多媒体数据提供了网络承载平台,它们非常适合传输多媒体数据。RTP 分组首部的字段的设置适合于多媒体数据的封装和描述,序号、时间戳等能够描述多媒体数据的时间属性。RTP 协议不规定载荷的格式和大小,这就为不同的媒体和应用环境提供了灵活的空间。RTCP 协议提供多媒体数据传输质量的反馈,为数据传输的管理提供了条件,可以用来监控传输的 QoS。RTCP 报告的信息对发送端、接收端是很有用的,RTCP 没有规定使用这些信息做什么,这完全取决于应用程序的开发人员。例如,接收端报告的某 RTP 流的分组丢失率太高,发送端就应当适当降低发送分组的速率。

13-28 描述加权公平排队(WFQ)分组转发算法。

解答:WFQ 为不同的分组流分配不同比例的输出链路带宽。WFQ 算法如下:

$$R_i = R \times W_i / \sum_{i=1}^n W_i \quad (i = 1, 2, \dots, n)$$

式中, R 和 R_i 分别为输出链路的总带宽和队列 i 的带宽, W_i 为队列 i 的权系数, n 为输出队列数。WFQ 算法是对路由器传统的 FIFO 算法在服务质量方面的重要改进。

13-29 RSVP 资源预留请求为什么设计为由接收端发起?这带来了什么问题? RSVP 如何解决?

解答:RSVP 支持有多个不同类型的接收端参与的多方会议,接收端可以独立地加入或离开,发送端并不知道;而且,不同的接收端对服务质量的需求可以是不同的,接收端自己才真正知道它所需要的带宽。因此,资源预留请求设计为由接收端发出。

RSVP 资源预留请求由接收端发起的一个主要问题是:接收端不知道资源预留请求分组发送的路径。RSVP 通过路径(Path)报文解决这一问题。Path 报文由发送端发出,沿单播/组播路径传送到接收端。Path 报文记录沿途的路径状态,其中包括该路径的

上一跳结点地址。当接收到 Path 报文后,接收端将以单播方式,使用由 Path 报文得到的传输路径的上一跳结点地址,沿上游方向向发送端发送资源预留请求报文。

13-30 图 1-13-1 是预留方式的例子。其中图 1-13-1(a)是一个 RSVP 路由器,包括两个输入接口 a 和 b 以及两个输出接口 c 和 d。输入接口 a 和 b 分别接收来自多播源 S_1 、 S_2 和 S_3 的分组流,路由器通过输出接口 c 和 d 分别转发至接收端 R_1 和 R_2 、 R_3 。

图 1-13-1(b)、(c)和(d)分别是 WF、FF 和 SE 方式预留请求的例子,图中标出了从接口 c 和 d 接收的不同方式的预留请求。请给出 c 和 d 接口的预留以及合并后由接口 a 和 b 向上游转发的预留请求。

解答:在图 1-13-1 的(e)、(f)和(g)中,给出了(b)、(c)和(d)中 c 和 d 接口的预留以及合并后由接口 a 和 b 向上游转发的预留请求。

13-31 什么是每跳行为(PHB) ?

解答:DiffServ 网络中,路由器将来自不同通信流但具有相同 DSCP 的分组聚合为一个行为集合(BA)。路由器对一种 BA 的转发处理行为的外特性描述称为 PHB,不涉及具体的实现机制。“每跳”强调了这里所说的转发处理“行为”只涉及到本路由器转发的

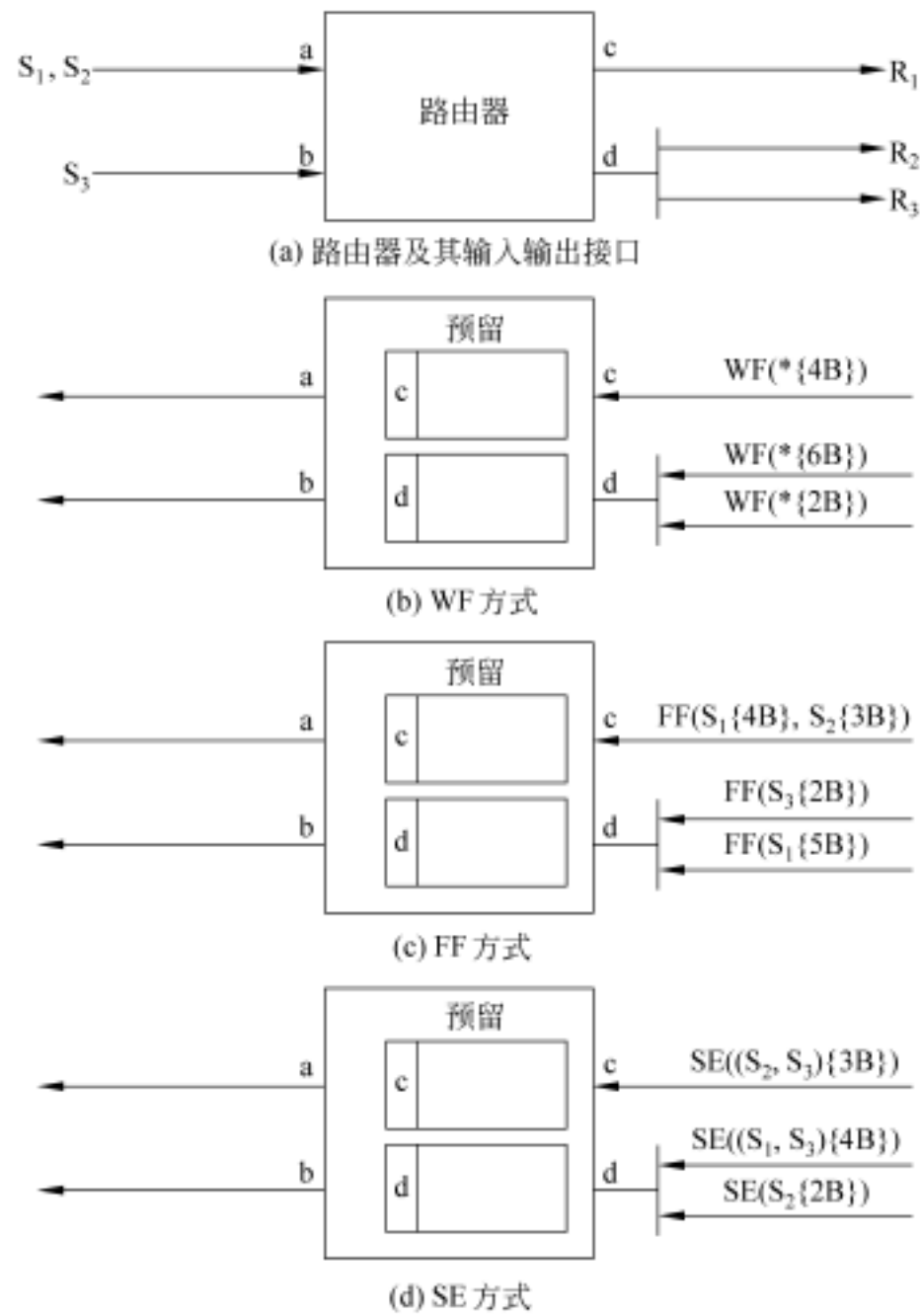


图 1-13-1 题 13-30 预留方式的例子和解答图

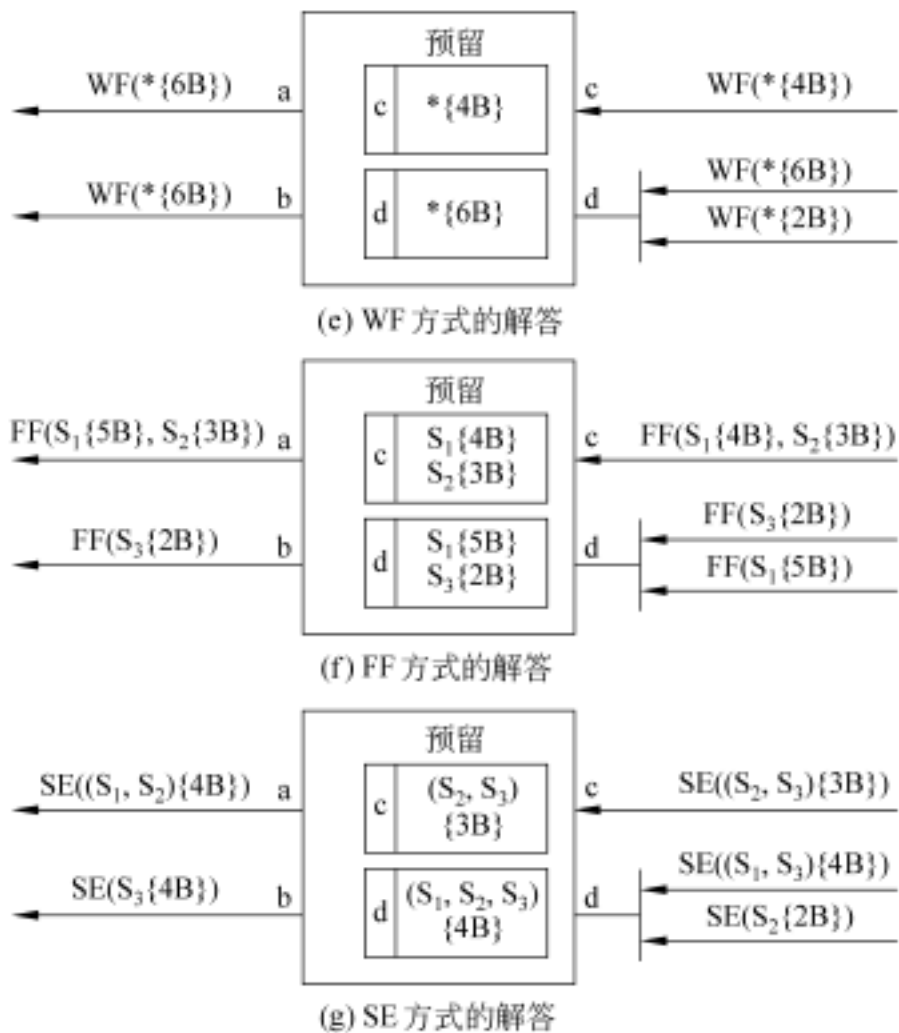


图 1-13-1(续)

这一跳,而下一跳怎样处理则与此无关。这和 IntServ/ RSVP 考虑的服务质量是端到端的不一样的。一个 PHB 的简单例子是,对于某一 BA,它保证提供不低于链路带宽 $x\%$ 的带宽分配。

13-32 DHCP 的作用和是什么?一台计算机如何通过 DHCP 获得一个 IP 地址?

解答:动态主机配置协议 DHCP 提供了动态配置 IP 地址的功能。

DHCP 使用客户-服务器模式。DHCP 在网络上设置一台或多台 DHCP 服务器,它们本身使用一个固定的 IP 地址,并拥有一个由一定数量的 IP 地址组成的 IP 地址池。申请 IP 地址的计算机配置成 DHCP 客户,向服务器租用 IP 地址。

一台计算机要通过 DHCP 获得一个 IP 地址,它应配置为 DHCP 客户,在它启动时会向本地网络广播一个发现报文 DHCPDISCOVER,请求一个 IP 地址。之所以使用全 1 的广播地址是因为 DHCP 客户此时还不知道服务器的 IP 地址。DHCP 客户此时还没有 IP 地址,其源地址设置为 0.0.0.0。本地网络上的主机都收到请求报文,但只有 DHCP 服务器作出响应,发回提供报文 DHCPOFFER,提议 IP 地址等信息。如果 DHCP 客户的 DHCPDISCOVER 请求没有得到响应,它会进行多次尝试。

可能有不止一个 DHCP 服务器响应提供报文,DHCP 客户从地址池中选择一个 IP,一般是第一个响应的服务器的提议,并发出一个请求报文 DHCPREQUEST,提供 IP 地址的服务器发回确认报文 DHCPACK。这样,IP 地址租约正式生效,DHCP 客户就获得了这个 IP 地址。

13-33 SNMP 网络管理系统由哪两类设备组成？它们运行什么软件？它们之间使用什么协议通信？

解答：SNMP 网络管理系统包含两类设备：网络管理站和被管理的网络设备，通常管理站是网络上的一台计算机，而被管理设备可以有多种，如路由器、交换机、服务器、工作站等。管理站一般提供图形化的人机界面，网络管理员通过管理站对网络中的各种资源进行管理，查看和设置被管理网络设备的运行状态。

网络管理站运行的软件是管理器 (manager) 或称管理进程，被管理的网络设备运行的软件称为代理 (agent) 或称代理进程。只有运行代理的设备才能被网络管理系统所管理。

管理器和代理之间的通信协议是 SNMP 协议，它运行于 UDP 之上。SNMP 包括一组简单的命令，用于管理器检索和设置代理的 MIB 中对象的数值，代理响应来自管理器的 SNMP 请求，完成相应的操作。代理也可以通过 trap 机制主动为管理器提供重要的非请求的信息。

13-34 SNMPv1 协议定义了几种报文？它们的功能是什么？通过什么操作方式实现这些功能？

解答：SNMPv1 规定了 5 种报文，用于在管理器和代理之间交换信息。这 5 种报文的功能如表 1-13-1 所示：

表 1-13-1 SNMPv1 5 种报文 (PDU) 的功能

类型	名称	执行者	功 能
0	get-request	管理器	查询代理一个或多个变量的值
1	get-next-request	管理器	在代理的 MIB 树上检索下一个变量，可反复进行
2	get-response	代理	对管理器的 get/ set 报文 (PDU0、1、3) 作出响应，并提供差错码、差错状态等信息
3	set-request	管理器	设置代理的一个或多个变量的值
4	trap	代理	向管理进程报告发生的事件

SNMP 的基本功能通过轮询操作来实现，管理器向被管理设备周期性地发送轮询信息。这种方式是客户-服务器模式，管理器是客户，代理是服务器。

SNMP 还采用 trap 机制，当代理进程捕捉到较严重的事件时，随即向管理进程报告发生的事件。trap 即陷阱，意思是它能捕捉“事件”，这种方式是基于中断的。

13-35 什么是管理信息库 (MIB)？说明 SMI 标准定义的对象标识符和对象命名树。

解答：SNMP 网络管理系统中，反映网络运行状态的管理信息称为被管理对象，它们是管理器通过代理所能查询和设置的。MIB 是所有可能的被管理对象的结构化的集合。

SMI 标准指明 MIB 中的对象必须由 ISO 提出的抽象语法记法 1 (ASN .1) 来定义。ASN .1 的对象采用分级结构的命名体系，类似于 DNS 中的域名命名树。分级结构的命名体系中，从根开始结点分成若干级，同级的结点都用一个不同的整数编号。这样，根据

结点在树上的位置,整数编号自高到低逐级向下用小数点连接排列,就构成一个整数序列,能够惟一地标识各个结点,称为对象标识符。对象标识符还对应一个用小数点连接的文字名,更便于阅读与记忆。

树型结构的对象标识符命名空间称为对象命名树,每个对象在树上有一个惟一的位置。对象命名树构成了全世界范围内一个全局性的可管理的结构化的对象标识符空间。实际上,对象命名树包含的对象不限于网络管理中使用的变量,MIB对象集合只是其中的一个子树。

13-36 客户机-服务器模式属于以__(1)__为中心的网络计算模式,其工作过程是客户端__(2)__,服务器__(3)__,并__(4)__,它的主要优点是__(5)__。

- (1) A.大型、小型机 B.服务器 C.通信 D.交换
- (2) A.向服务器发出服务请求 B.向服务器发出浏览查询请求
C.向网络发送服务请求 D.在本机上发出自我请求
- (3) A.接收请求并告诉请求端再发一次
B.接收请求,进入中断服务程序,打印本次请求内容
C.响应请求并在服务器端执行相应的请求服务
D.把响应请求转回到请求端并执行
- (4) A.把执行结果在打印服务器上输出 B.把显示内容送回客户机
C.把整个数据库内容送回客户机 D.把执行结果送回客户机
- (5) A.网络通信线路上只传送请求命令和计算结果,减轻通信压力
B.网络通信线路上只传递数据,从而减轻通信开销
C.数据的安全性得到保障
D.数据的完整性得到保障

答案: B, A, C, D, A

13-37 Internet 提供了大量的应用服务,分为通信、获取信息与共享计算机资源等三类。

__(1)__ 是世界上使用最广泛的一类 Internet 服务,它使用 RFC 822 规定的格式和 SMTP 协议。

__(2)__ 是用来在计算机之间进行文件传输。利用该服务不仅可以从远程计算机获取文件,而且可以将文件从本地机器传送到远程计算机。

__(3)__ 是目前 Internet 上非常丰富多彩的应用服务,其客户端软件称为浏览器。目前较为流行的 Browser/Server 网络应用模式就以该类服务作为基础。

__(4)__ 应用服务将主机变为远程服务器的一个虚拟终端;在命令方式下运行时,通过本地机器传送命令,在远程计算机上运行相应程序,并将相应的运行结果传送到本地机器显示。

- (1) A. E-mail B. Gopher C. BBS D. TFTP
- (2) A. DNS B. NFS C. WWW D. FTP
- (3) A. BBS B. Gopher C. WWW D. NEWS
- (4) A. ECHO B. WAIS C. RLOGIN D. TELNET

答案：A, D, C, D

13-38 如下__(1)__协议支持 E-mail 程序 ?在邮件地址中, @ 之后的字符通常为__(2)__。

- | | | | |
|--------------|----------|-------------|------------|
| (1) A . SNMP | B . POP3 | C . FTP | D . Telnet |
| (2) A . 邮件地址 | B . 用户账号 | C . 邮件服务器域名 | D . 邮件密码 |

答案：B, C

第 14 章

Socket 网络通信程序设计

14-1 操作系统包括哪两个层次？什么是应用程序编程接口 (API)？它有哪些两种实现方式？

解答：操作系统包含内核和系统应用程序两个层次。系统启动后，内核总是常驻内存，它提供最基本的系统功能，比如设备驱动、进程调度、资源管理等。在内核之外是系统应用程序，包括外部命令、应用平台和软件开发环境等。

应用程序只有通过内核才能访问计算机的各种硬件资源。API 是应用程序（包括用户自己开发的应用程序和系统应用程序）如何访问系统内核的接口。

API 有两种实现方式：一种是系统内核的系统调用，另一种是以库函数方式，它在核外实现。在 UNIX 中就系统调用来实现，而在 Windows 中则用库函数来实现。

14-2 解释套接字 (Socket)、Socket 机制和套接字对。

解答：套接字 (Socket) 的英文原意是孔、插口等，这里用来表示 UNIX TCP/IP 网络通信的接口，类似现实生活中的电话插口，提供了电话和电话网络之间的接口。

基于套接字概念形成了 TCP/IP 网络环境下应用程序之间通信的一套程序设计方法，一种 TCP/IP 网络通信 API，称为 Socket 机制。

可以把套接字机制看成是网络环境下提供通信端口的 UNIX 文件访问机制的一般化。UNIX 操作系统在文件读写之前调用 `open()` 时，系统返回一个文件描述字与某个文件或设备相关联，并用它作为读 `read()`、写 `write()` 的参数来标识该文件或设备。套接字机制最早是由 BSD UNIX 引入的一种网络通信编程机制，这种机制继承了 UNIX 文件读写的思路。应用程序在进行网络读写时请求操作系统创建一个套接字，系统返回一个类似文件描述字的整数，可以称为 Socket 描述字，应用程序使用它标识创建的套接字，提供通信的端口。套接字机制的使用也和文件访问类似，一旦应用程序创建了一个套接字，并进行了地址绑定和外部地址的 TCP 连接，就可以利用 Socket 描述字作为参数使用 `write()` 在此连接上发送数据流，在连接的另一端则使用 `read()` 接收数据。

套接字对是表示 TCP 连接的两个端点的四元组：(本地 IP 地址，本地 TCP 端口号；远程 IP 地址，远程 TCP 端口号)，通过 Socket 对连接了通信两端的应用程序。

14-3 什么是流套接字？什么是数据报套接字？

解答：流套接字和数据报套接字是两种不同类型套接字，同一协议族可能提供多种不同的通信服务类型，创建 Socket 的应用程序使用不同类型套接字可以指定网络提供的通信服务类型。流套接字提供面向连接的数据流通信服务，数据报套接字提供不连接的

数据报通信服务。TCP/ IP 协议族中,流套接字和数据报套接字分别对应 TCP 和 UDP 协议。

14-4 什么是套接字命名?套接字有了号,为什么还要命名?

解答:套接字命名即是 将本地 Socket 地址赋予 Socket。本地 Socket 地址包括本地主机 IP 地址和本地端口号。

创建了一个 Socket 并有了 Socket 号,这个通信端口还不能使用,当它命名之后,将本地主机 IP 地址和本地端口号赋予它,它才能和特定主机上的特定的应用程序相关联,才能通过这个通信端口找到通信的端点。

14-5 accept()调用为什么设计成阻塞方式的?描述 accept()调用后的状态。画图说明 accept()调用后服务器如何产生一个从服务器进行并发处理。

解答:服务器程序调用了 accept()后,就进入阻塞状态,这样就可等待本地套接字上到达的连接请求。

accept()调用后将返回连接客户的 Socket 地址及其长度并将它们分别放入调用参数所指定的位置。accept()调用后还给调用者返回一个新的 Socket 号,这一新 Socket 与请求的客户建立了连接,而原来的 Socket 仍保持打开状态,可以用来继续接收新的连接请求。

下图表示 accept()调用后服务器如何产生一个从服务器,主要包括 3 个步骤:

(1) accept()调用返回后为服务器创建了一个新套接字 newsock,并且它与客户建立了连接。原来的 initsock 仍保持打开状态。

(2) 调用 fork()产生一个从服务器(子进程), fork()以后,initsock 和 newsock 都是主服务器和从服务器所共享的。图 1-14-1(a)给出了 fork()返回后的状态。

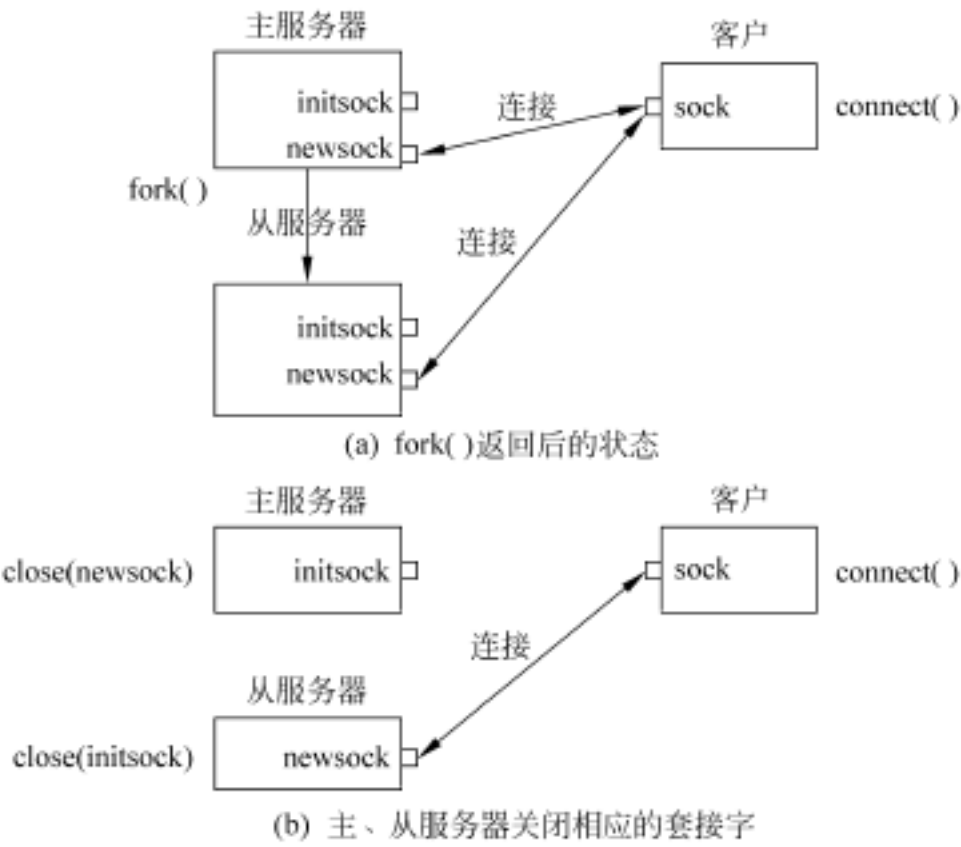


图 1-14-1 题 14-5 解答图示

(3) 主服务器关闭 newsock, 从服务器关闭 initsock, 这是所期望的最终状态, 如图 1-14-1(b)。从服务器使用 newsock 与客户连接, 进行数据交换, 而主服务器可对 initsock 套接字再次调用 accept() 来处理下一个客户的连接请求。

14-6 画图给出客户-服务器模式下面向连接的 Socket 网络通信程序的一个实现框架。

解答: 图 1-14-2 是面向连接的客户-服务器模式的 Socket 网络通信的一个实现框架。面向连接模式下套接字的连接是不对称的, 服务器进程和客户进程在连接套接字时需采取不同的动作。服务器程序必须先启动, 它首先, 通过系统调用 socket() 创建一个流套接字。随后服务器进程要给该套接字命名一个周知的名字, 以便客户程序能够藉此向服务器发出请求与之通信。因为它们无法知道套接字的号, 套接字的名称将是客户可能连接的一个服务器标识。命名套接字使用 bind() 系统调用。

系统调用 listen() 用于建立侦听队列, 系统调用 accept() 用于接收套接字上到达的连接请求。服务器程序调用了 accept() 后, 就进入阻塞状态, 等待客户的连接请求。

客户进程通过调用 socket() 创建一个套接字, 然后通过将服务器进程的已命名套接字作为目的地址调用 connect(), 与服务器进程建立连接。

一旦建立连接, 客户和服务进程两端就可以使用套接字进行双向通信。通信完毕可关闭套接字。

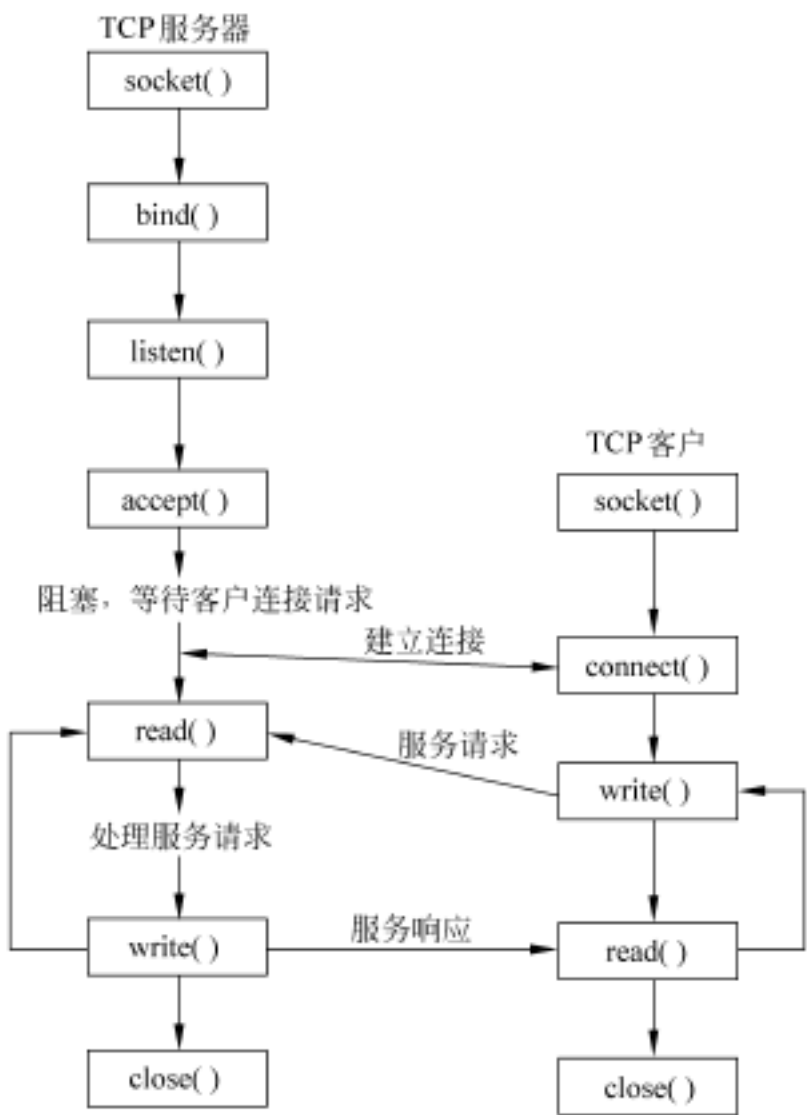


图 1-14-2 面向连接的客户-服务器模式的 Socket 网络通信实现框架

14-7 编写网络通信程序,使用无连接的网络通信,客户机-服务器方式,服务器为重复服务器。要求服务器提供回显(echo)服务:在客户端输入一个字符串后发送给服务器,服务器判断该字符串是否为结束通讯标志(字符串“END”),如不是,服务器将把该字符串再回送给客户端,否则结束与客户端的通信。

解答:1.服务器端程序

```

/ *
    udpServer.c - - - - - main
*/
#include <unistd.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <sys/signal.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/resource.h>
#include <sys/wait.h>
#include <sys/errno.h>
#include <netinet/in.h>

#define DEFAULT_PORT 3456          / * 服务器默认绑定端口 */
#define BUFSIZE 1024              / * 读缓冲区大小 */
/ *
    main - - - 提供回显服务的 UDP 重复服务器端程序主函数
    usage: udpServer [port]
*/
int main(int argc, char * argv[])
{
    int sock;                      / * 套接字描述符 */
    struct sockaddr_in server;     / * 存放服务器信息 */
    struct sockaddr_in client;     / * 存放客户端信息 */
    int port;                      / * 服务期绑定端口号 */
    int rval, length;
    char buf[BUFSIZE];
    switch( argc )
    {
        case 1:
            port = DEFAULT_PORT; / * 不带参数运行,使用默认端口号 */
            break;
        case 2:
            port = atoi(argv[1]); / * 使用运行时指定的端口号 */
            break;
    }

```

```

        default:
            perror( usage: multiTcpServer [port]\n );
            exit(1);
    }
    /* 创建套接字 */
    sock = socket(PF_INET, SOCK_DGRAM, 0);
    if( sock < 0 )        /* 错误检测 */
    {
        perror( can't create socket\n );
        exit(1);
    }
    /* 填写服务器地址信息 */
    server.sin_family = AF_INET;
    server.sin_addr.s_addr = INADDR_ANY;
    server.sin_port = htons(port);
    /* 绑定到端口 */
    rval = bind( sock, (struct sockaddr *)&server, sizeof(server) );

    if ( rval < 0 ) /* 错误检测 */
    {
        perror( binding error\n );
        exit(1);
    }
    /* 服务期进入死循环,等待客户端连入 */
    do
    {
        /* 接受客户端输入 */
        bzero(buf, sizeof(buf));
        length = sizeof(client);
        rval = recvfrom(sock, buf, sizeof(buf), 0, (struct sockaddr *)&client, &length);
        if( rval < 0 )    /* 错误检测 */
        {
            perror( reading error\n );
            exit(1);
        }
        /* 判断客户端是否输入 END,如是则结束和这个客户的对话 */
        if( strcmp( buf, END ) != 0 )
        {
            /* 将接受的字符串再回送给客户端 */
            rval = sendto(sock, buf, strlen( buf ) + 1, 0, (struct sockaddr *)&client, sizeof(client));
            if( rval < 0 ) /* 错误检测 */
            {
                perror( writing error );
            }
        }
    } while( 1 );
}

```



```
        exit(1);
    }
}
while (1);    /* 循环结束 */
}            /* 主函数结束 */
```

2 . 客户端源程序

```
/*
    udpClient.c - - - - - main
*/
#include <sys/ types.h>
#include <sys/ socket.h>
#include <netinet/ in.h>
#include <netdb.h>
#include <stdio.h>
#define DEFAULT_PORT 3456    /* 服务器默认监听端口 */
#define BUFSIZE 1024        /* 读缓冲区大小 */
/*
    main - - - 回显服务的客户端程序(UDP)
    usage: udpClient [xxx.xxx.xxx.xxx, [port]]
*/
int main(int argc, char * argv[])
{
    int sock;                /* 套接字描述符 */
    struct sockaddr_in server; /* 存放服务器信息 */
    struct sockaddr_in client; /* 存放客户端信息 */
    struct hostent * hp;      /* 存放服务器地址 */
    int port;                 /* 服务器绑定端口号 */
    int rval, length;
    char buf[BUFSIZE];

    switch( argc )
    {
        case 1:
            /* 不带参数运行,使用本机地址和默认的服务器端口号 */
            hp = gethostbyname( localhost );
            port = DEFAULT_PORT;
            break;
        case 2:
            /* 使用运行时指定的 ip 地址和默认端口号 */
            hp = gethostbyname( argv[1] );
            port = DEFAULT_PORT;
            break;
```

```

    case 3:
        /* 使用运行时指定的 ip 地址和端口号 */
        hp = gethostbyname(argv[1]);
        port = atoi(argv[2]);
        break;
    default:
        perror( usage: udpClient [xxx.xxx.xxx.xxx, [port]]\n );
        exit(1);
}
if (hp == 0) /* 错误检测 */
{
    printf( %s:unknown host ,argv[1]);
    exit(1);
}
/* 填写服务器地址信息 */
server.sin_family = hp -> h_addrtype;
memcpy((char *) &server.sin_addr.s_addr, hp -> h_addr_list[0], hp -> h_length);
server.sin_port = htons(port);
/* 创建套接字 */
sock = socket(PF_INET, SOCK_DGRAM, 0);
if( sock < 0 ) /* 错误检测 */
{
    perror( can't create socket\n );
    exit(1);
}
/* 客户端绑定到任意端口 */
client.sin_family = AF_INET;
client.sin_addr.s_addr = htonl(INADDR_ANY);
client.sin_port = htons(0);
rval = bind( sock, (struct sockaddr *) &client, sizeof(client) );
if ( rval < 0 ) /* 错误检测 */
{
    perror( binding error\n );
    exit(1);
}
/* 客户端接受键盘输入的字符串,发送给服务器后,再接受服务器返回的同样
内容,并打印出来 */
do
{
    scanf( %s , buf);
    rval = sendto(sock, buf, strlen(buf) + 1, 0, (struct sockaddr *) &server, sizeof(serv-
er));
    if( rval < 0 )
    {

```

```
        perror( writing stream message );
        exit(1);
    }
    if( strcmp(buf, END ) == 0 )
        break;
    length = sizeof( server);
    rval = recvfrom(sock, buf, sizeof(buf), 0, (struct sockaddr *) &server, &length);
    if( rval < 0 )
    {
        perror( reading stream message );
        exit(1);
    }
    printf( Echo from the host: %s\n , buf);
}
while(1);    /* 循环结束 */
}            /* 主函数结束 */
```

第 15 章

网 络 安 全

15-1 网络攻击主要有哪几种方式？网络安全服务的主要涉及哪些方面？

解答：对网络的攻击大致可分为下面几种方式：

截取(interception) 攻击者通过监控网络或搭线窃听等手段截取网上传输的信息,这是对访问控制的攻击；

篡改(Modification) 攻击者截获传输的信息并篡改信息的内容后再进行传输,这严重破坏了数据的完整性；

伪造(fabrication) 攻击者假冒合法用户伪造信息在网上传送；

中断(interruption) 使系统中断,不正常工作甚至瘫痪。如破坏通信设备,切断通信线路,破坏文件系统等。除了上述物理性破坏之外,攻击者还通过对特定目标发送大量的信息流,使目标超载乃至瘫痪,不能正常提供网络服务。

网络安全的设计中,应该充分考虑到抵御上述各种攻击的能力。1989 年国际标准化组织在 ISO7498-2 中提出了网络安全结构 SA,称为 ISO-SA,它规定的计算机网络安全服务涉及以下 5 个方面：

身份认证(authentication) 鉴别某一成员的身份是否与其声称的身份一致,可以防御假冒攻击；

访问控制(access control) 即对访问网络的权限加以控制,规定每个用户对网络资源的访问权限,使得网络资源不被非授权用户所访问和使用；

数据保密(data confidentiality) 为用户提供保密通信服务,使得网上传输的信息不被非授权用户所获知,保密性技术是基于密码机制的；

数据完整(data integrity) 使数据在网络传输过程中不被未授权者修改、替换和删除等；

不可否认(nonrepudiation) 为通信用户提供保护以免对方否认所进行的信息交换,包括发送者和接收者的不可否认。

15-2 什么是密码技术中的 Kerckoff 原则？为什么有这样的原则？

解答：密码技术中的 Kerckoff 原则是:加密和解密算法是公开的,而密钥是保密的。在现代密码学研究中加密和解密算法是要经过极大的努力进行设计、测试和安装的,一般要经过几年时间才能改变,因此将加密和解密算法本身进行保密的做法在现实中并不可行。而密钥是相对较短的字符串,可以根据需要容易地频繁地改变,容易进行保密。因此,就有 Kerckoff 原则。

15-3 什么样的密钥是计算上不可破译的？试举一例说明。

解答：保守密钥的秘密无疑是防止攻击的关键。对于攻击者来说，密钥的穷举猜测是一种重要攻击手段。但当密钥足够长且随机分布时，以当时的计算水平，穷举猜测实际上难以实现。即使使用当时最先进的计算机系统，穷举猜测也需要相当漫长的时间，这样的密钥是计算上不可破译的。实用的密码体制一般都是计算上不可破译的，而不是理论上不可破译的。

比如，当密钥长度为二进制 128 比特，则密钥空间为 2^{128} ，约 3.4×10^{38} 。若最快的计算机系统可以达到每微秒对密钥空间进行 500 万次搜索的计算速度，那么完成密钥空间全部搜索的时间也将超过 2×10^{18} 年，可见，穷举猜测实际上难以实现。

15-4 画图简要说明对称密钥密码体制的加密解密过程。

解答：对称密钥密码体制的加密和解密变换过程示于图 1-15-1。图中，用 $C = E_K(P)$ 表示使用加密算法 $E()$ 和密钥 K 对明文 P 加密得到密文 C ，类似地，用 $P = D_K(C)$ 表示使用解密算法 $D()$ 和密钥 K 对密文 C 解密得到明文 P ，那么加密解密过程为： $D_K(E_K(P)) = P$ 。



图 1-15-1 对称密钥密码体制的加密解密过程

15-5 DES 密钥长度为 56 比特，假设某台计算机每微秒可执行 10 次 DES 算法，那么，搜索完整个密钥空间需要多少年？如果密钥长度扩大到 128 比特呢？

解答：56 比特密钥： $(2^{56} \text{ 次} \div 10 \text{ 次} / \mu\text{s}) \times 10^{-6} \text{ s} / \mu\text{s} \div 3600 \text{ s} / \text{h} \div 24 \text{ h} / \text{d} \div 365 \text{ d} / \text{年} = 228 \text{ 年}$ ；

128 比特密钥： $(2^{128} \text{ 次} \div 10 \text{ 次} / \mu\text{s}) \times 10^{-6} \text{ s} / \mu\text{s} \div 3600 \text{ s} / \text{h} \div 24 \text{ h} / \text{d} \div 365 \text{ d} / \text{年} = 1.08 \times 10^{24} \text{ 年}$ 。

15-6 画图简要说明公开密钥密码体制的加密解密过程。

解答：公开密钥密码体制的算法过程如图 1-15-2 所示。发送者使用加密算法 $E()$ 和加密密钥 PK 对明文 P 加密后，接收者使用解密算法 $D()$ 和解密密钥 SK 解密即可恢复出明文，那么加密解密过程为： $D_{SK}(E_{PK}(P)) = P$ 。因为只有私钥 SK 的拥有者才能对 P

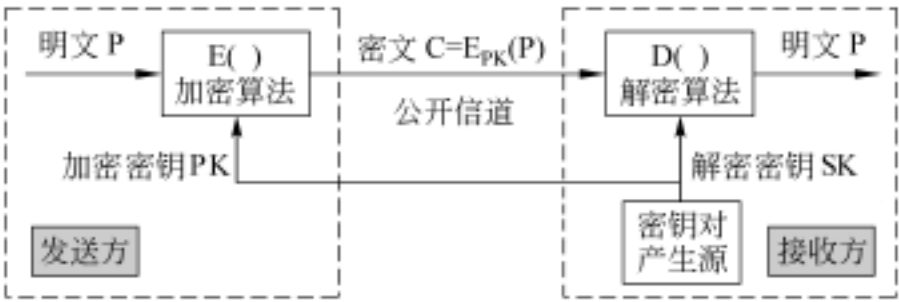


图 1-15-2 公开密钥体制的加密解密过程

解密,这就保证了消息的保密性。

15-7 试举一个简单的例子,说明 RSA 算法生成密钥的方法,并用生成的密钥对一个简单的明文进行加密,然后再解密。

解答: 以下用一个简单的例子来说明 RSA 生成密钥的方法。

选择两个素数,设为: $p=3$, $q=17$,计算出 $n = pq = 3 \times 17 = 51$ 。

计算 $\phi(n) = (p-1)(q-1) = 2 \times 16 = 32$ 。

从 $[0, (n)-1] = [0, 31]$ 中选择一个与 32 互素的数 e ,选 $e=5$ 。

由 $e \times d = 1 \pmod{\phi(n)}$,有 $5d = 1 \pmod{32}$,解出 $d=13$ 满足。

于是得出密钥: 公开密钥 $PK = \{e, n\} = \{5, 51\}$, 秘密密钥 $SK = \{d, n\} = \{13, 51\}$ 。

下面使用上例得到的密钥进行加密和解密。首先将明文划分为一个个分组,使得每个明文分组的二进制值不超过 n ,即不超过 51。现在设明文的一个分组为 $P=12$ 。

使用公开密钥 $PK = \{5, 51\}$ 加密。先计算 $P^e = 12^5 = 248\ 832$,再除以 51,商为 4 879,余数为 3。这就是对应于明文 12 的密文,即 $C=3$ 。

使用秘密密钥 $SK = \{13, 51\}$ 解密。先计算 $C^d = 3^{13} = 1\ 594\ 323$ 。再除以 51,得出商为 31 261,余数为 12。此余数即解密后应得出的明文,即 $P=12$ 。

15-8 为保证报文的真实可靠,数字签名应该满足哪三点要求? 画图说明使用公开密钥算法的数字签名并说明它如何满足上述三点要求。

解答: 为保证报文的真实可靠,数字签名应该满足以下三点要求:

可校验 接收者能够核实报文确实是由发送者签发;

不可篡改和伪造 数字签名的报文无法被中途窃取者和接收者所篡改和伪造;

不可否认 发送者事后无法否认他签发的报文。

采用公开密钥算法的数字签名如图 1-15-3。发送者 A 用其秘密密钥 $SK-A$ 对所发报文 P 进行加密运算,将结果 $D_{SK-A}(P)$ 传送给接收者 B。B 收到后,用已知的 A 的公开密钥 $PK-A$ 解密得出: $E_{PK-A}(D_{SK-A}(P)) = P$ 。这一过程示于图 1-15-3。

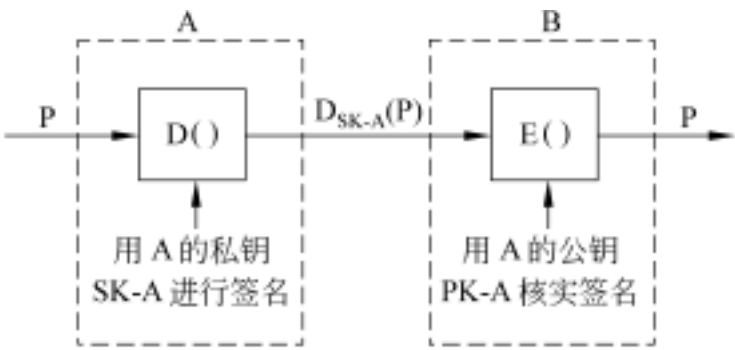


图 1-15-3 采用公开密钥算法的数字签名

因为报文要用 A 的公开密钥才能解密,所以是用 A 的秘密密钥加密的,因此, B 可以确认报文 P 一定是 A 签名发送的。因为报文只能用 A 的秘密密钥进行签名,中途窃取者和接收者无法进行篡改和伪造。假若 A 欲否认曾发送报文给 B, B 可将 P 及 $D_{SK-A}(P)$ 出示给第三者,第三者很容易用 $PK-A$ 由 $D_{SK-A}(P)$ 得到 P,证实是 A 签发了报文 P。可见,数字签名可以如何满足上述三点要求,提供报文源的认证和报文的完整性传输。

15-9 为什么明文 P 的报文摘要 MD(P)可以充分地代表 P?

解答：报文摘要算法具有如下特点：

给定一个报文 P ，容易计算其报文摘要 $MD(P)$ ，但反过来，给定一个报文摘要 X ，想由 X 找到一个报文 P 使得 $MD(P) = X$ ，在计算上不可行；

若想找到任意两个报文 P 和 P' ，使得 $MD(P) = MD(P')$ ，在计算上也不可行。

上述的两个条件表明： $MD(P)$ 可以充分地代表 P ，若 P 和 $MD(P)$ 是发送者产生的报文和报文摘要，即使攻击者截获了 P 和经数字签名的 $MD(P)$ 并得到了 $MD()$ ，攻击者也不可能由 P 和 $MD(P)$ 伪造出另一个报文 P' ，使得 P' 和 P 具有同样的报文摘要。

15-10 和一般的数字签名相比，使用报文摘要的数字签名的优点是什么？

解答：数字签名一般采用公开密钥算法对整个报文进行加密和解密处理，处理时间长，尤其是长度大的文件。而且在网络应用中，许多报文并无加密要求（但也需要防止篡改、伪造和否认），对于不需要加密的报文进行加密和解密，也给计算机增加了不必要的负担。报文摘要就是一种有效的提高处理效率的改进方法。

报文摘要将发送的长的报文映射到一个短的位串，即报文摘要。仅对短的定长报文摘要进行数字签名，要比对整个长报文进行数字签名要简单省时得多。发方将经数字签名的报文摘要加在未经数字签名的报文后面一起发送，收方收到的报文后进行相关的计算就可以确认收到的报文就是由 A 签发的非篡改和伪造的报文 P 。这样，使用报文摘要的数字签名既保持了数字签名的作用，又节省了处理时间。

15-11 为什么建立密钥分发中心(KDC)？它的作用是什么？

解答：对称密钥密码体制中，加解密的双方使用相同的密钥。对称密钥密码体制的最大问题是如何将共享密钥安全地传送给对方。可以事先约定，还可以用信使来传送，这称为网外分发方式。但在大型计算机网络中，用信使来传送密钥显然是不合适的。如果事先约定密钥，就会给密钥的管理和更换都带来极大的不便。网上的主机通常要和很多主机通信，而且为了安全，密钥还要经常改变，这就使密钥的选定、分发和管理的工作量很大。为此，一般采取网内分发方式，对密钥进行自动分发。建立通信双方都信任的密钥分发中心(KDC)是目前常用的网内分发方式，KDC 为通信双方生成和分发通信用的会话密钥。KDC 保存有所有注册用户和它通信的共享密钥，KDC 使用它们和各用户进行加密通信。

15-12 公钥密码体制中，在不知道对方的公钥情况下，一个攻击者欲欺骗用户 B ，冒充用户 A 与通信 B 通信，攻击者可以如何进行欺骗？

解答：攻击者可以伪造一个用户 A 的报文发送给用户 B ，但此报文用攻击者自己的秘密密钥进行数字签名且附上自己的公开密钥，并谎称是 A 的公开密钥。用户 B 不知道对方的公开密钥，用攻击者的公钥解密报文并继续与攻击者通信，却以为自己在与 A 在会话。

15-13 从技术上讲，防火墙主要分为哪两类？它们分别工作的网络的什么层次？简述这两种防火墙技术。

解答：从技术上讲，目前防火墙主要分为两类，一类使用包过滤技术，由包过滤路由器实现；另一类使用代理服务技术，由应用网关实现，应用网关也称为代理服务器。两种防火墙技术可以组合在一起，形成某种结构的防火墙系统。

包过滤路由器工作在 Internet 的 IP 层,位于内部网络和外部网络的连接处,根据 IP 和 TCP/UDP 的首部进行 IP 包的过滤。IP 包过滤软件可以根据源地址、目的地址、源端口号、目的端口号等对 IP 包进行过滤,允许或阻拦来自或去往某些 IP 地址或端口的访问。包过滤路由器的优点就是结构和实现比较简单,但 IP 包过滤的访问控制只能控制到 IP 地址和端口级,无法做到用户级别的身份认证和访问控制。

应用网关工作在网络的应用层。应用网关针对特定的应用构建,内部网络通常需要有多个应用网关,比如, Telnet 网关、HTTP 网关、FTP 网关和 E-mail 网关等。多个应用代理服务程序可以同时运行在同一个主机上。所有的网络入/出访问都必须通过相应的应用网关代理。应用网关可以进行用户级的身份认证、日志记录和账号管理。但要想提供全面的安全保证,就要对每一项服务都要建立对应的应用网关。

15-14 防火墙的体系结构主要分为哪几种?画图并简要描述它们。

解答:防火墙的体系结构主要分为以下 4 种:

包过滤防火墙(packet filtering firewall)

双穴主机网关防火墙(dual-homed gateway firewall)

屏蔽主机网关防火墙(screened host gateway firewall)

屏蔽子网防火墙(screened subnet firewall)

1. 包过滤防火墙

包过滤防火墙如图 1-15-4 所示,这种防火墙结构使用包过滤路由器,它位于内部网络和外部 Internet 的连接处,是数据流的惟一通道,进行包过滤处理,阻断不合法的数据包。

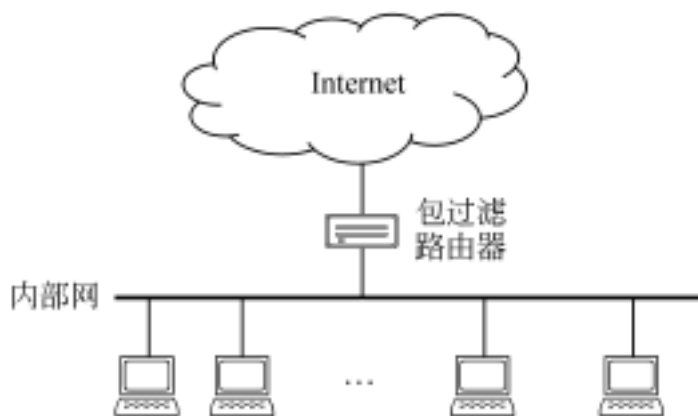


图 1-15-4 包过滤防火墙

2. 双穴主机网关防火墙

双穴主机网关防火墙系统如图 1-15-5 所示,它使用一台双穴主机作为堡垒主机,双穴主机是用一台装有两块网卡的主机,两块网卡分别与内部网络和外部网络相连,物理连接上就像包过滤路由器一样,外部网络和内部网络之间的通信必须经由双穴主机。双穴主机运行各种应用网关代理服务程序,通过网络服务代理提供网络安全控制。

双穴主机网关防火墙另一种常用的结构是在双穴主机外侧再连接一台包过滤路由器,通过它连接到外部网络。

3. 屏蔽主机网关防火墙

这种防火墙中,内部网络通过一台包过滤路由器连接到外部网络,内部网络上再设置

一台堡垒主机运行应用网关代理服务程序。包过滤路由器和堡垒主机一起构成屏蔽主机网关防火墙。屏蔽主机网关防火墙如图 1-15-6 所示。

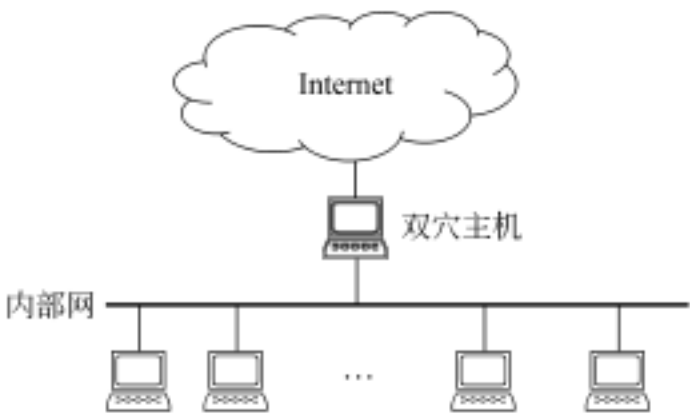


图 1-15-5 双穴主机网关防火墙



图 1-15-6 屏蔽主机网关防火墙

一般情况下,包过滤路由器只准许外部网络与堡垒主机通信,使堡垒主机成为外部网络所能到达的惟一结点,并根据建立的过滤规则进行访问控制,网络服务由堡垒主机上相应的应用代理服务程序来支持。对于内部网络中的主机直接对外的通信,包过滤路由器将予以拒绝,必须通过堡垒主机代理对外部网络的访问。

4 . 屏蔽子网防火墙

屏蔽子网防火墙如图 1-15-7 所示。屏蔽子网防火墙在内部网络和外部网络之间建立一个独立的周边子网,又称为非军事区 DMZ,使用内部包过滤路由器和外部包过滤路

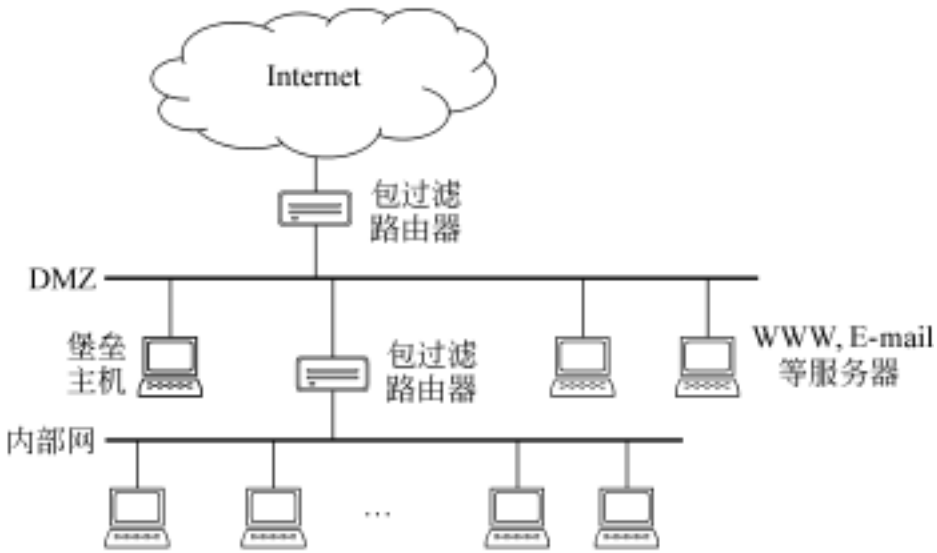


图 1-15-7 屏蔽子网防火墙

由器将这一子网分别与内部网络和外部网络连接,周边子网中设有一台堡垒主机。在两个包过滤路由器上都可以设置过滤规则,堡垒主机运行应用代理服务程序,进行网络服务代理。

DMZ 用来作为一个额外的缓冲区以进一步隔离内部网络和外部网络。企业对外的信息服务器,如 WWW、E-mail 服务器等,一般放在 DMZ 内。

内部网络和外部网络均能访问 DMZ 上的某些资源,但一般不能通过 DMZ 让内部网络和外部网络直接进行信息传输,跨越防火墙的数据流需经过外部包过滤路由器、堡垒主机和内部包过滤路由器。

15-15 简述 IP 层安全协议的认证首部(AH)和封装安全净荷(ESP)的作用。

解答:认证首部 AH 提供 IP 数据报的完整性校验和源站身份认证,但不提供数据报的加密。AH 可防范 IP 欺骗等重要的网络攻击。AH 对 IP 数据报(除传输中会发生变化的 TTL、头校验和、片偏移之外的所有字段)计算报文摘要后再进行数字签名,即计算报文认证码 MAC,MAC 存于 AH 的一个字段之中。AH 标准规定必须支持报文摘要算法 MD5 和 SHA-1。在数据报传输过程中,中间的路由器都不检查 AH 首部,到达目的站时才做处理,进行源站认证和数据报的完整性校验。

ESP 比 AH 复杂,可以实现数据完整性校验和源站身份认证,还可以实现 IP 数据报的加密。完整性校验和认证也基于报文认证码 MAC 的计算,ESP 实现也必须支持 MD5 和 SHA-1,IP 数据报的加密要求支持 DES-CBC。

15-16 传输层安全协议 TLS 工作在什么层?由哪两层组成?

解答:TLS 协议工作在传输层,在 TCP 之上,应用层之下。TLS 由两层协议组成,上层主要是 TLS 握手协议,还有密码变更规范协议和报警协议,下层是 TLS 记录协议。

15-17 根据图 1-15-8 所示的 PGP 加密发送电子邮件的过程,画图并说明用户 B 接收到用户 A 的邮件后 PGP 的操作过程。

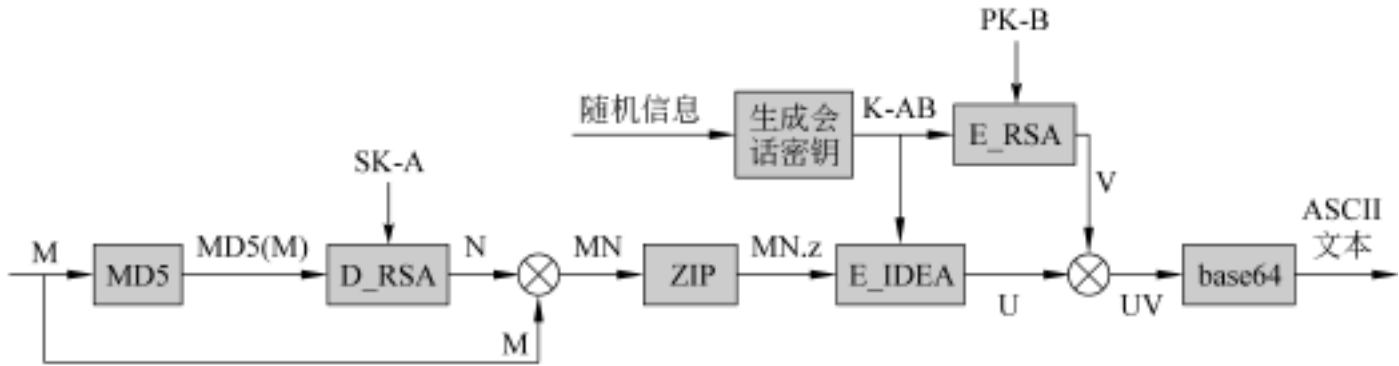


图 1-15-8 PGP 加密发送电子邮件的过程

解答:收方用户 B 接收到邮件后 PGP 的操作与发送时的加密过程相反,如图 1-15-9 所示,图中仍使用 PGP 发送图中所使用的符号,但这里代表接收到的和经过接收处理的信息。

接收后的解密操作过程说明如下:

对收到的邮件 ASCII 码文本进行 base64 算法解码运算 d_base64(), 得到 UV 并将它分开;

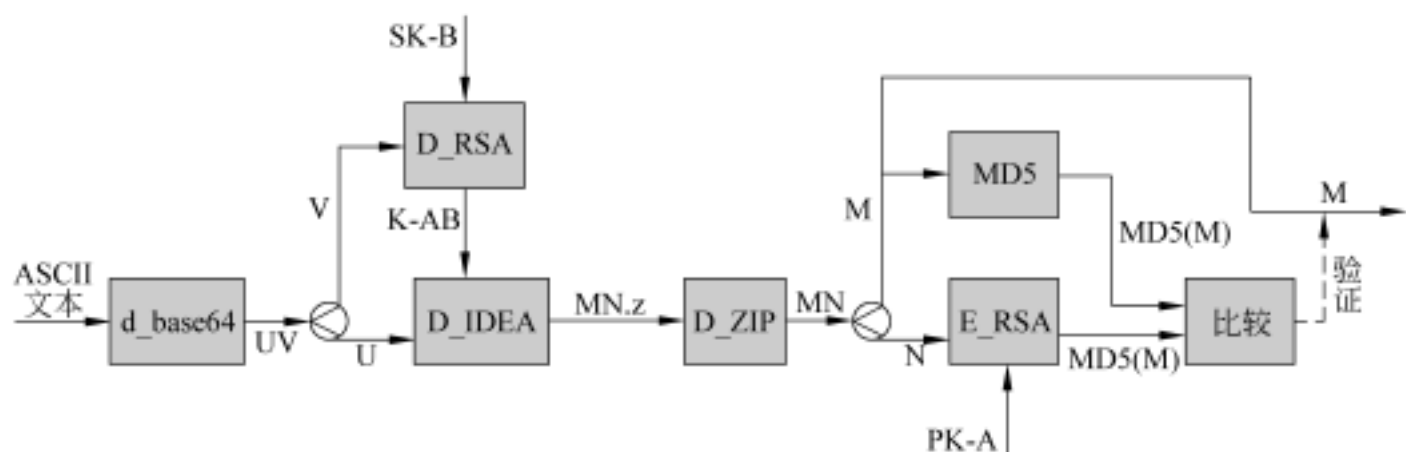


图 1-15-9 用户 B 接收到用户 A 的邮件后的 PGP 解密操作过程

使用自己的私钥 SK-B 和 D_RSA() 算法对 V 进行解密运算, 得到 IDEA 算法的会话密钥 K-AB, 即 $K-AB = D_RSA_{SK-B}(V)$;

使用会话密钥 K-AB 和算法 D_IDEA() 对 U 进行解密运算, 得到 MN.z 即 $MN.z = D_IDEA_{K-AB}(U)$;

对 MN.z 进行解压缩运算 D_ZIP(), 得到 MN 并将 MN 分开, M 是收到的邮件, N 是邮件的报文认证码 MAC;

使用 A 的公钥 PK-A(B 有 A 的公钥) 和算法 E_RSA() 对 N 进行解密运算, 得到 MD5(M), 即 $MD5(M) = E_RSA_{PK-A}(N)$;

对收到的电子邮件 M 进行报文摘要 MD5 运算, 也应该得 MD5(M)。比较运算结果是否与第(5)步得到的 MD5(M)一致, 核实用户 A 对电子邮件报文摘要的电子签名, 如果一致, 那么用户 B 知道收到的电子邮件确实是来自用户 A, 而且邮件也是正确的。

15-18 对照 ISO/OSI 参考模型各个层中的网络安全服务, 在物理层可以采用 (1) 加强通信线路的安全; 在网络层可以采用 (2) 来处理信息内外网络边界流动和建立透明的安全加密信道; 在传输层主要解决进程到进程间的加密, 最常见的传输层安全技术有 (3); 为了将低层安全服务进行抽象和屏蔽, 最有效的一类做法是可以在传输层和应用层之间建立 (4) 层次实现通用的安全服务功能, 通过定义统一的安全服务接口向应用层提供安全服务。

- | | | | |
|---------------|-----------|------------|-----------|
| (1) A . 防窃听技术 | B . 防火墙技术 | C . 防病毒技术 | D . 防拒认技术 |
| (2) A . 防窃听技术 | B . 防火墙技术 | C . 防病毒技术 | D . 防拒认技术 |
| (3) A . SET | B . IPsec | C . S-HTTP | D . SSL |
| (4) A . 防火墙 | B . 认证中心 | C . 中间件 | D . 数据加密 |

答案: A, B, D, C

15-19 防火墙是建立在内外网络边界上的一类安全保护机制, 它的安全架构基于 (1)。双穴主机防火墙上装有 (2), 其上运行的是 (3), 其中用户身份认证在 (4) 进行。而 IP 过滤型防火墙在 (5) 通过控制网络边界的信息流动, 来强化内部网络的安全性。

- | | |
|----------------|------------|
| (1) A . 流量控制技术 | B . 加密技术 |
| C . 信息流填充技术 | D . 访问控制技术 |

- (2) A . 一块网卡且有一个 IP 地址 B . 两个网卡且有两个不同的 IP 地址
 C . 两个网卡且有相同的 IP 地址 D . 多个网卡且动态获得 IP 地址
- (3) A . 代理服务器软件 B . 网络操作系统
 C . 数据库管理系统 D . 应用软件
- (4) A . 网络层 B . 会话层 C . 物理层 D . 应用层
- (5) A . 应用层 B . 数据链路层 C . 网络层 D . 会话层

答案: D, B, A, D, C

15-20 防火墙系统通常由__(1)___组成,防止不希望的、未经授权的通信进出被保护的内部网络,它__(2)___内部网络的安全措施,也__(3)___感染了病毒的软件带来的安全问题。

- (1) A . 杀病毒卡和杀毒软件 B . 代理服务器和入侵检测系统
 C . 过滤路由器和入侵检测系统 D . 过滤路由器和代理服务器
- (2) A . 可以替代 B . 不能替代 C . 是一种 D . 是外部和
- (3) A . 物理隔离了 B . 能够区分 C . 不能解决 D . 可以解决

答案: D, B, C

15-21 公钥密码体制是__(1)___。常用的公钥加密算法有__(2)___,它可以实现加密和数字签名。传统密码体制是__(3)___,它最基本的加密算法是__(4)___。

- (1) A . 对称密钥技术,有 1 个密钥 B . 非对称密钥技术,有 2 个密钥
 C . 对称密钥技术,有 2 个密钥 D . 非对称密钥技术,有 1 个密钥
- (2) A . DES B . IDES C . 三重 DES D . RSA
- (3) A . 对称密钥技术,有 1 个密钥 B . 非对称密钥技术,有 2 个密钥
 C . 对称密钥技术,有 2 个密钥 D . 非对称密钥技术,有 1 个密钥
- (4) A . RSA B . IDES C . 三重 DES D . DES

答案: B, D, A, D

15-22 在分布式环境中实现身份认证可以有多种方案,以下选项中最不安全的身份认证方案是_____。

- A . 用户发送口令,由通信对方指定共享密钥
B . 用户从 KDC 获取会话密钥
C . 用户从 CA 获取数字证书

答案: A

15-23 数字公钥证书采用公钥体制进行加密和解密。X.509 标准规定,公钥证书由__(1)___发放,将其放入公共目录中,以供用户访问。X.509 数字证书中的签名字段是指__(2)___。如果发送方要向一个陌生人发送保密信息,又没有对方的公钥,那么他可以__(3)___。

- (1) A . 密钥分发中心 B . 证书权威机构
 C . 国际电信联盟 D . 当地政府
- (2) A . 用户对自己证书的签名 B . 用户对发送报文的签名
 C . 发证机构对用户证书的签名 D . 发证机构对发送报文的签名

- (3) A . 向对方打电话索取公钥
- B . 从公钥证书权威机构获取对方的公钥
- C . 制造一个公钥发给对方
- D . 向对方发一个明文索取公钥

答案: B, C, B

15-24 A 向 B 发送消息 P, 并使用公钥体制进行数字签名。设 E 表示公钥, D 表示私钥, 则 B 要保留的证据是 (1)。基于数论原理的 RSA 算法的安全性建立在 (2) 的基础上。和对称密钥密码体制的 DES 算法相比, RSA 算法的速度 (3), 不适于 (4)。

- (1) A . $E_A(P)$ B . $E_B(P)$ C . $D_A(P)$ D . $D_B(P)$
- (2) A . 大数难以分解因子 B . 大数容易分解因子
- C . 容易获得公钥 D . 私钥容易保密
- (3) A . 快 B . 慢 C . 相等 D . 差不多
- (4) A . 少量数据的加密 B . 对报文摘要进行数字签名
- C . 密钥分发 D . 大量数据的加密

答案: C, A, B, D

第二部分

实验指导

- 实验一 以太网组建
- 实验二 虚拟局域网
- 实验三 FTP 服务器的配置与管理
- 实验四 Web 服务器的配置
- 实验五 DNS 服务器的配置与管理
- 实验六 电子邮件服务器的配置与管理
- 实验七 DHCP 服务器的配置与管理
- 实验八 常用网络操作命令
- 实验九 Socket 网络通信程序设计

实验一

以太网组建

在本实验中,采用 5 类非屏蔽双绞线(UTP)作为传输介质组建以太网。通过组建以太网,可以熟悉构建局域网所使用的基本设备、器件和工具,学习非屏蔽双绞线电缆的制作方法,了解网卡的配置方法,了解以太网的连通性测试方法。

1.1 实验设备、器件及测量工具

1. 所需设备和器件

根据组建以太网的类型(10Mb/s、100Mb/s),选择相应的实验设备。

10Mb/s:一台 10M 以太网集线器(两台可以做级联);两台微机(自带独立网卡或集成网卡);RJ-45 水晶接头 4 个以上;3 类以上非屏蔽双绞线。

100 Mb/s:一台 100M 以太网集线器(两台可以做级联);两台微机(自带独立网卡或集成网卡);RJ-45 水晶接头 4 个以上;5 类以上非屏蔽双绞线。

2. 制作 UTP 电缆接头及连通性测试工具

制作 UTP 电缆接头及连通性测试工具如图 2-1-1 所示。



a—剥线钳；b—夹线钳；c—电缆测试仪

图 2-1-1 制作 UTP 电缆接头及连通性测试工具

3 . 制作非屏蔽双绞线

首先,根据图 2-1-3、图 2-1-4 来决定制作所需的 UTP 电缆,然后,根据图 2-1-2 来排列线对。用夹线钳将 RJ-45 水晶头与非屏蔽双绞线相连,最后,用电缆测试仪检测该电缆的连通性。

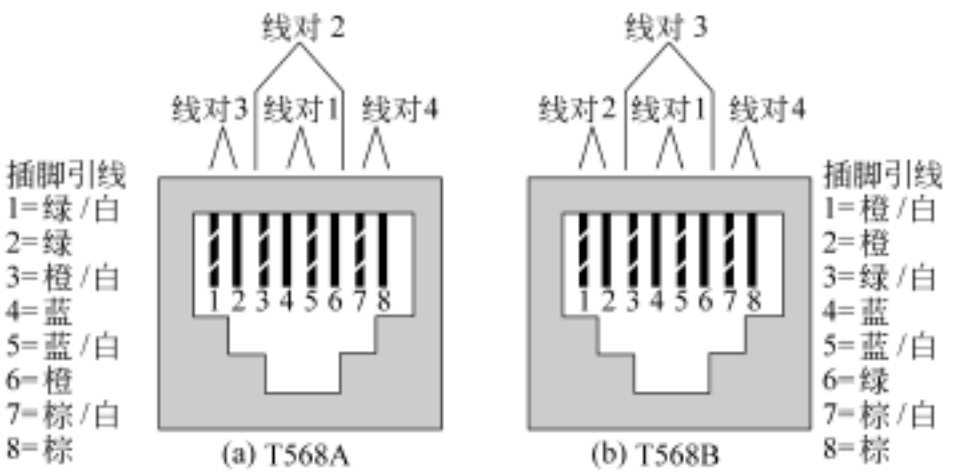


图 2-1-2 RJ-45 接头的以太网标准

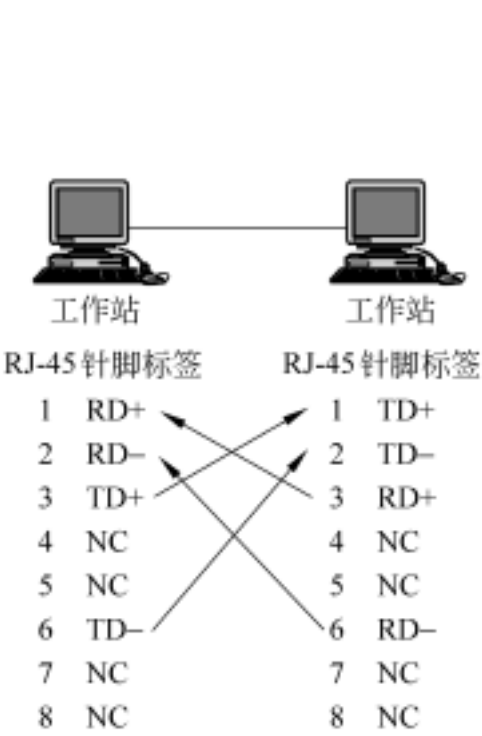


图 2-1-3 交叉线缆

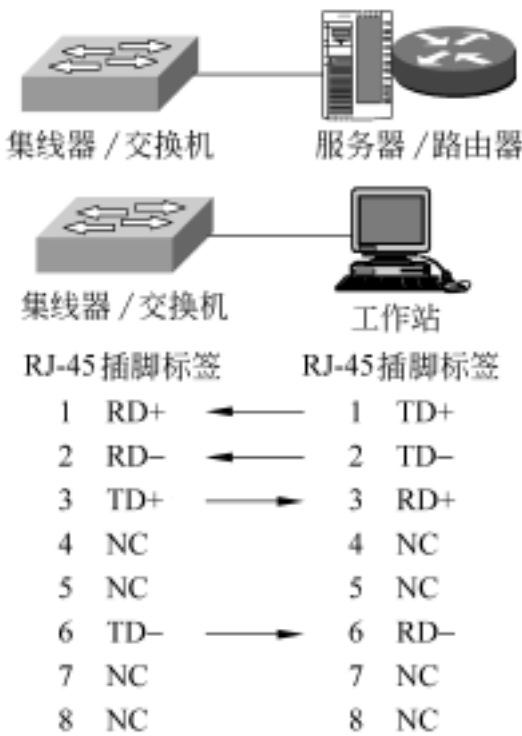


图 2-1-4 直通线缆

4 . 安装以太网卡

网卡是计算机与网络的接口,简称为 NIC。目前,大部分微机都自带独立网卡或与主板集成的网卡,一般来说,网卡都支持即插即用的配置方式,现今流行的操作系统(如 Windows 系列)也都支持即插即用。所以,由操作系统自动完成对网卡驱动的安装,我们所要做的只是为网卡分配一个固定的 IP 地址,如: 192 .168 .1 .3/ 24; 192 .168 .1 .100/ 24。

网卡驱动安装后,分配 IP 地址的方法如下:

单击“开始”“设置”“网络和拨号连接”,出现如图 2-1-5 所示窗口。

在图 2-1-5 中,右击“本地连接”“属性”,弹出如图 2-1-6 所示界面。



图 2-1-5 “网络和拨号连接”窗口

在图 2-1-6 中,选择 Internet 协议(TCP/ IP),然后单击“ 属性 ”,弹出图 2-1-7 所示对话框,并在该窗口中选择“ 使用下面的 IP 地址选项 ”,填入相应的 IP 地址即可。



图 2-1-6 属性设置界面



图 2-1-7 分配 IP 地址界面

5. 将微机接入网络

用做好的 UTP 电缆将微机 and 集线器(hub)连接起来,就形成了一个如图 2-1-8 所示

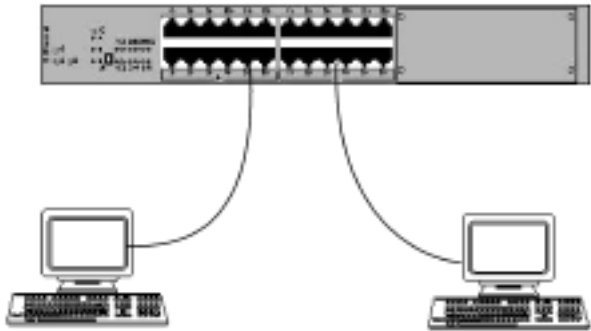


图 2-1-8 简单以太网示意图

的简单以太网。

1.2 网络连通性测试

硬件连接完成之后,分别将微机和 hub 的电源打开,待 hub 启动后,可分别观察与微机相连的 hub 端口、微机上网卡的状态指示灯,以确定网络的连通性。

另一种常用的测试网络连通性的方法是用 ping 命令,如图 2-1-9 所示。

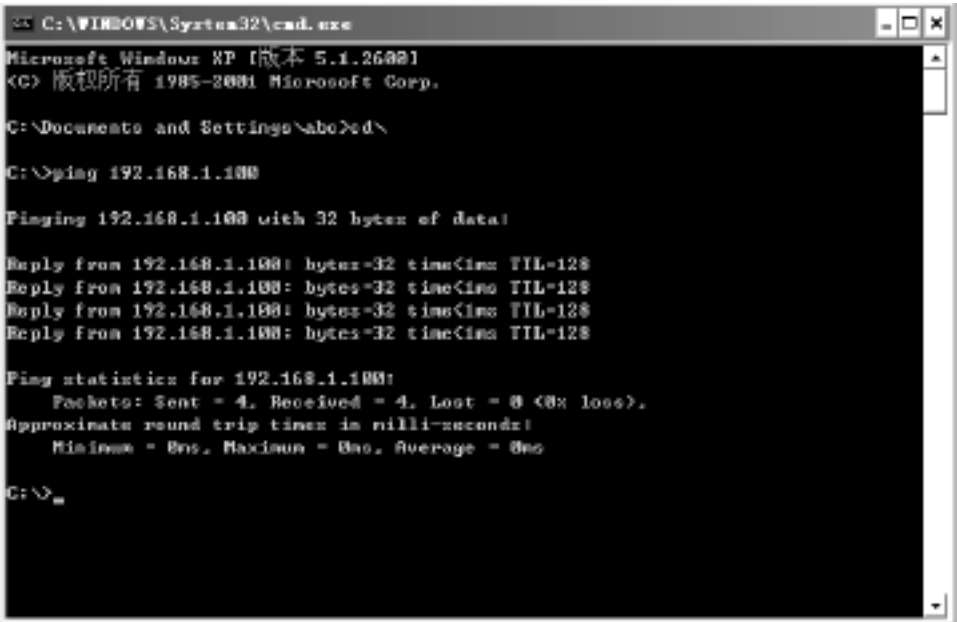


图 2-1-9 连通性测试(1)

如果网络不通, ping 命令将给出超时提示,这时,就需要重新检查网络的硬件和软件。

1.3 多个集线器相连

hub 的连接有两种方式:堆叠和级联。

(1) 堆叠:用专用的堆叠电缆,将 hub 连接起来。

(2) 级联:有两种方式进行 hub 的级联。

对于具有级联端口的 hub:

用直通 UTP 电缆将一台 hub 的级联端口与一台 hub 的普通端口相连。

对于不具备级联端口的 hub:

用交叉 UTP 电缆连接两台 hub。

两台计算机分别接到两个 hub,然后采用实验一 1.2 节中所描述的方法,进行连通性测试。

实验二

虚拟局域网

以太网交换技术的一个主要特征是 VLAN,它使用交换机将工作站和服务器聚集到逻辑概念上的组中。在一个 VLAN 中的设备只能够与在同一个 VLAN 中的设备通信,这样,一个交换式的网络工作起来就像是许多互不相联的单独的 LAN 一样。

虚拟网络技术打破了地理环境的制约,在不改动网络物理连接的情况下可以任意将工作站在工作组或子网之间移动,工作站组成逻辑工作组或虚拟子网,提高信息系统的运作性能,均衡网络数据流量,合理利用硬件及信息资源。同时,利用虚拟网络技术,大大减轻了网络管理和维护工作的负担,降低网络维护费用。随着虚拟网络技术的应用,随之必然产生了在虚拟网间如何通讯的问题。

VLAN 在交换机上的实现方法,可以大致划分为 6 类:

- 基于端口划分的 VLAN;
- 基于 MAC 地址划分 VLAN;
- 基于网络层协议划分 VLAN;
- 根据 IP 组播划分 VLAN;
- 按策略划分 VLAN;
- 按用户定义、非用户授权划分 VLAN。

实验中采用第一种方式,即基于端口划分 VLAN。

2.1 实验内容

- (1) 在两个不同交换机上分别建立 VLAN2、VLAN3
- (2) 两个不同交换机上的同一个 VLAN(VLAN2、VLAN3)分别进行通信
- (3) 分析内容二中实现方法的弊病,利用“中继”实现内容(2)
- (4) 通过三层交换机实现不同 VLAN 之间的通信

2.2 实验环境

Catalyst 3500 series XL 24 口及 48 口交换机各一台,Catalyst 4006 三层交换机一台;两台微机;网线。

为了下面描述方便,以下称 Catalyst 3500 24 口交换机为 A、48 口交换机为 B,

Catalyst 4006 三层交换机为 C。

2.3 实验步骤

1. 通过命令行界面配置 Cisco Catalyst 3500—24
首先,用串口线将一台微机与一台交换机的 Console 端口相连,然后,单击“开始”“程序”“附件”“通讯”“超级终端”,如图 2-2-1 所示。
2. 按照提示,为这个新建的连接指定一个名称为 test,然后单击“确定”按钮
如图 2-2-2 所示。



图 2-2-1 新建连接界面



图 2-2-2 “连接到”界面

3. 选择连接交换机 Console 口的微机的串口为 COM1
如图 2-2-3 所示。
4. 设置 COM1 端口的属性
选择“还原为默认值”,如图 2-2-4 所示。



图 2-2-3 设置波特率界面(1)



图 2-2-4 设置波特率界面(2)

5. 配置新交换机
按下“确定”按钮之后,出现空白的窗口,这时按下回车键就进入到交换机的命令行配置界面了,如果是新的交换机,交换机名默认为 Switch,提示符为: Switch > ,如图 2-2-5 所示。输入 enable(或缩写 ena)并回车,进入特权模式,此时提示符为: Switch #。

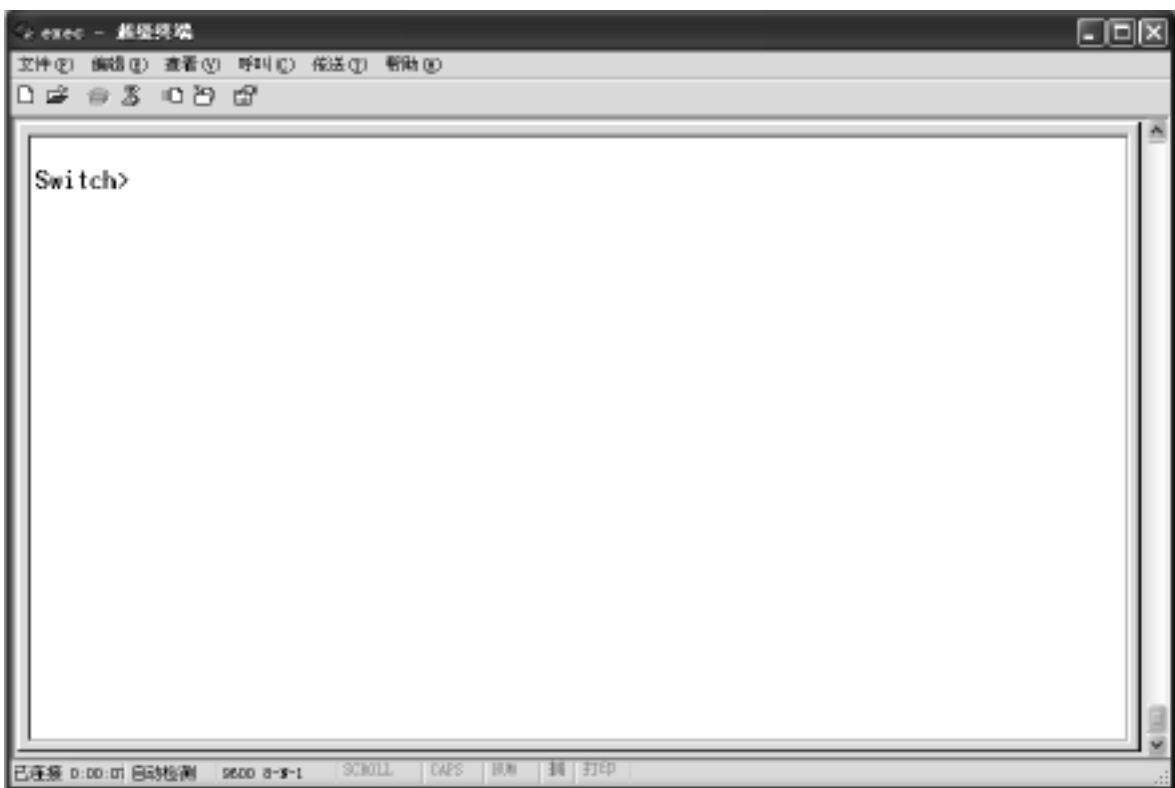


图 2-2-5 命令行配置界面

6 . 查看交换机中存储的内容

如果是没有做过配置的新交换机,那么,它的闪存目录(flash directory)里没有包含任何 VLAN 数据库文件(vlan .dat),也没有保存的配置文件(config .text)。其中,vlan .dat 文件用来储存本地 VLAN 的信息,交换机使用该文件与其他交换机共享 VLAN 的信息。我们首先看看交换机中存储了哪些内容,输入命令:

dir flash:

回车后将显示交换机内部 Flash 存储器中的文件,如图 2-2-6 所示。

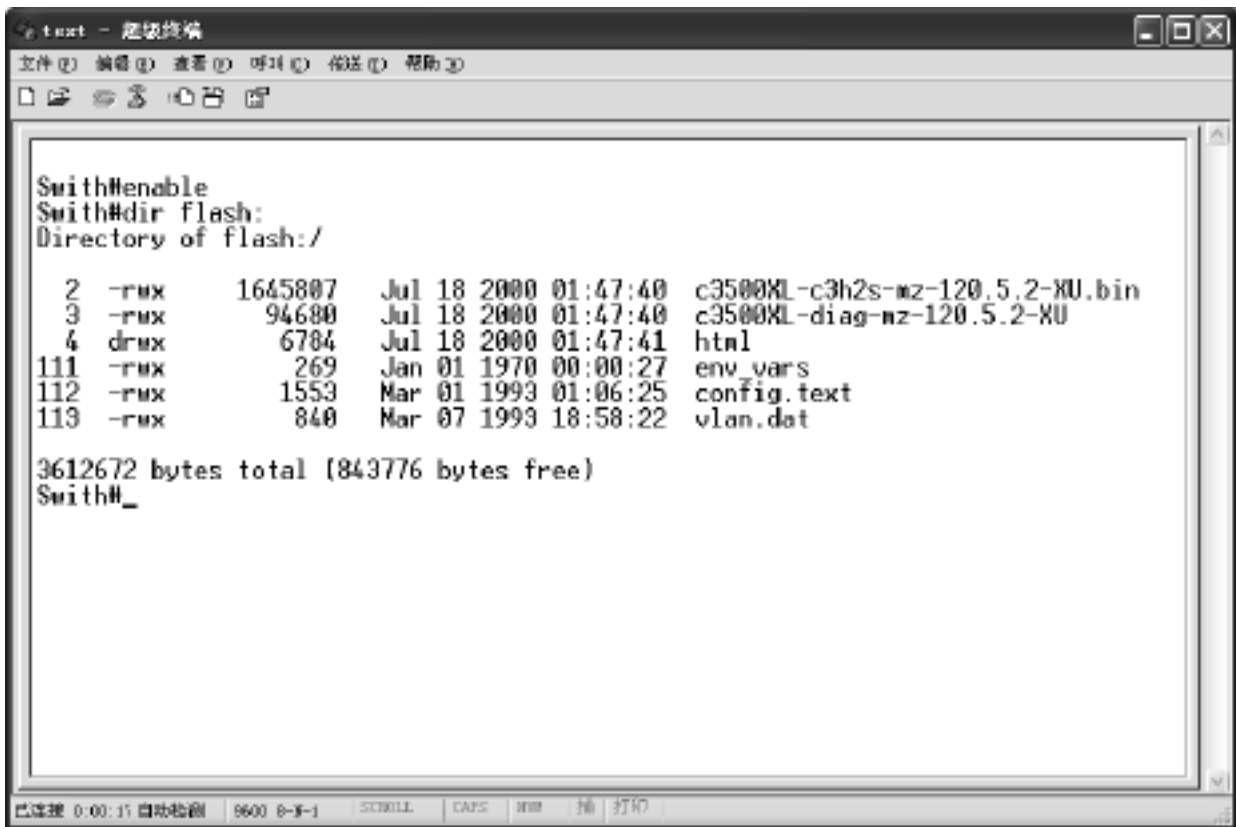


图 2-2-6 特权模式界面

7 . 查看交换机配置清单

格式:

```
Switch # show startup
```

该命令将显示出交换机的配置情况。从中可以看到交换机有几个快速以太网端口和几个 Gigabit 以太网端口等信息。

8 . 进行交换机的初始化配置

当交换机首次加电启动时,在它的运行配置文件中有默认的配置数据。交换机的默认名称为 Switch,控制台或虚拟终端(VTY)线路都没有设置密码。进行交换机的初始化配置的格式:

```
Switch # setup
```

9 . 创建 VLAN

创建 VLAN2 和 VLAN3,对 A,B 交换机分别进行如下配置:

(1) 配置 VLAN 之前,查看 VLAN 分配情况,输入格式:

```
Switch # show vlan
```

有关的显示如下:

VLAN Name	Status	Ports
1 default	active	Fa0/ 1, Fa0/ 2, Fa0/ 3, Fa0/ 4, Fa0/ 5, Fa0/ 6, Fa0/ 7, Fa0/ 8, Fa0/ 9, Fa0/ 10, Fa0/ 11, Fa0/ 12, Fa0/ 13, Fa0/ 14, Fa0/ 15, Fa0/ 16, Fa0/ 17, Fa0/ 18, Fa0/ 19, Fa0/ 20, Fa0/ 21, Fa0/ 22, Fa0/ 23, Fa0/ 24, Gi0/ 1, Gi0/ 2

(2) 创建 VLAN2、VLAN3,输入:

```
Switch # vlan database
Switch(vlan) # vlan 2 name jiance
VLAN 2 added:
    Name: jiance
Switch(vlan) # vlan 3 name xinxi
VLAN 3 added:
    Name: xinxi
Switch(vlan) # exit
Switch #
```

分别将 vlan 2 、 vlan 3 命名为 jiance 、 xinxi

(3) 将交换机 A 的 1, 2, 3, 4 端口分别加入 VLAN2;5, 6, 7, 8, 9 端口分别加入 VLAN3;将交换机 B 的 1, 2 端口分别加入 VLAN2;3、4 端口分别加入 VLAN3。

```
Switch(config) # interface fa0/ 1
Switch(config-if) # switch acc vlan 2
Switch(config-if) # exit
```

将端口 1 加入 vlan 2

```
Switch(config) # interface fa0/ 2
Switch(config-if) # switch acc vlan 2
Switch(config-if) # exit
```

将端口 2 加入 vlan 2

创建完成后查看 VLAN 信息：

```
Switch # show vlan
```

有关 A 交换机的显示如下：

VLAN Name	Status	Ports
1 default	active	Fa0/ 10, Fa0/ 11, Fa0/ 12, Fa0/ 13, Fa0/ 14, Fa0/ 15, Fa0/ 16, Fa0/ 17, Fa0/ 18, Fa0/ 19, Fa0/ 20, Fa0/ 21, Fa0/ 22, Fa0/ 23, Fa0/ 24, Gi0/ 1, Gi0/ 2
2 jiance	active	Fa0/ 1, Fa0/ 2, Fa0/ 3, Fa0/ 4,
3 xinxi	active	Fa0/ 5, Fa0/ 6, Fa0/ 7, Fa0/ 8, Fa0/ 9

有关 B 交换机的显示如下：

		Fa0/ 22, Fa0/ 23, Fa0/ 24, Fa0/ 25, Fa0/ 26, Fa0/ 27, Fa0/ 28, Fa0/ 29, Fa0/ 30, Fa0/ 31, Fa0/ 32, Fa0/ 33, Fa0/ 34, Fa0/ 35, Fa0/ 36, Fa0/ 37, Fa0/ 38, Fa0/ 39, Fa0/ 40, Fa0/ 41, Fa0/ 42, Fa0/ 43, Fa0/ 44, Fa0/ 45, Fa0/ 46, Fa0/ 47, Fa0/ 48, Gi0/ 1, Gi0/ 2
2 jiance	active	Fa0/ 1, Fa0/ 2
3 xinxi	active	Fa0/ 3, Fa0/ 4

(4) 两个不同交换机上的同一个 VLAN(如 VLAN2、VLAN3)进行通信

首先验证同一个交换机的同一个 VLAN 进行通信,如交换机 A 的端口 1 与端口 2(属于 VLAN2 通信),将两台微机的 IP 地址分别设置为如图 2-2-7、2-2-8 所示,并将其分别接到同一个 VLAN 的端口上;然后再验证不同交换机上的同一个 VLAN 进行通信,将两台微机分别接到两个不同交换机的同一个 VLAN 上。

图 2-2-9、2-2-10 证明同一台交换机上的 VLAN 中的机器通信成功,说明连线正确。

测试不同交换机上的同一个 VLAN 是否能够通信时,要将交换机 A 与 B 连起来,连接线必须连接到同一个 VLAN。

用同样的方法进行测试,通讯成功表明方法正确。

交换机 A 上的 VLAN3 与交换机 B 上的 VLAN3 此时能否通信？

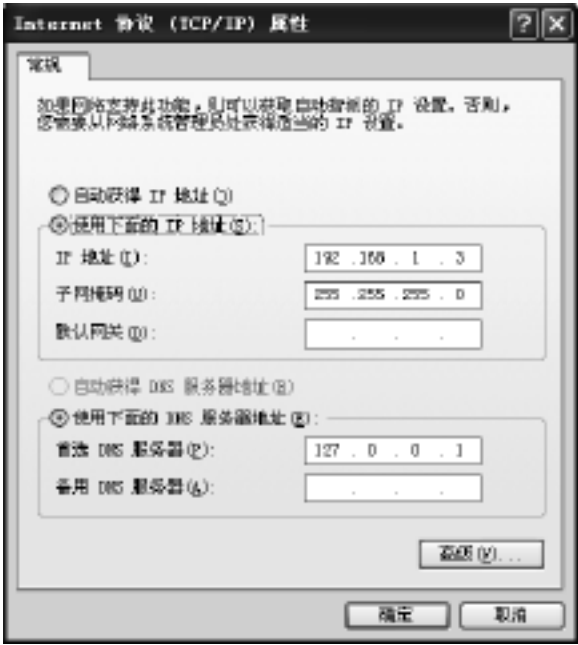


图 2-2-7 IP 地址设置界面(1)



图 2-2-8 IP 地址设置界面(2)

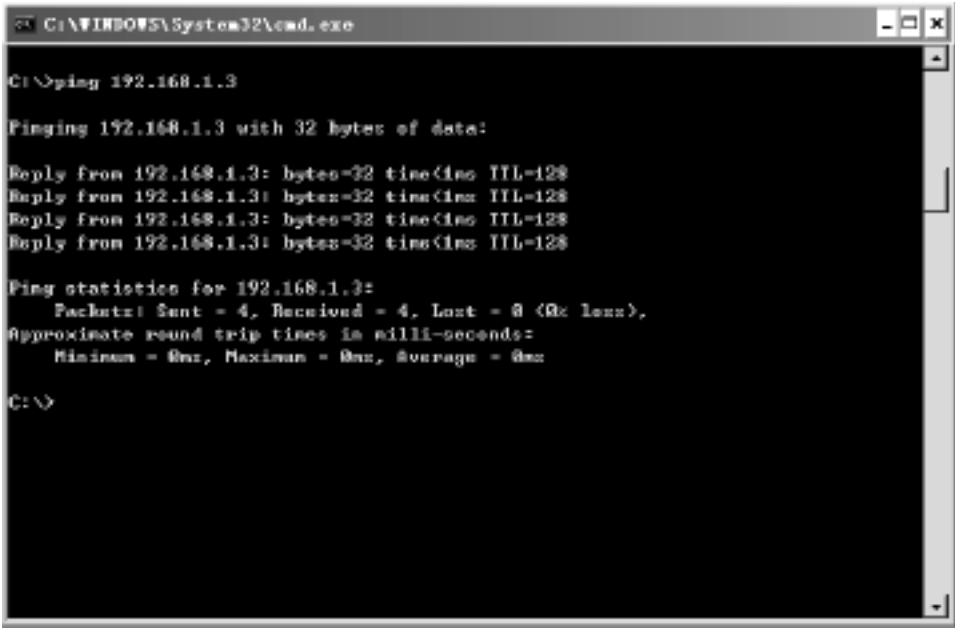


图 2-2-9 连通性测试显示界面(2)

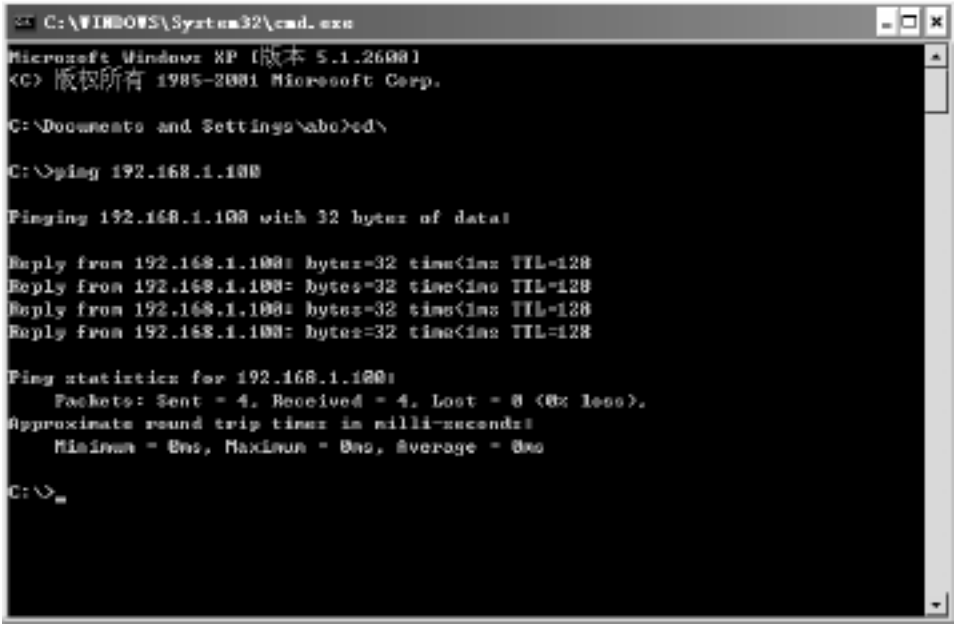


图 2-2-10 连通性测试显示界面(3)

图 2-2-11 表明这样做不行。同理,我们必须像 VLAN2 通信时那样,在两个交换机上各设置一个 VLAN3 端口,然后将它们连接起来,这样一来,就会造成交换机端口的浪费(浪费的端口数取决于 VLAN 的数量),所以,为了解决这个问题,可以采用 VLAN 中继(TRUNK)的方式实现不同交换机上的相同 VLAN 之间的通信。这样就可以做到一条中继多条虚拟(逻辑)链路捆绑在一条物理链路上。

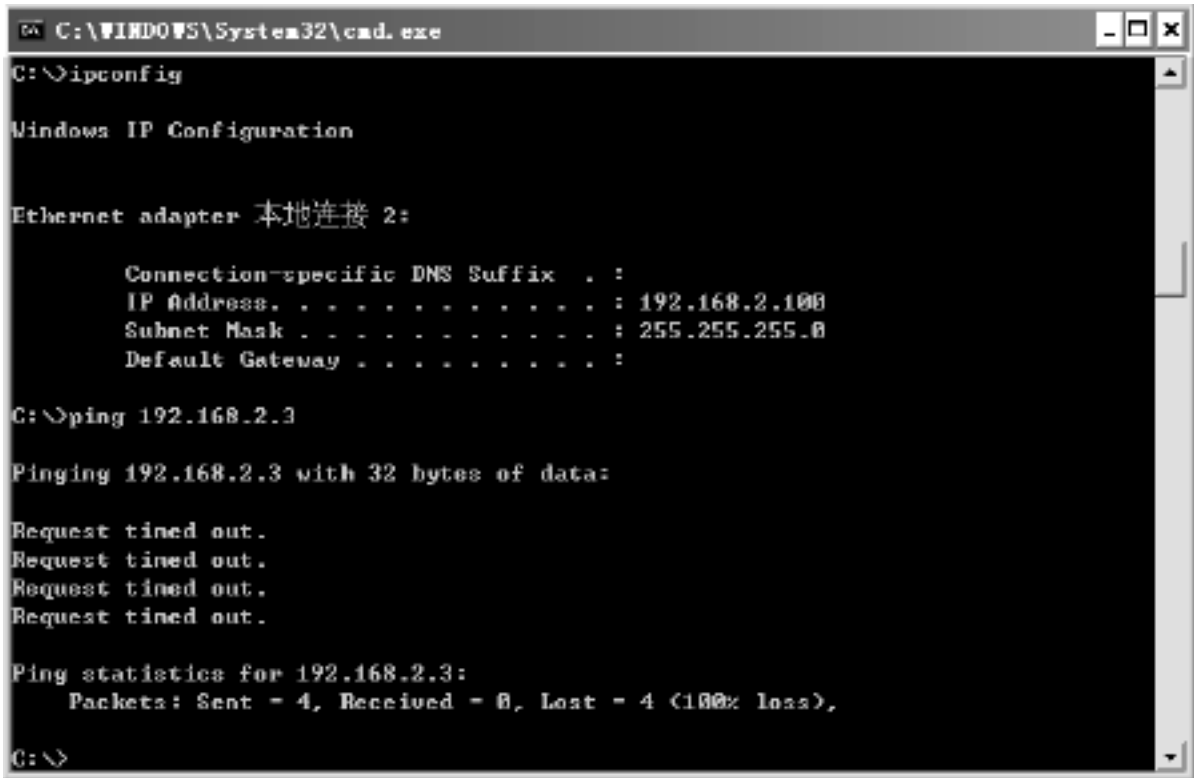


图 2-2-11 连通性测试显示界面(4)

(5) 用“中继”来实现不同交换机上同一个 VLAN 之间的通信

将 A 交换机的某个没有分配 VLAN 的端口(如第 24 个端口)设置为 trunk 模式,选择封装协议为 ISL:

```

Switch(config) # interface fa0/ 24
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport trunk encapsulation isl
  
```

将 B 交换机的某个没有分配 VLAN 的端口(如第 48 个端口)设置为 trunk 模式,选择封装协议为 ISL:

```

Switch(config) # interface fa0/ 48
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport trunk encapsulation isl
  
```

将两个被设为 trunk 的端口连起来,这时再测试一下通信是否成功。如图 2-2-12 所示。

结果表明通信成功,实验结果正确。

同样地,VLAN3 之间的通信也成功,两台微机的 IP 地址分别为:192 .168 .2 .3、192 .168 .2 .100。子网掩码均为:255 .255 .255 .0。

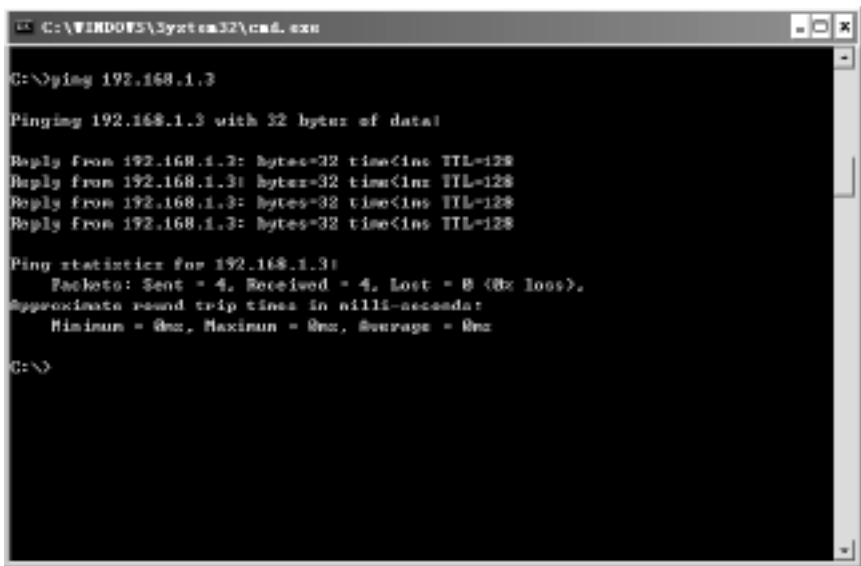


图 2-2-12 连通性测试显示界面(5)

(6) 实现不同 VLAN 之间的通信(如 VLAN2 和 VLAN3 之间的通信)

实现不同 VLAN 之间的通信必须通过具有路由功能的三层交换机或者路由器。

下面我们介绍用三层交换机实现不同 VLAN 之间通讯的方法：

将上面设置好的 trunk 去除,将它们分别接到三层交换机 C 的两个端口(分别属于 vlan2 和 vlan3)

```
Switch(config) # interface fa0/ 24
Switch(config-if) # no switchport mode trunk
Switch(config-if) # switchport acc vlan 2
Switch(config) # interface fa0/ 48
Switch(config-if) # no switchport mode trunk
Switch(config-if) # switchport acc vlan 3
```

配置交换机的第 24 个端口
将该端口的 trunk 去除

将三层交换机 C 的第 1 个端口设置为 VLAN2;第 2 个端口设置为 VLAN3,然后将交换机 A 的 VLAN2 与 C 的 VLAN2 连接起来,交换机 B 的 VLAN3 与 C 的 VLAN3 连接起来,C 的 VLAN 分配如图 2-2-13 所示。

为 VLAN2、VLAN3 配置 IP 地址

```
Switch(config) # interface vlan 2
Switch(config-if) # ip address 192 .168 .1 .1 255 .255 .255 .0
Switch(config) # interface vlan 3
Switch(config-if) # ip address 192 .168 .2 .1 255 .255 .255 .0
```

配置各个 VLAN 中主机的默认网关为相应 VLAN 的 IP 地址,并将 IP 地址分别设到两个 VLAN 的网段内,这样交换机中的三层交换模块就会自动完成路由功能。

两台微机的 IP 配置如图 2-2-14、图 2-2-15 所示。

测试 VLAN2 与 VLAN3 之间的通信,如图 2-2-16 所示。

这样就实现了跨 VLAN 的通信。VLAN2 和 VLAN3 是不同的网段,是单独的两个广播域,VLAN2 内部的广播通信不会进入到 VLAN3 中,VLAN3 内部的广播通信也不会进入 VLAN2 中,这样就提高了网段内部网络流量的性能。

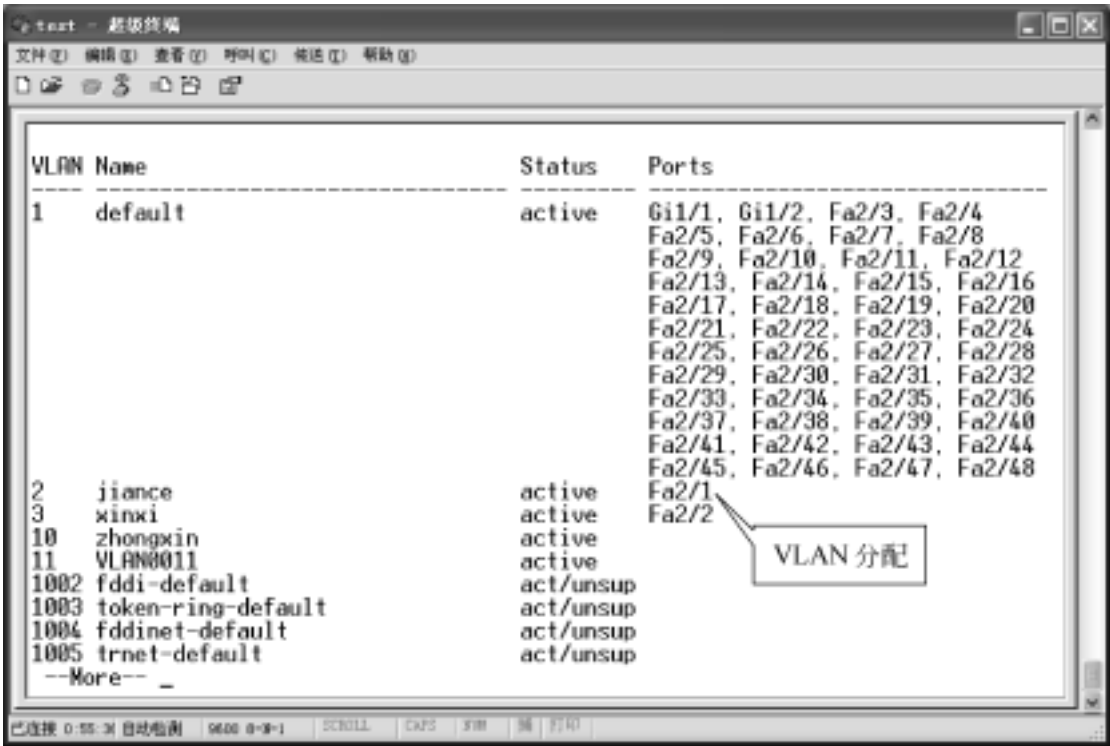


图 2-2-13 交换机 C 的 VLAN 分配信息界面

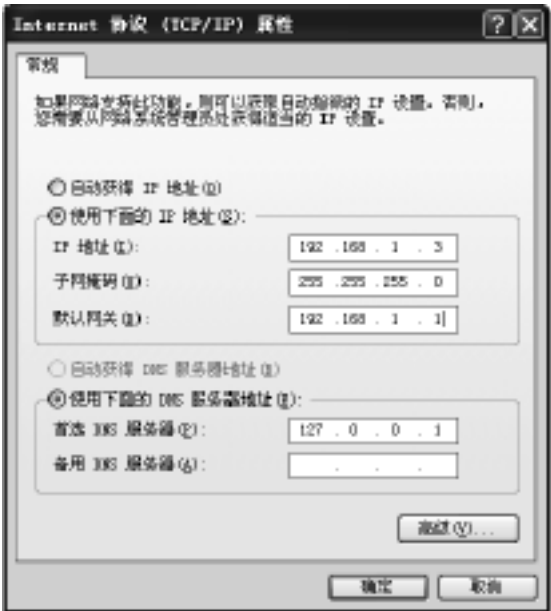


图 2-2-14 VLAN2 中微机的 IP 地址设置界面

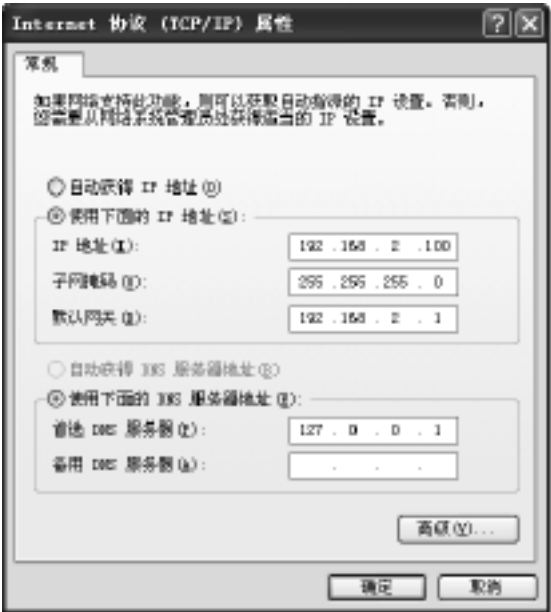


图 2-2-15 VLAN3 中微机的 IP 地址设置界面

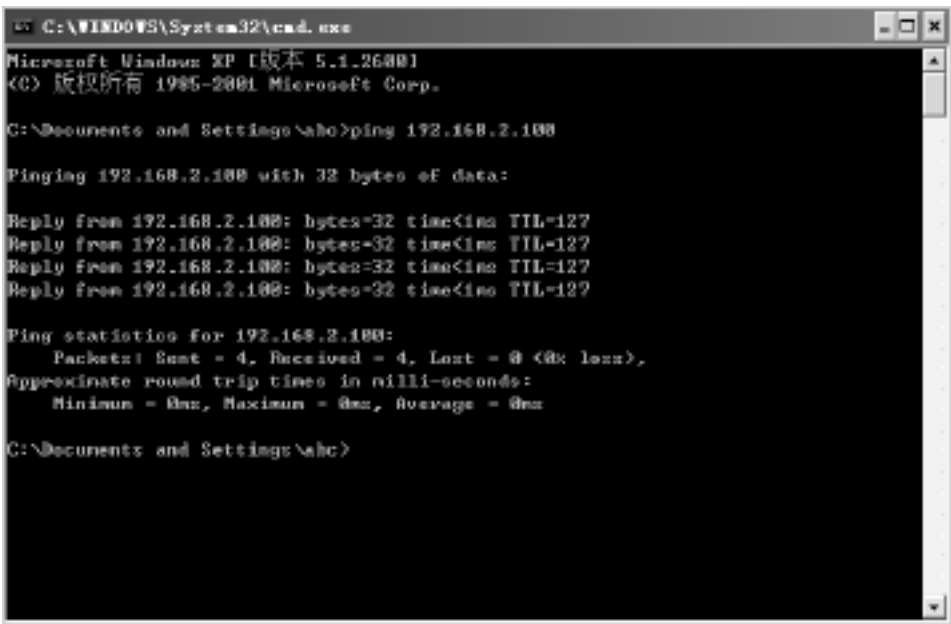


图 2-2-16 连通性测试显示界面(6)

实验三

FTP 服务器的配置与管理

目前,两种最常见的 Web 服务器是 Microsoft 的 Internet Information Server (简称 IIS)和 Apache Web Server。前者只能运行在 Windows 平台上,而后者则通常可以运行在 UNIX 和 Linux 平台上。本章将介绍在 Windows 2000 Professional 操作系统上 IIS 的配置和管理方法。

Internet Information Server 集成了 IIS 版本 5 .0。在 Windows 2000 Professional 中,可以使用一台计算机容留一个 Web 和 FTP 站点。操作系统在默认安装时并没有 IIS 管理,做实验之前,需要安装该组件。可以从“ 控制面板 ” “ 添加/ 删除程序 ” “ 添加/ 删除 Windows 组件 ” “ 选择 IIS 组件 ”进行安装,除了 SMTP service 选项(实验中用 Imail 代替),其他全部选上,然后进行安装,安装结束后,可以在控制面板的管理工具中找到 Internet服务管理器,这样实验环境就建好了。

3 .1 实验目的

通过该实验使学生掌握 FTP 服务器的配置方法、如何在客户端下载服务器端的文件,以及如何将客户端的文件上传到服务器上。

3 .2 启动管理控制台

单击“ 开始 ” “ 设置 ” “ 控制面板 ” “ 管理工具 ” “ Internet 服务管理器 ”,便可启动 Microsoft 的管理控制台(如图 2-3-1 所示)。

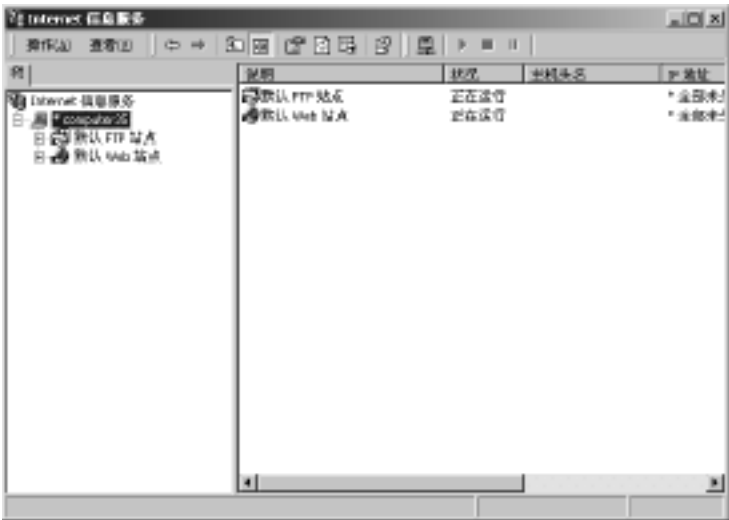


图 2-3-1 Internet 服务管理器窗口

3.3 配置 FTP 站点属性

右击默认“ FTP 站点 ” “ 属性 ”,弹出如图 2-3-2 所示选项卡。

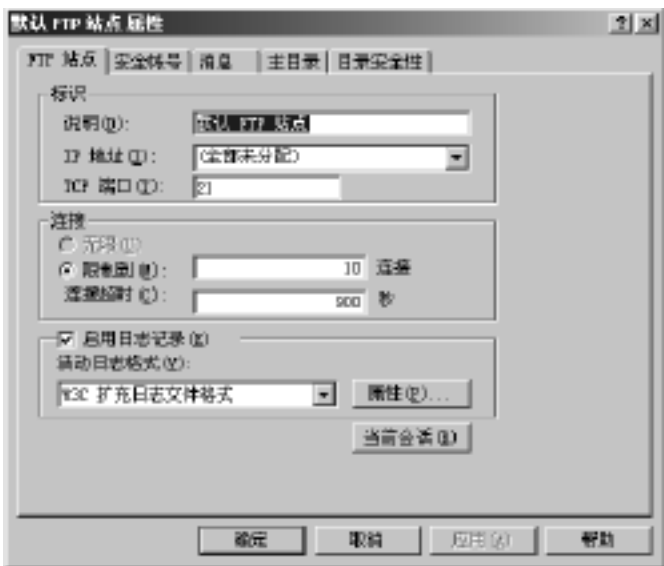


图 2-3-2 FTP 站点属性—“ FTP 站点 ”选项卡

在“ FTP 站点 ”选项卡中：

IP 地址 选择你的 FTP 服务器的地址。

TCP 端口 确定运行服务所在的端口,默认值是端口 21。可以将此端口更改为任意的惟一 TCP 端口号。但是,客户在请求端口号之前,必须知道这个端口号,否则,请求将无法连接到服务器。

单击“ 消息 ”标签:弹出如图 2-3-3 所示的选项卡。



图 2-3-3 FTP 站点属性—“ 消息 ”选项卡

在“ 消息 ”标签中,可以填写一些信息,当用户访问您的站点时会将这些消息显示给用户。同样地,在“ 退出 ”标签中,也可以填写一些信息,客户从 FTP 服务器注销时,将显示此文本。当 FTP 服务的连接数已达到所允许的最大值时,如果客户仍试图进行连接,则显示“ 最大连接数 ”项的文本,以上三项默认情况下均为空。

单击“ 主目录 ”标签,弹出如图 2-3-4 所示选项卡：



图 2-3-4 FTP 站点属性—“主目录”选项卡

主目录是 FTP 站点中用于已发布文件的中心位置。在安装 FTP 服务时,创建了一个名为 \ftproot 的默认主目录。主目录的位置可以更改,同时在此输入对该目录的读写权限,以决定客户端在服务器上进行上传或下载文件的权限。

至此,就完成了 FTP 服务器的配置与管理工作,然后在客户端通过 FTP 连接进行文件传输的操作了。

实验四

Web 服务器的配置

4 .1 实验目的

通过该实验使学生掌握 Web 服务器的配置方法,以及如何发布自己的网页。

4 .2 实验准备

在做实验之前,先准备一个简单的个人主页,要求有个人信息。

4 .3 Web 服务器的配置

1 . 配置 Web 站点属性

在图 2-3-1 中,右击默认“ Web 站点 ” “ 属性 ”,弹出如图 2-4-1 所示对话框,在“ Web 站点 ”标签中进行如下操作。



图 2-4-1 默认 Web 站点属性—Web 站点

IP 地址: 填上 Web 服务器的地址。

TCP 端口: 确定运行服务所在的端口,默认值是端口 80。可以将此端口更改为任

意的惟一 TCP 端口号。但是,客户在请求端口号之前,必须知道这个端口号,否则,请求将无法连接到服务器,其他采用默认值。

2 .“ 主目录 ”属性

单击“ 主目录 ”标签,弹出如图 2-4-2 所示对话框:

在“ 主目录 ”标签中:可以更改系统建立时创建的名为 \wwwroot 的默认主目录,该主目录中存放你的个人主页,其他采用默认值。

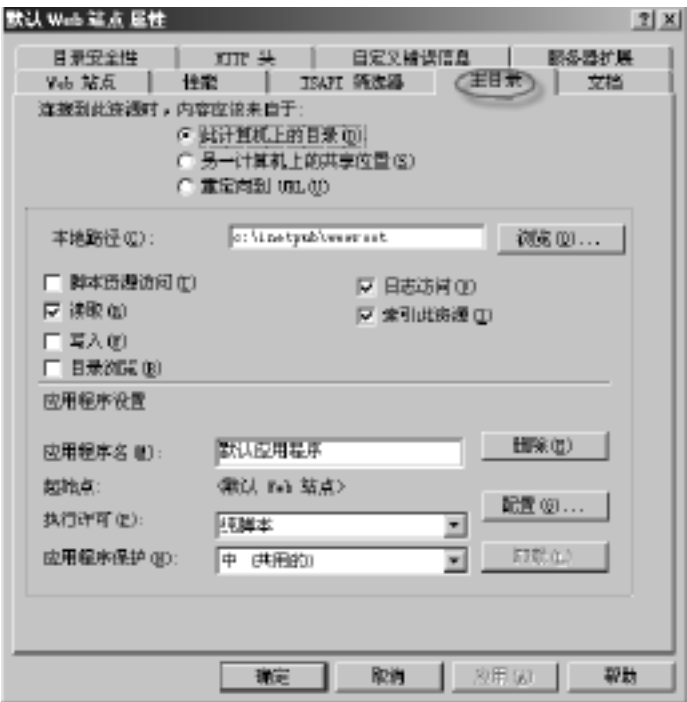


图 2-4-2 默认 Web 站点属性—“ 主目录 ”选项卡

3 .“ 文档 ”属性

单击“ 文档 ”标签,弹出如图 2-4-3 所示对话框。



图 2-4-3 默认 Web 站点属性—“ 文档 ”选项卡

选择启用默认文档,默认文档可以是目录的主页或包含站点文档目录列表的索引页。要添加一个新的默认文档,单击“ 添加 ”。可以使用该特性指定多个默认文档。按出现在

列表中的名称顺序提供默认文档。服务器将返回所找到的第一个文档。要更改搜索顺序,请选择一个文档并单击箭头按钮。要从列表中删除默认文档,选中文档后,单击“删除”即可。

完成上述配置之后,就可以在另外一台客户机的浏览器中输入 IP 地址,来查看个人主页。

实验五

DNS 服务器的配置与管理

DNS 是将因特网名字(如 info.tsinghua.edu.cn)解析为 IP 地址。做该实验时需要与 Web 服务器实验结合起来,前面的 Web 服务器实验,是在 Windows 2000 Professional 环境下做的,而只有在 Windows 2000 Server 中才有 DNS 服务。所以,需要在 Windows 2000 Server 中再次配置 Web 服务,方法与前面的 Web 服务器实验类似。同样,也需要事先建立好自己的个人主页,在此基础上,我们来学习配置 DNS,使客户机能够访问服务器上的个人主页。

5.1 实验目的

通过该实验使学生掌握 DNS 服务器的配置方法,从而加深对域名解析的理解。

5.2 启动 DNS 管理控制台

(1) 在 Windows 2000 Server 桌面上,选择“开始”“程序”“管理工具”“DNS”出现如图 2-5-1 所示窗口。

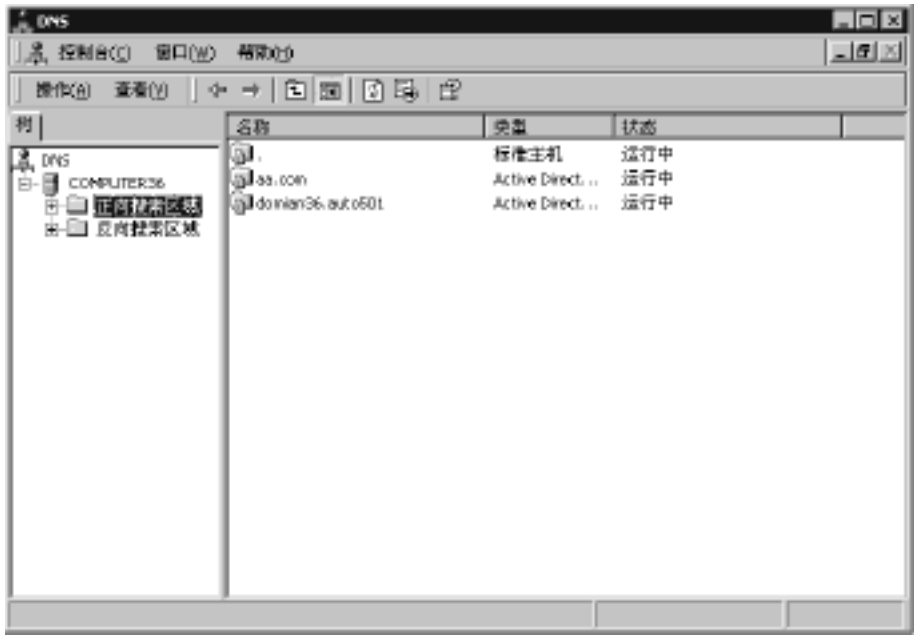


图 2-5-1 DNS 管理控制台界面

(2) 在主机名处单击鼠标右键,选择“属性”,就可以对主要的属性进行配置。如图

2-5-2 ~ 图 2-5-4 所示,分别对“ 接口 ”、“ 转发器 ”、“ 监视 ”等属性进行设置。

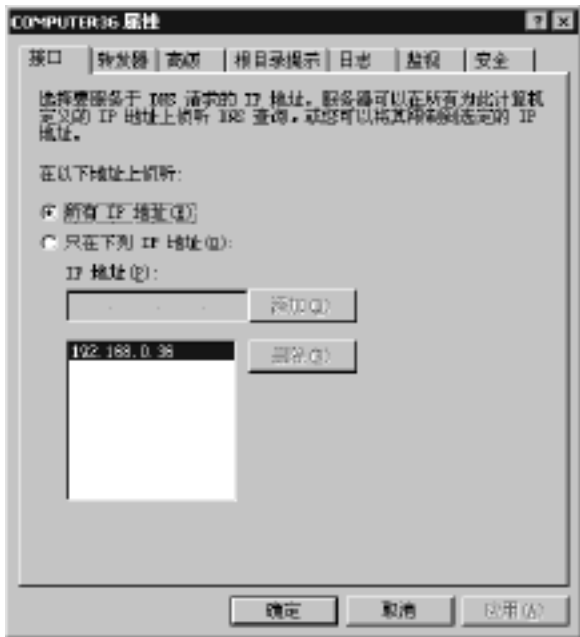


图 2-5-2 DNS 属性—“ 接口 ”选项卡

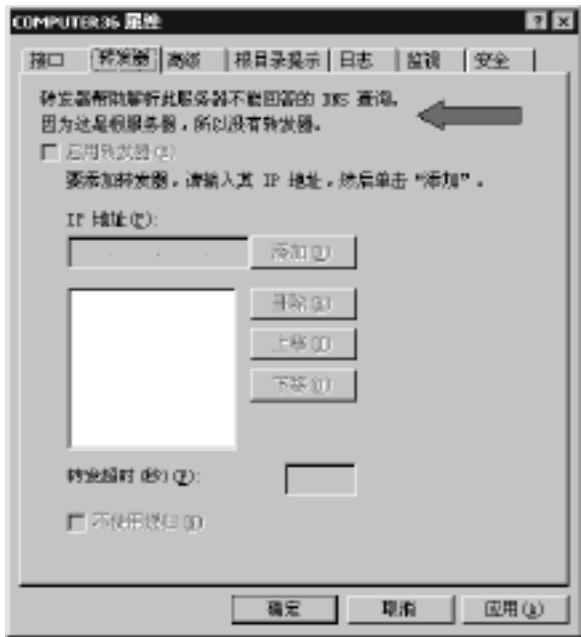


图 2-5-3 DNS 属性—“ 转发器 ”选项卡

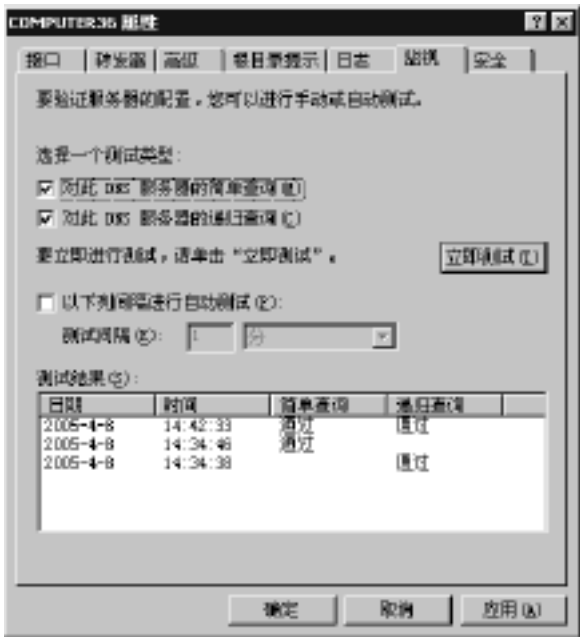


图 2-5-4 DNS 属性—“ 监视 ”选项卡

在图 2-5-4 中,单击“ 立即测试 ”按钮,可以进行手动测试。

5.3 DNS 配置与管理

1. 新建区域

如图 2-5-1 所示,在正向搜索区域处右击出现“ 新建区域 ”,利用向导完成新区域的创建。如图 2-5-5、2-5-6 所示。

按照提示,单击“ 下一步 ”。

在此,选择“ 标准主要区域(S) ”,然后单击“ 下一步 ”,见图 2-5-7。

选择“ 正向搜索区域 ”,即建立一个名称到地址的数据库,域名解析时将域名转换为 IP 地址。



图 2-5-5 启动“新建区域向导”界面

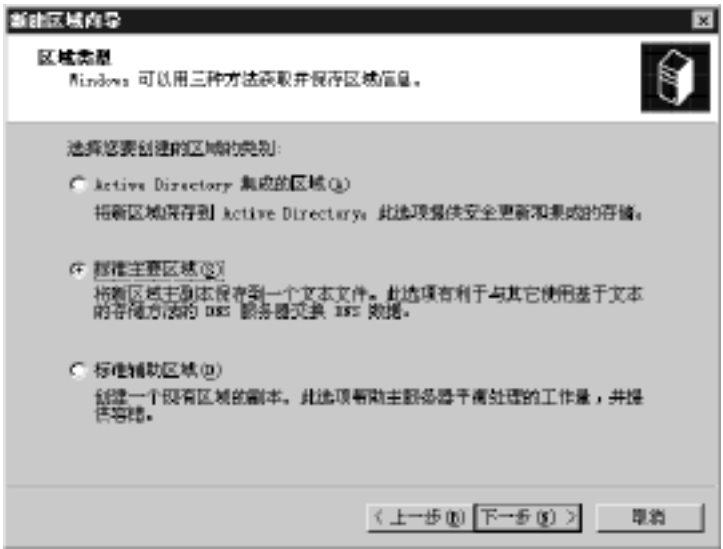


图 2-5-6 选择“区域类别”界面

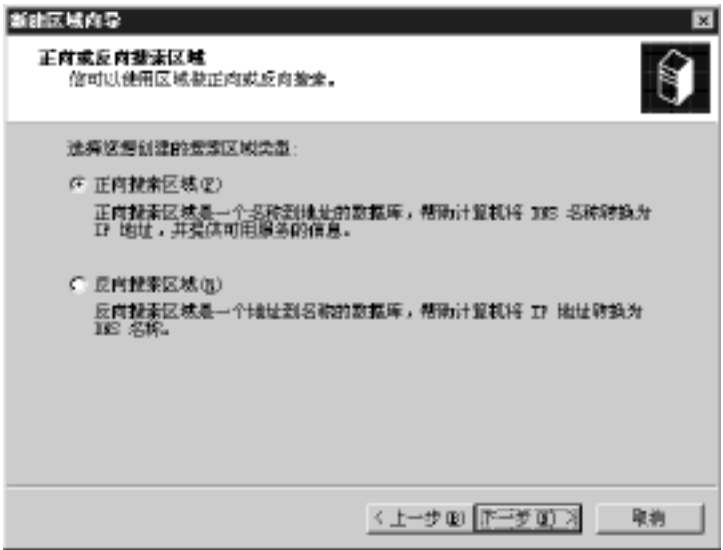


图 2-5-7 选择区域类型界面

这里,假设区域名为: test .cn,见图 2-5-8。
在图 2-5-9 中,选择创建新文件,并命名为: test .cn .dns。
确认新建区域的设置,并单击“完成”,见图 2-5-10。



图 2-5-8 输入区域名称界面

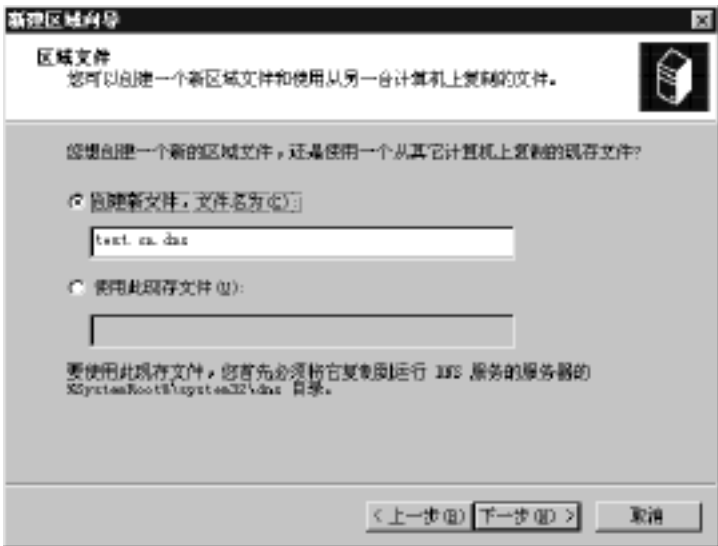


图 2-5-9 创建新区域文件界面



图 2-5-10 新建区域的设置界面

2 . 查看新建区域的属性

如图 2-5-11, 右击 test .cn, 出现如图 2-5-12 ~ 图 2-5-16 所示对话框, 可以查看新区域的各个属性设置。

在图 2-5-14 中, 可以添加其他的服务器名, 或对现有服务器进行编辑、删除等操作。



图 2-5-11 正向搜索区域展开



图 2-5-12 新建区域文件的属性—“常规”选项卡

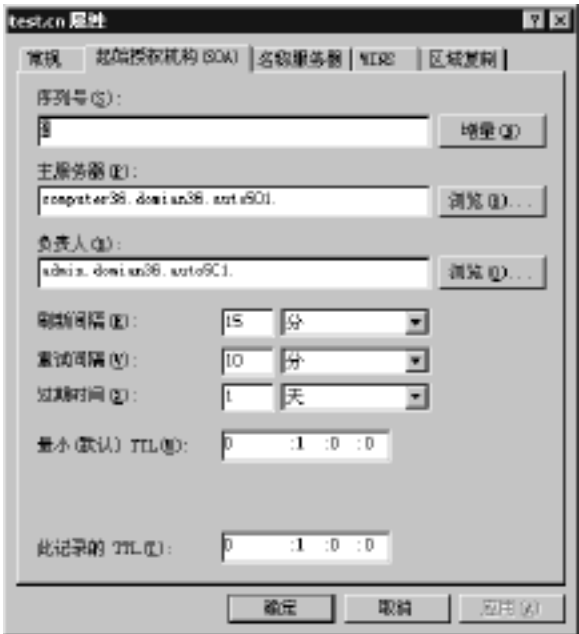


图 2-5-13 新建区域文件的属性—“起始授权机构”选项卡



图 2-5-14 新建区域文件的属性—名称服务器

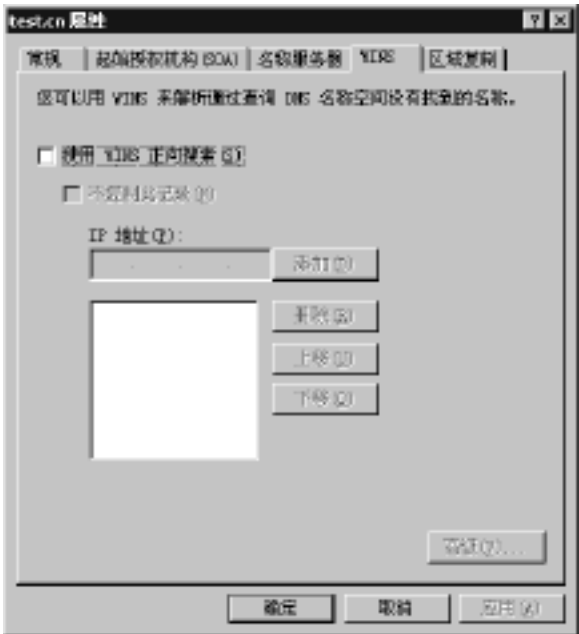


图 2-5-15 新建区域文件的属性—“WINS”选项卡

如图 2-5-15, 可以用 WINS 来解析通过查询 DNS 名称空间没有找到的名称, 此处, 我们没有选择此功能, 即: 不使用 WINS 正向搜索。

3 . 在新建的区域上新建主机

在新建的正向搜索区域 test .cn 处, 单击鼠标右键选择“新建主机”, 如图 2-5-17 所示。

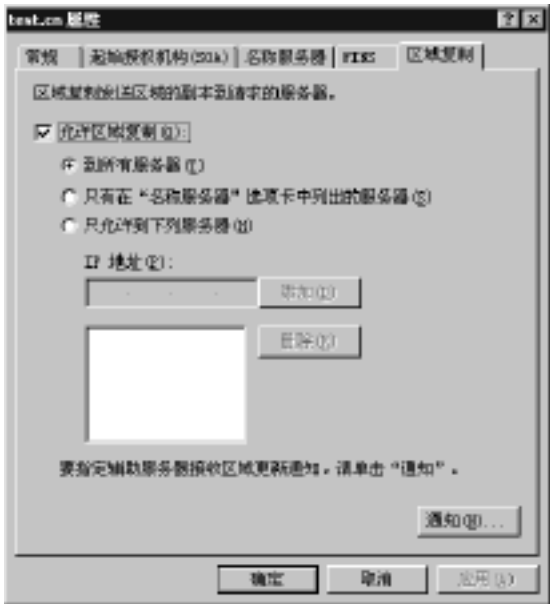


图 2-5-16 新建区域文件的属性—“区域复制”选项卡



图 2-5-17 “新建主机”界面

在“名称”栏内, 添加主机名, 如 www, “IP 地址”栏内填写 DNS 服务器的地址。

对比图 2-5-18 和图 2-5-19, 可以看出, 主机记录 www .test .cn 的命名是符合 DNS 的命名规则的。



图 2-5-18 主机记录

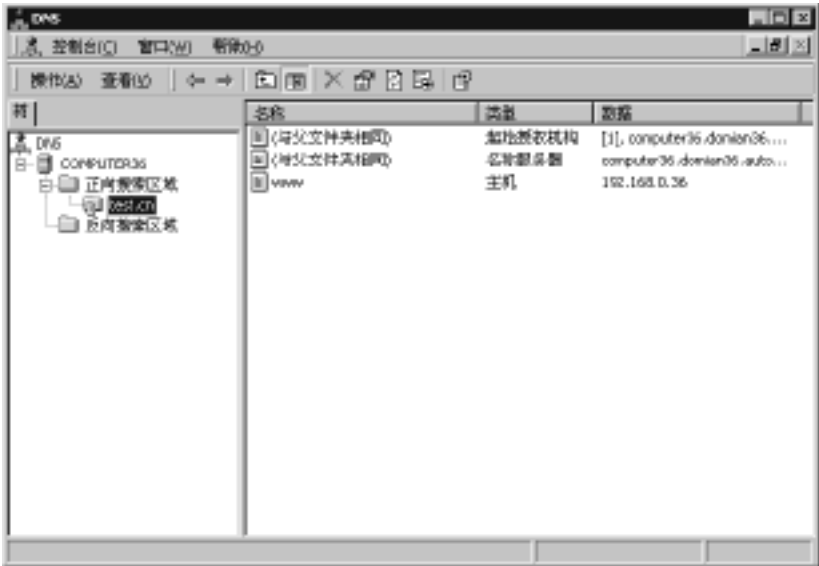


图 2-5-19 新建区域下的新主机

通过上述的配置过程, 就可以用 IE 浏览此前设定好的主页了。

实验六

电子邮件服务器的配置与管理

6.1 实验目的

通过该实验使学生了解并掌握一种电子邮件服务器的配置方法,并了解如何在客户端用 Outlook Express 进行邮件的发送和接收。

6.2 Imail 的配置与管理

1. Imail 的基本情况

运行环境: Windows NT/ 2K

软件功能: E-mail 服务器端软件

Imail 是 Ipswitch 公司开发的一个高性能的,基于标准的 SMTP/ POP3/ IMAP4/ LDAP 邮件服务器。通过一个简单直观的图形用户界面管理,操作简单,功能异常强大。主要特色包括: 多域名支持,远程管理,Web 邮件,可创建邮递清单(mailing lists),反垃圾邮件支持,等等。用它可以很方便地创建一个邮件服务器。下面是邮件服务器安装与配置过程。

2. Imail 的安装

首先双击安装文件,即可进行安装,如图 2-6-1 所示。



图 2-6-1 安装向导界面

启动安装向导,单击 next 按钮,出现图 2-6-2 输入主机名界面。

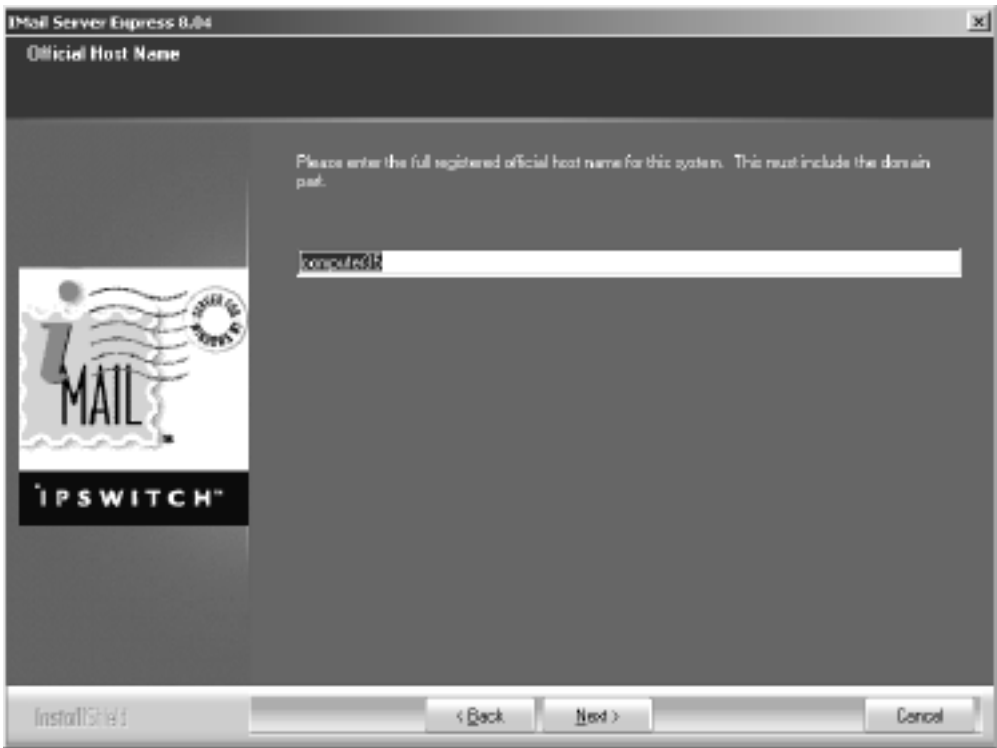


图 2-6-2 输入主机名界面

输入主机名,单击 next 按钮,出现的界面如图 2-6-3 所示。



图 2-6-3 选择安装路径界面

选择安装路径后,单击 next 按钮,出现的界面如图 2-6-4 所示。

选择程序文件夹后,单击 next 按钮,出现的界面如图 2-6-5 所示。

提示是否添加用户,此处选择“否”,出现如图 2-6-6 所示的界面,在安装完成后再添加用户。

单击完成 Finish 按钮,安装结束。

3 . Imail 的配置

安装结束后,就要开始进行 Imail 服务器的配置工作了。

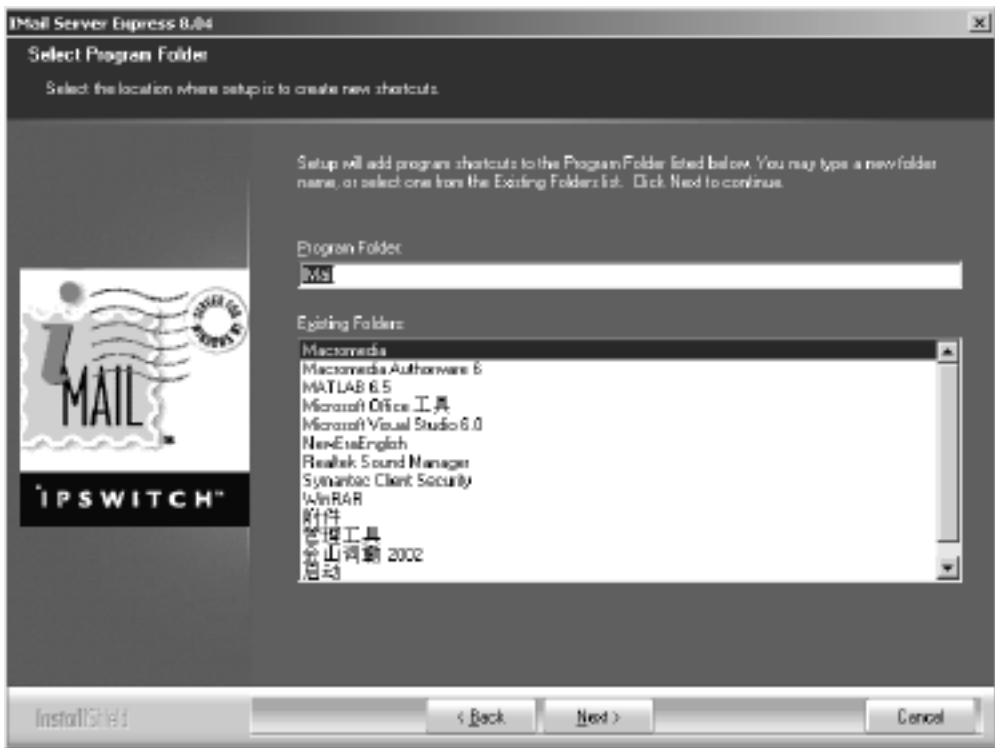


图 2-6-4 选择程序文件夹界面

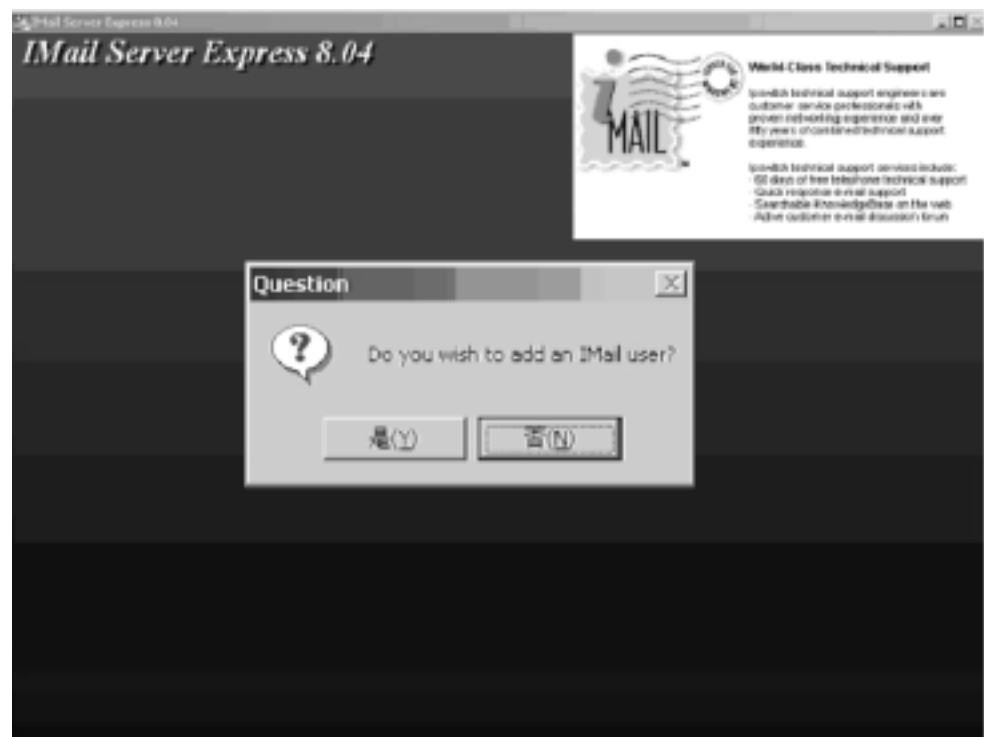


图 2-6-5 添加用户提示界面

首先,从“开始”“程序”“Imail 服务器” Imail Administrator,出现图 2-6-7 所示窗口。

下面,开始添加用户。在图 2-6-7 所示的窗口中,单击 Add User,弹出如图 2-6-8 所示对话框。

提示输入新用户的标识 (ID),然后单击“下一步”按钮,出现如图 2-6-9 所示对话框:

按照提示,输入所建用户的密码,并单击“下一步”按钮,出现如图 2-6-10 所示界面。
单击完成,这样我们就建好了一个用户。

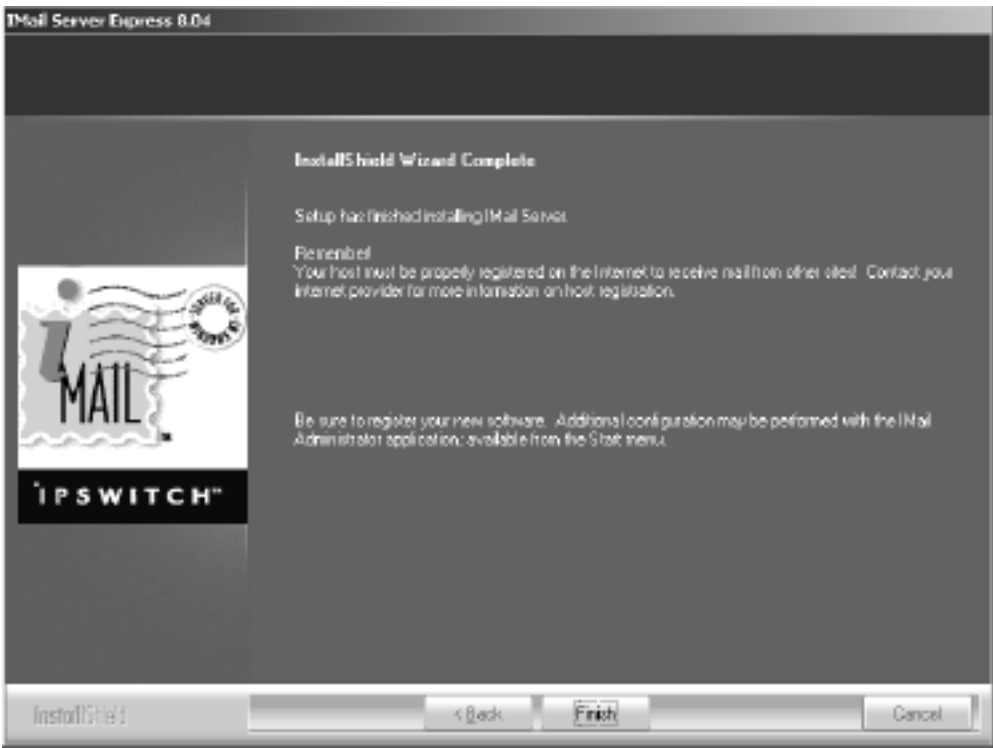


图 2-6-6 安装向导完成界面

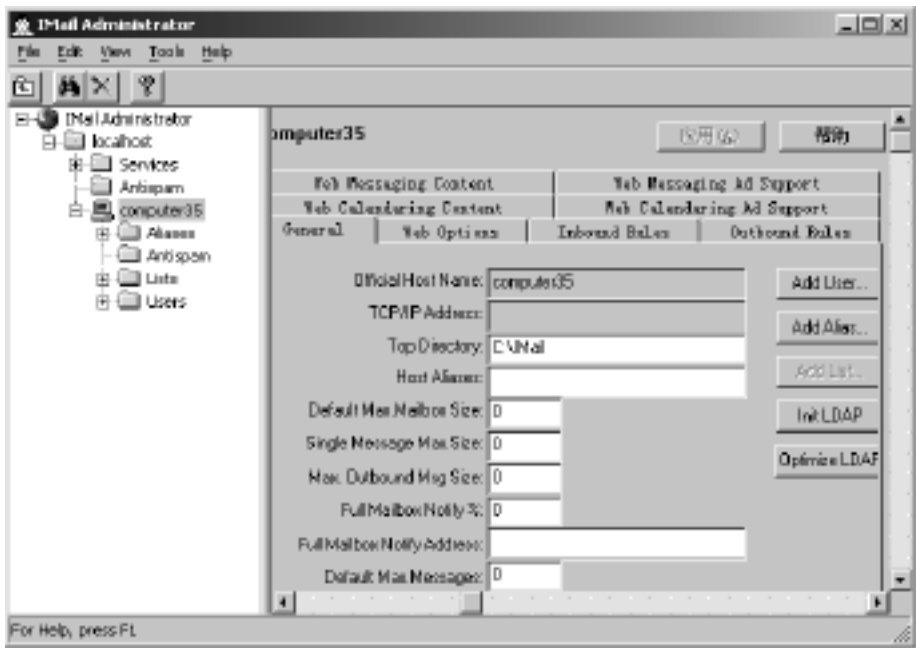


图 2-6-7 服务器配置界面



图 2-6-8 输入用户标识对话框

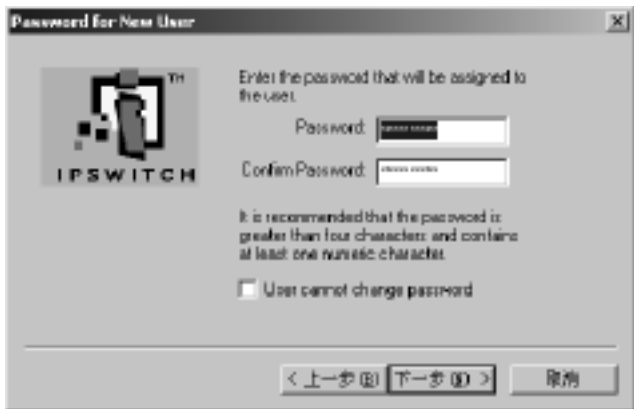


图 2-6-9 输入用户密码对话框



图 2-6-10 新建用户完成界面

6.3 Imail 的使用

照前面所说的那样,再建其他的用户。例如,我们这里建好了 2 个用户: lming 和 dx x,从图 2-6-11 可以看出, dx x 的全名: dingxiaoxiao, 邮箱地址: dx x@computer35,单击其他选项还可以看到更多信息。

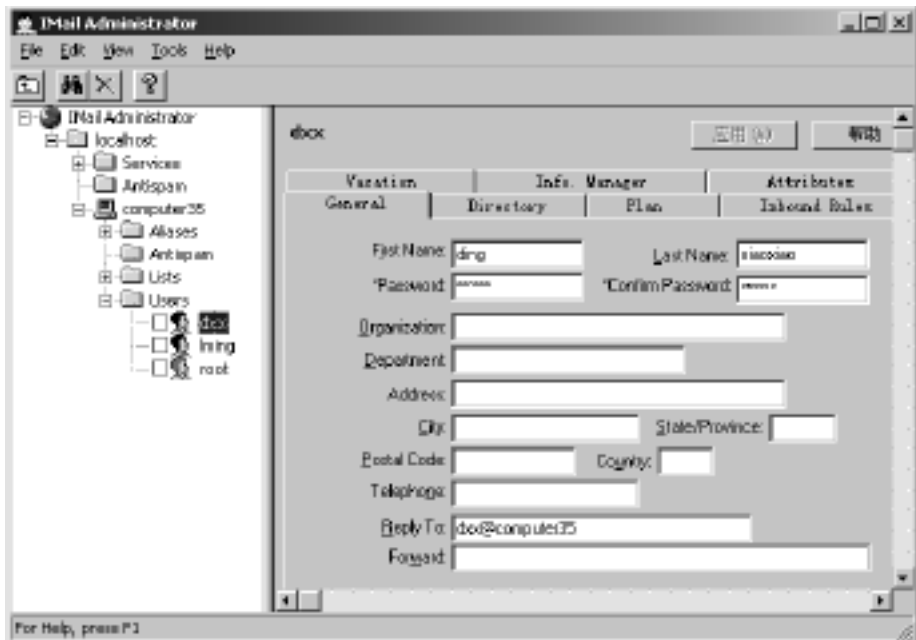


图 2-6-11 显示用户信息窗口

下面,我们来看看用户之间怎样发邮件吧:从“ 开始 ” “ 程序 ” Imail Client,弹出如图 2-6-12 所示对话框。

此时,用户是 root,这是随着服务器的建立而建立的默认用户,它的全称是: System Administrator ,单击 OK 按钮,出现如图 2-6-13 所示窗口。



图 2-6-12 显示登录用户对话框



图 2-6-13 登录用户的信箱窗口

菜单栏下方有一排按钮,可以用于发送、回复、转寄文件等。要发送邮件,则单击 Send,出现如图 2-6-14 所示窗口。

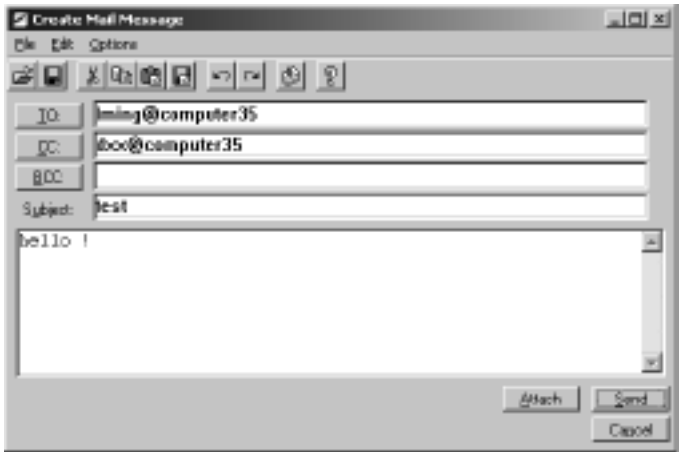


图 2-6-14 写邮件窗口

在窗口中填入对方的邮箱地址,主题,内容等,还可以单击 Attach 选择附件,然后单击 Send,完成邮件的发送。发送完成后出现如图 2-6-15 所示对话框。



图 2-6-15 发送方信息对话框

在图 2-6-15 中完成确认回复地址等信息,然后选择 OK 按钮,出现图 2-6-16。



图 2-6-16 发送方信箱窗口

现在,来验证一下用户是否收到邮件。

单击 File POPLogn(Ctrl + L), 弹出如图 2-6-17 所示的对话框后,选择 User ID: lming 或 dx x。

在图 2-6-17 中,单击 OK 按钮后,出现如图 2-6-18 所示窗口。其中,显示出发件人是: System Administ ,发件时间为: 2005 年 6 月 13 日 15:01 ,主题是: test,说明发送成功。



图 2-6-17 接收方登录对话框



图 2-6-18 接收方信箱窗口

接着在此处可以发信、回复等,双击邮件名称可以察看信件内容,如图 2-6-19 所示。

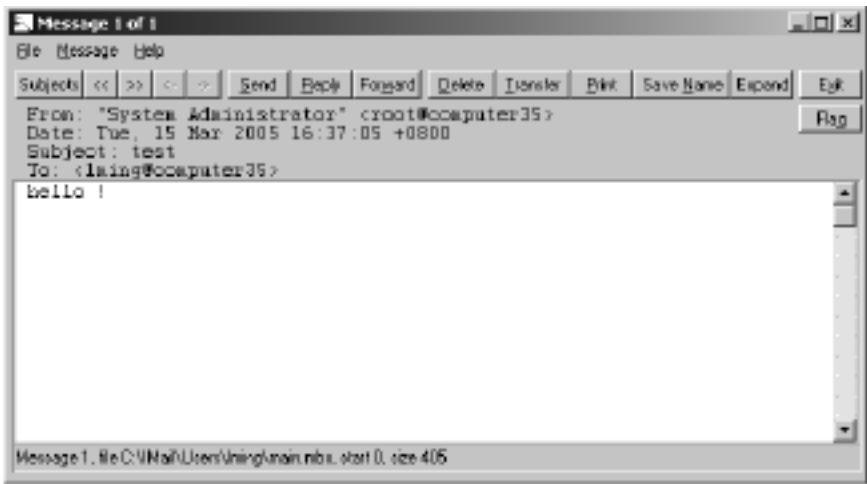


图 2-6-19 信件内容显示界面

6.4 客户端使用 Outlook Express 发送 / 接收邮件

本实验验证一下 lming 这个客户接收和发送邮件的情况。具体步骤如下:

1 . 启动 Outlook Express

单击“ 开始 ” “ 程序 ” Outlook Express, 出现图 2-6-20 所示界面。

2 . 启动 Internet 连接向导

若此前没有配置过 Outlook Express,则启动 Outlook Express 时自动开启该连接向导,进行配置,如图 2-6-21 ~ 图 2-6-25 所示。

在“ 显示名 ”处,输入 lming (因为该客户端为 lming)。



图 2-6-20 启动 Outlook Express 界面



图 2-6-21 输入显示名界面



图 2-6-22 输入电子邮件地址界面

在图 2-6-23 中分别输入接收、发送邮件的服务器名称后,单击“ 下一步 ”按钮,出现如图 2-6-24 所示的界面。

在图 2-6-24 中输入 Imail 服务器创建的用户名及其密码作为账户名、密码,然后单击“ 下一步 ”按钮,出现如图 2-6-25 所示的界面。



图 2-6-23 输入接收/发送邮件服务器界面

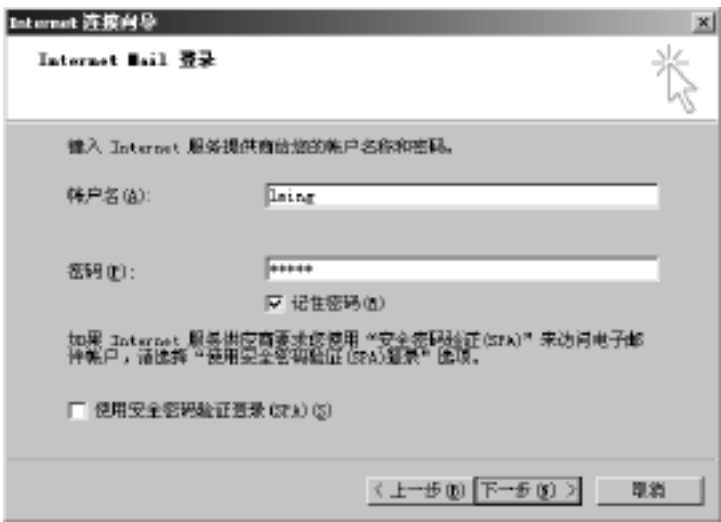


图 2-6-24 输入账号及密码界面



图 2-6-25 “Internet 连接向导”界面

3 . 邮件属性设置

在 OutlookExpress 中,单击“ 工具 ”“ 账户 ”,如图 2-6-26 所示。
单击“ 属性 ”,如图 2-6-27、图 2-6-28 所示。
在图 2-6-26 中,单击“ 添加 ”“ 邮件 ”即可添加新的账户,过程同上。
在图 2-6-29 中,computer35 为默认值,即接收、发送邮件均基于该默认账户,所以此

处的默认账户为 lming。



图 2-6-26 默认的邮件账户



图 2-6-27 新建账户的属性——“常规”选项卡



图 2-6-28 新建账户的属性——“服务器”选项卡



图 2-6-29 邮件账户显示界面

4 . 发送/ 接收邮件

在图 2-6-30 中, 单击“ 发送/ 接收 ”, 即可查看收件箱中是否有新邮件。

在图 2-6-31 中, 可以看到 System Administrator 发来的邮件, 单击该邮件, 可以查看其内容, 双击该邮件名, 出现如图 2-6-32 所示窗口。

在图 2-6-32 中, 可以回复邮件, 写好信件内容后, 单击“ 发送 ”即可。

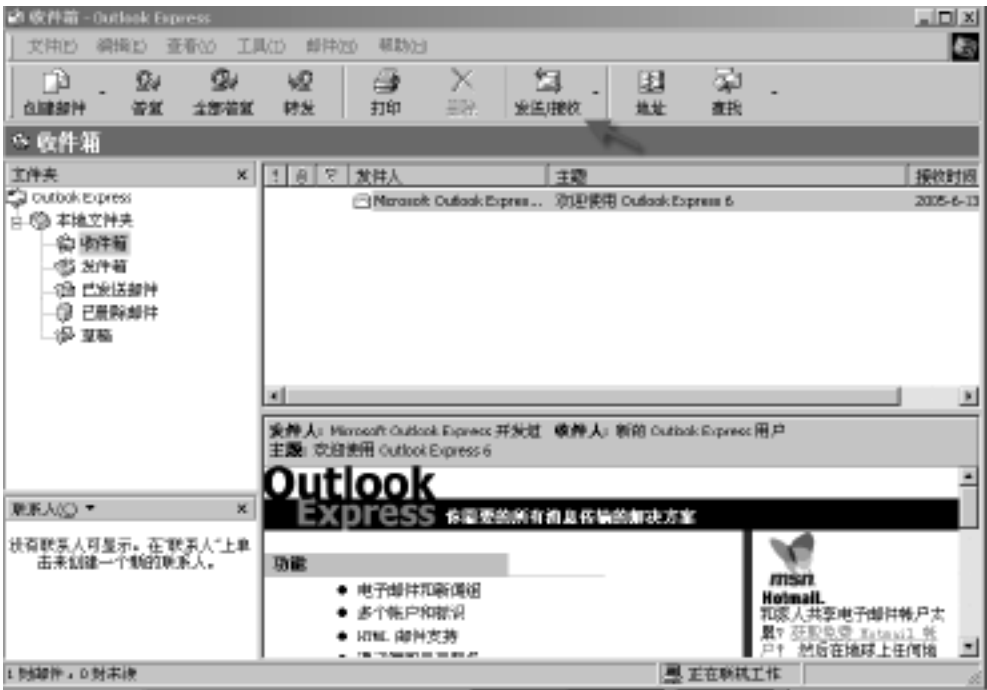


图 2-6-30 查看收件箱界面



图 2-6-31 收件箱中的信件界面



图 2-6-32 信件内容显示窗口

5 . 验证“ 发送 ”

在服务器端收到如图 2-6-33 所示邮件,证明在 Outlook Express 中,发送邮件成功。

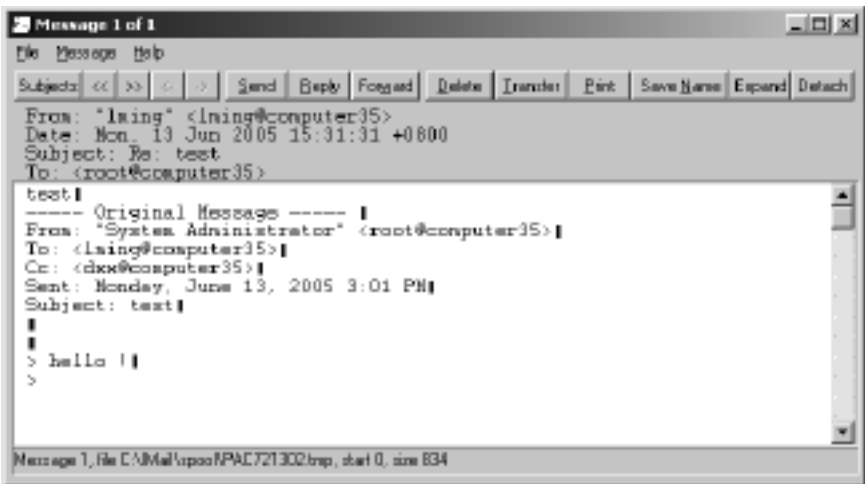


图 2-6-33 发信人收到回信显示窗口

实验七

DHCP 服务器的配置与管理

在一个使用 TCP/ IP 协议的网络中,每一台计算机都必须至少有一个 IP 地址,才能与其他计算机连接通信。路由器、服务器和其他关键结点通常需要一个固定的 IP 地址。但是,一般客户却并不需要一个特定的地址,而是一段地址范围中的一个。这个范围通常在一个 IP 子网内。为了便于统一规划和管理网络中的 IP 地址,DHCP(Dynamic Host Configure Protocol,动态主机配置协议)应运而生了。这种网络服务的真正目的是减少管理员在管理大型网络时的工作量,同时使得 IP 地址得到充分利用。

7.1 实验目的

通过该实验使学生掌握 DHCP 服务器的配置,了解如何在局域网中设置 DHCP 服务器使客户机获得 IP 地址。

7.2 DHCP 服务的安装

DHCP 指的是由服务器控制一段 IP 地址范围,客户机可以自动获得服务器分配的 IP 地址和子网掩码。首先,DHCP 服务器必须是一台安装有 Windows 2000 Server/ Advanced Server 系统的计算机;其次,该计算机需要安装 TCP/ IP 协议,并为其设置静态 IP 地址、子网掩码、默认网关等内容。默认情况下,DHCP 作为 Windows 2000 Server 的一个服务组件不会被系统自动安装,必须把它添加进来:

单击“开始”“设置”“控制面板”“添加/删除程序”“添加/删除 Windows 组件”,打开相应的对话框。

单击选中对话框的“组件”列表框中的“网络服务”一项,单击“详细信息”按钮,出现带有具体内容的对话框。

在对话框“网络服务的子组件”列表框中勾选“动态主机配置协议(DHCP)”,单击“确定”按钮,根据屏幕提示放入 Windows 2000 安装光盘,复制所需要的程序。

在“开始”“程序”“管理工具”下就会出现 DHCP 一项,说明 DHCP 服务安装成功。

7.3 DHCP 服务器的授权

出于对网络安全管理的考虑,并不是在 Windows 2000 Server 中安装了 DHCP 功能后就能直接使用,还必须进行授权操作,未经授权操作的服务器无法提供 DHCP 服务。对 DHCP 服务器授权操作的过程如下:

依次单击“开始”“程序”“管理工具”DHCP,打开 DHCP 控制台窗口,如图 2-7-1 所示。

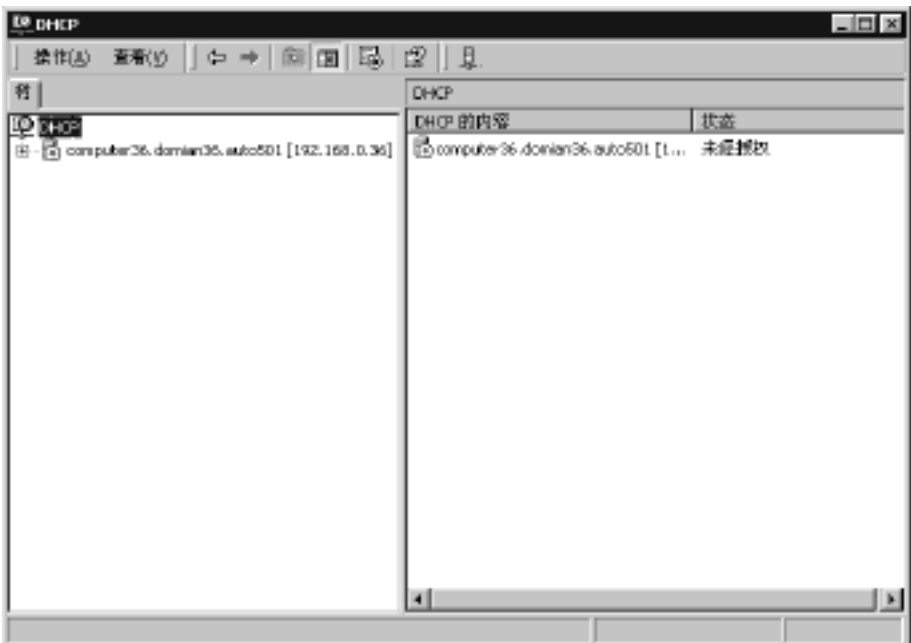


图 2-7-1 DHCP 控制台

在控制台窗口中,单击选中服务器名,出现图 2-7-2。

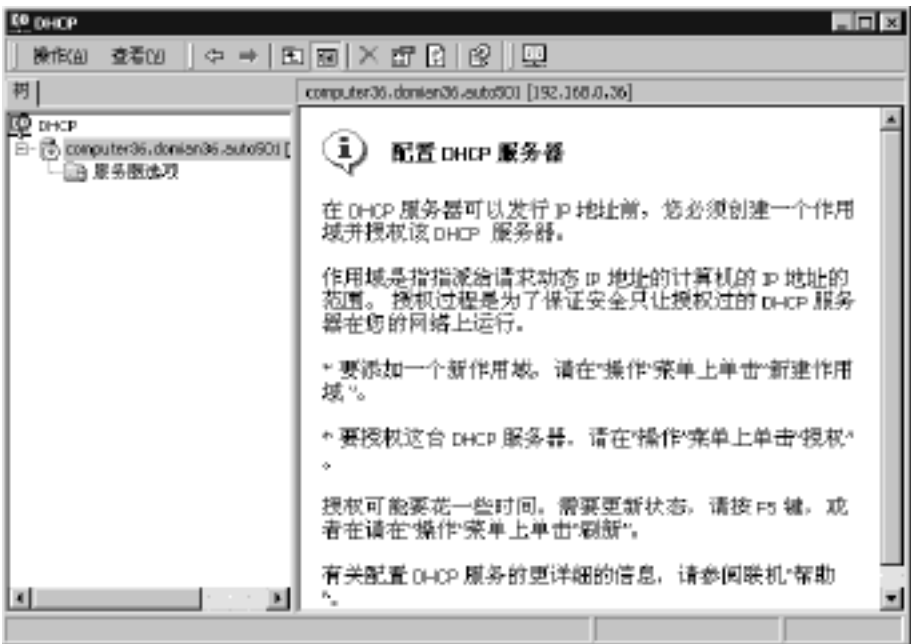


图 2-7-2 配置 DHCP 服务器提示

在图 2-7-2 中,单击选中服务器名,然后单击右键,在快捷菜单中选中“授权”,此时需要几分钟的等待时间。注意:如果系统长时间没有反应,可以按 F5 键或选择菜单工具中的“操作”下的“刷新”进行屏幕刷新,或先关闭 DHCP 控制台,右击服务器名。如果快

捷菜单中的“授权”已经变为“撤销授权”,则表示对 DHCP 服务器授权成功,这样,这台被授权的 DHCP 服务器就有分配 IP 的权利了。如图 2-7-3 所示,表明授权成功。

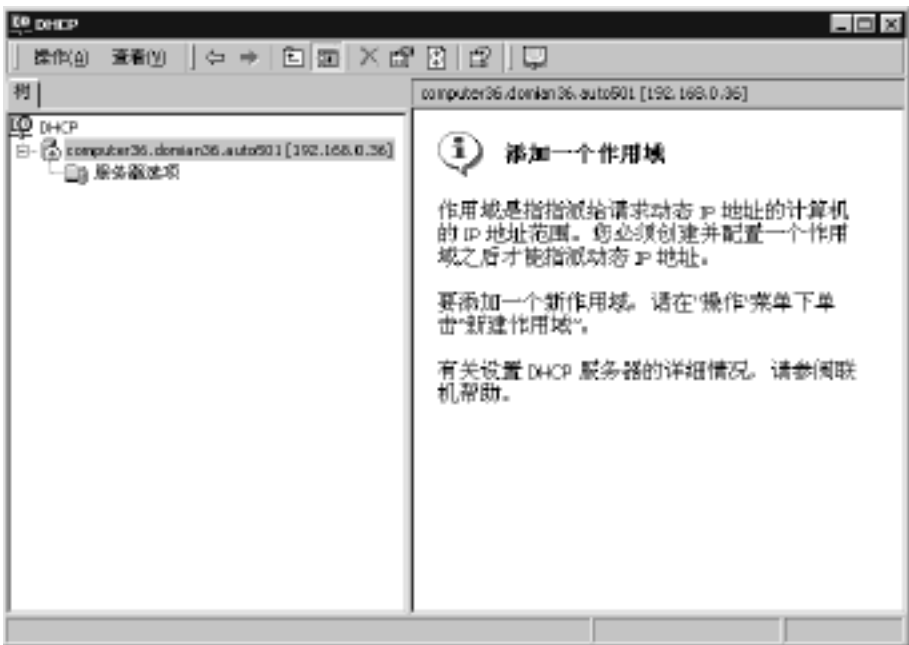


图 2-7-3 授权成功

7.4 DHCP 服务器的配置与管理

当 DHCP 服务器被授权后,还需要对它设置 IP 地址范围。通过给 DHCP 服务器设置 IP 地址范围后,当 DHCP 客户机在向 DHCP 服务器申请 IP 地址时,DHCP 服务器就会从所设置的 IP 地址范围中选择一个还没有被使用的 IP 地址进行动态分配。

具体操作如下:在图 2-7-3 中选中 DHCP 服务器名,在服务器名上单击鼠标右键,在出现的快捷菜单中选择“新建作用域”,启动新建作用域向导,如图 2-7-4 所示。



图 2-7-4 “新建作用域向导”界面

单击“下一步”按钮,如图 2-7-5 所示,填写作用域名称等信息。
单击“下一步”按钮,准备添加 IP 地址,如图 2-7-5 所示。
在图 2-7-6 所示的界面中,根据自己网络的实际情况,对各项进行设置,这里以私用

IP 地址为例。然后单击“ 下一步 ”按钮,出现如图 2-7-7 所示的界面。



图 2-7-5 输入作用域名称界面

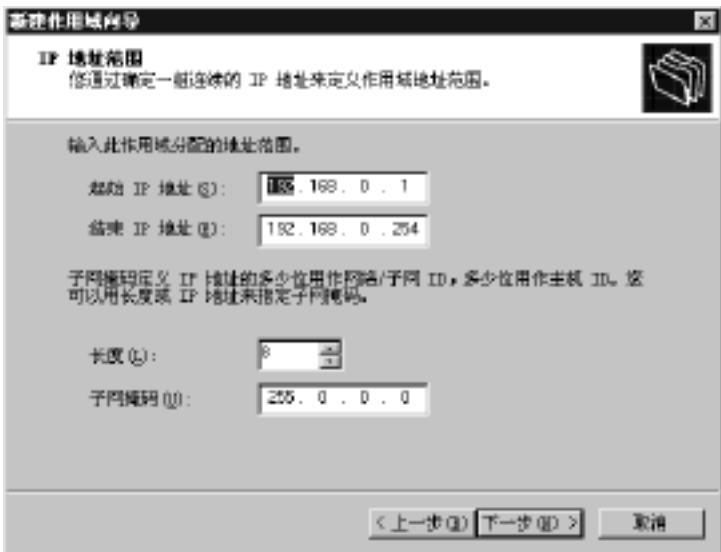


图 2-7-6 输入 IP 地址范围界面

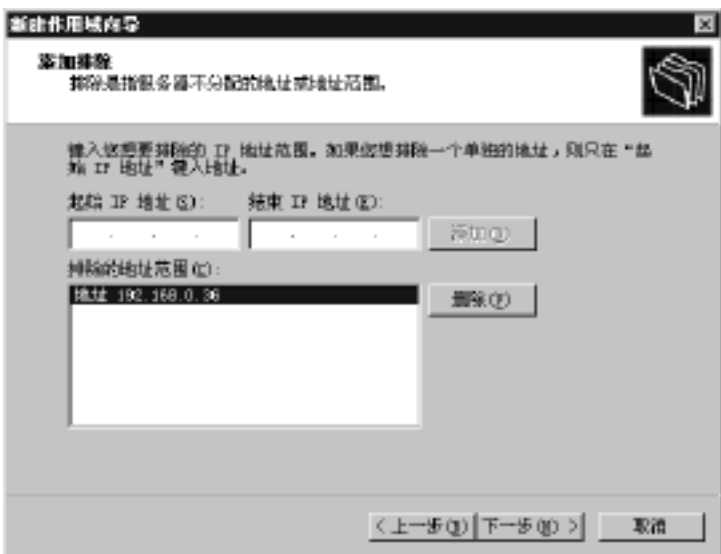


图 2-7-7 输入需要排除的 IP 地址范围界面

在图 2-7-7 中,输入需要排除的 IP 地址范围。由于校园网络中有很多网络设备需要指定静态 IP 地址(即固定的 IP 地址),如服务器、交换机、路由器等,此时必须把这些已经分配的 IP 地址从 DHCP 服务器的 IP 地址范围中排除,否则会引起 IP 地址的冲突,导致

网络故障。

如图 2-7-8 所示,在出现的“ 租约期限 ”界面中可以设置 IP 地址租期的时间值。一般情况下,如果校园网络中的 IP 地址比较紧张的时候,可以把租期设置短一些,而 IP 地址比较宽松时,可以把租期设置长一些。设置完后,单击“ 下一步 ”按钮,出现“ 配置 DHCP 选项 ”界面。如图 2-7-9 所示。



图 2-7-8 指定租约期限界面

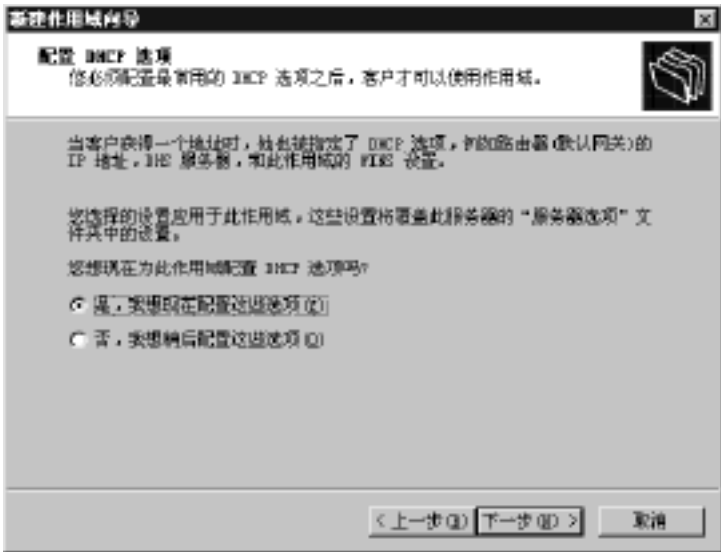


图 2-7-9 “ 配置 DHCP 选项 ”界面

在图 2-7-9 中,如果选择“ 是,我想现在配置这些选项 ”,此时可以对默认网关、DNS 服务器、WINS 服务器地址等内容进行设置;如果选择“ 否,我想稍后配置这些选项 ”,可以在需要这些功能时再进行配置。此处,我们选择前者,单击“ 下一步 ”按钮。开始配置默认网关,如图 2-7-10 所示。

在出现的界面中,常常输入网络中路由器的 IP 地址(即默认网关的 IP 地址)或是 NAT 服务器(网络地址转换服务器)的 IP 地址。这样,客户机从 DHCP 服务器那里得到的 IP 信息中就包含了默认网关的设定了,从而可以接入 Internet。

在图 2-7-11 中,设置有关客户机 DNS 域的名称,同时输入 DNS 服务器的名称和 IP 地址,然后单击“ 添加 ”按钮进行确认。添加完各地址后,单击“ 解析 ”按钮,自动解析到主机的 IP 地址,并填入 IP 地址框中。单击“ 下一步 ”按钮,在出现的界面中进行 WINS 服务

器的相关设置,如图 2-7-12 所示。



图 2-7-10 默认网关界面



图 2-7-11 “域名和 DNS 服务器”界面

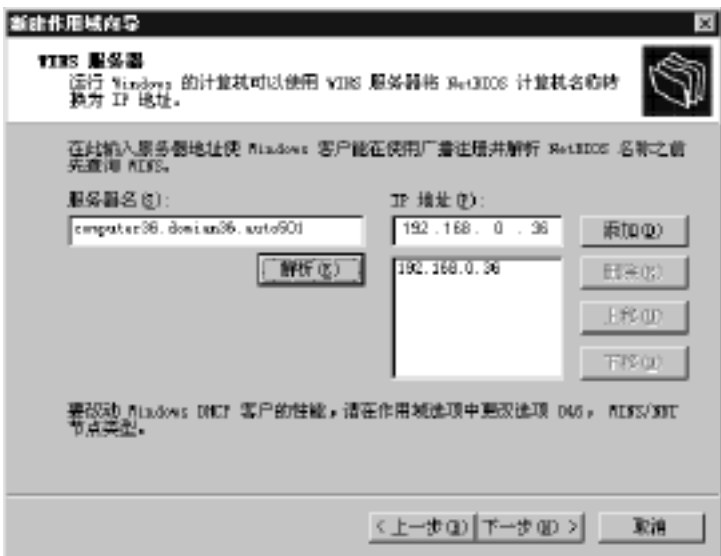


图 2-7-12 “WINS 服务器”界面

设置完成后,单击“解析”按钮,然后单击“下一步”按钮,出现如图 2-7-13 的界面。如图 2-7-13 所示,选择“是,我想现在激活此作用域”后,单击“下一步”按钮。在图 2-7-14 中单击“完成”按钮,设置结束。此时,就可以在 DHCP 管理器中看到刚

刚建好的作用域。如图 2-7-15 所示。



图 2-7-13 “激活作用域”界面



图 2-7-14 完成新建作用域向导界面

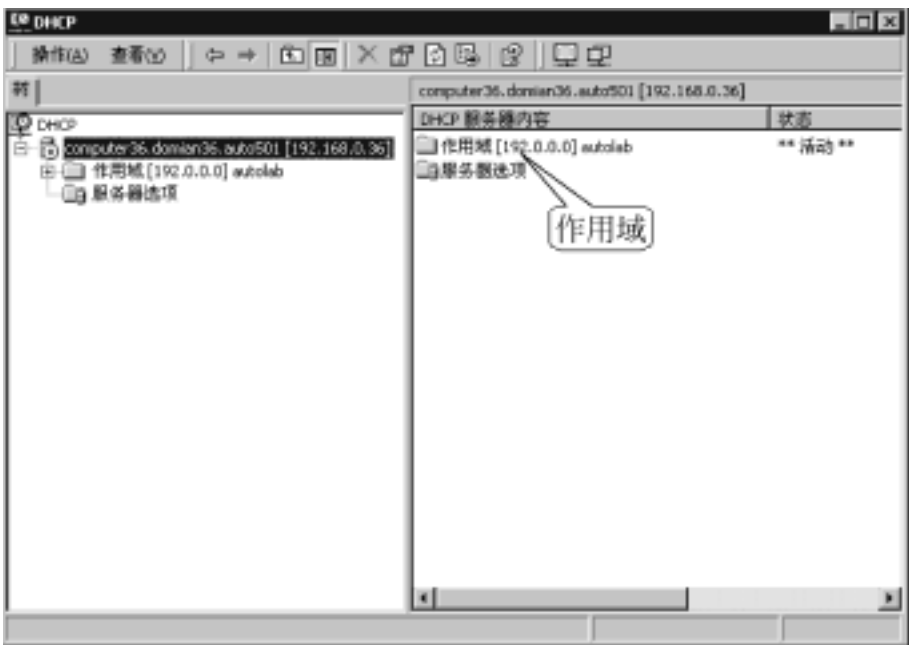


图 2-7-15 查看新建作用域窗口

在图 2-7-15 中,展开作用域,选中地址池,即可查看地址分配情况,如图 2-7-16 所示。

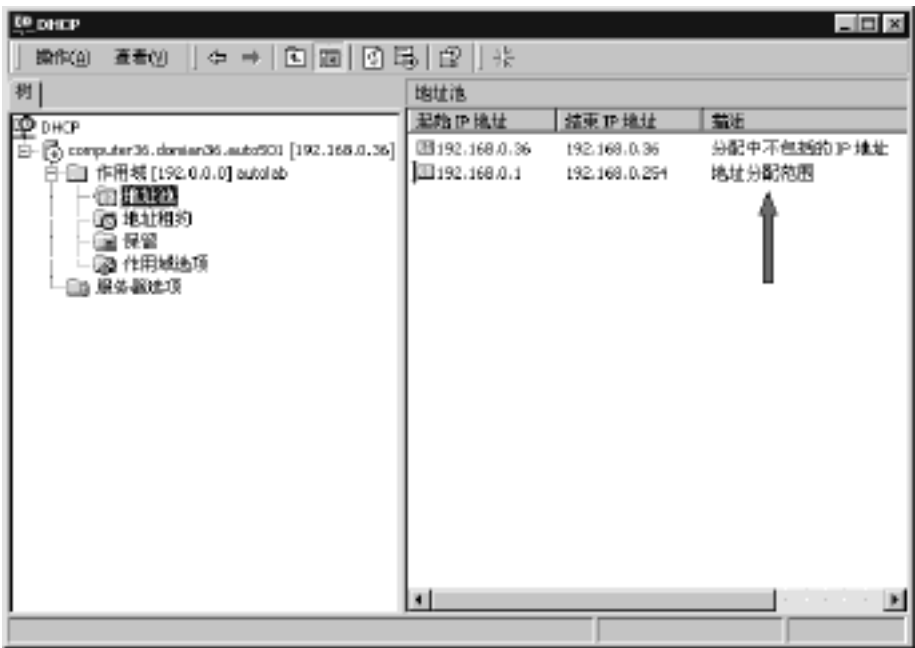


图 2-7-16 查看地址分配范围窗口

7.5 DHCP 服务的测试

经过上述设置,DHCP 服务已经正式启动,我们需要在客户机上进行测试。只需把客户机的 IP 地址选项设为“自动获得 IP 地址”,“自动获得 DNS 服务器地址”。如图 2-7-17所示。

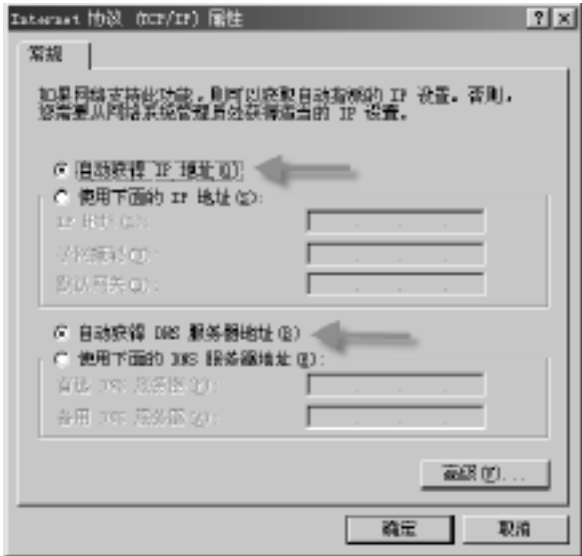
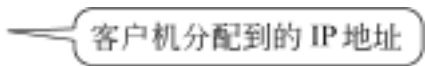


图 2-7-17 客户机 IP 地址设置界面

如果客户机为 Windows98 的操作系统则需要重新启动客户机,在客户机的“运行”对话框中输入“ Ipconfig/ all ”,即可看到客户机分配到的动态 IP 地址。

例 7-1

```
D: \> ipconfig / all
Windows 2000 IP Configuration
    Host Name . . . . . : computer35
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Hybrid
```

IP Routing Enabled : No
WINS Proxy Enabled : No
DNS Suffix Search List : computer36 .domian36
Ethernet adapter 本地连接:
 Connection-specific DNS Suffix . : computer36 .domian36
 Description : Realtek RTL8139(A) PCI Fast Etherne Adapter
 Physical Address : 00-50-70-61-0C-C5
 DHCP Enabled : Yes
 Autoconfiguration Enabled : Yes
 IP Address : 192 .168 .0 39  客户机分配到的 IP 地址
 Subnet Mask : 255 0 0 0
 Default Gateway : 192 .168 .0 36
 DHCP Server : 192 .168 .0 36
 DNS Servers : 192 .168 .0 36
 Primary WINS Server : 192 .168 .0 36
 Lease Obtained : 2005 年 4 月 8 日 10:23:02
 Lease Expires : 2005 年 4 月 16 日 10:23:02

实验八

常用网络操作命令

由于在不同的操作系统下操作命令也不尽相同,下面描述的操作命令都是在 Windows 2000 的命令行方式下实现的。

8.1 实验目的

通过该实验使学生掌握发现网络故障的方法,从而解决网络连通性问题。

8.2 常用命令

1 . arp

该指令的功能是将网络(IP)地址解析为物理(MAC)地址。

常用命令选项:

arp -a 或 arp -g: 用于查看当前 ARP 缓冲区中的内容。-a 和-g 参数的结果是一样的,多年来-g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项,而 Windows 用的是 arp -a,但它也可以接受比较传统的-g 选项。

arp -a IP: 如果你有多个网卡,那么使用 arp -a 加上接口的 IP 地址,就可以只显示与该接口相关的 ARP 缓存项目。

arp -s IP 物理地址: 你可以向 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。

arp -N 显示指定硬件地址的 ARP 条目。

例 8-1

```
D:\> arp -a
Interface: 166 .111 .73 .197 on Interface 0x10000003
Internet Address      Physical Address      Type
166 .111 .73 .1       00-04-0d-36-24-62    dynamic
166 .111 .73 .46      00-50-70-61-0e-11    dynamic
166 .111 .73 .128     00-50-70-61-0c-fa    dynamic
```

2 . ftp

该命令的格式为: ftp 服务器的名称或 IP 地址。

例 8-2

```
D:\> ftp ftp.tsinghua.edu.cn
Connected to ftp.tsinghua.edu.cn .
220 FTP Server of Tsinghua University ready .
User (ftp.tsinghua.edu.cn:(none)): anonymous
230-
230-      = = = = =
230-      Welcome to the FTP Server of
230-      Tsinghua University
230-
230-      = = = = =
230-      本站点由清华大学建立并维护,以服务于教育和科学研究为目的,
230-      面向但不仅限于清华大学的网络用户,提供相关数据、资料、软件等电子文件的下载服务。
230-
230-      本站倡导并推广开源软件文化,提供开源、免费系统及其应用软件
230-      的下载。本站努力追求原发数据的有效性和转发数据的完整性。在使用本站提供的数据、
230-      资料及软件时,请遵守其发行时所附带的许可证的要求。
230-
230-      用户在使用本站软件时必须遵守中华人民共和国、北京市人民政府、中国教育与科研计
230-      算机
230-      网络中心、清华大学信息网络工程研究中心和用户所在地的有关法律与相关规定。
230-
230-      本站目前提供 HTTP、FTP 和 RSYNC 三种方式的服务。
230-      = = = = =
230-
230 Anonymous user logged in
ftp> get welcome.msg ftpinfo
200 PORT command successful
150 Connecting to port 1381
226-File successfully transferred
226 0.001 seconds (measured here), 0.61 Mbytes per second
ftp: 817 bytes received in 0.02Seconds 51.06Kbytes/ sec .
ftp> bye
221-Goodbye . You uploaded 0 and downloaded 1 kbytes .
221 Logout .
> type ftpinfo

      = = = = =
      Welcome to the FTP Server of
      Tsinghua University

      = = = = =
      本站点由清华大学建立并维护,以服务于教育和科学研究为目的,面向但不仅限于清华大学的
      网络用户,提供相关数据、资料、软件等电子文件的下载服务。
```

本站倡导并推广开源软件文化,提供开源、免费系统及其应用程序的下载。本站努力追求原发数据的有效性和转发数据的完整性。在使用本站提供的数据、资料及软件时,请遵守其发行时所附带的许可证的要求。

用户在使用本站软件时必须遵守中华人民共和国、北京市人民政府、中国教育与科研计算机网络中心、清华大学信息网络工程研究中心和用户所在地的有关法律与相关规定。

本站目前提供 HTTP、FTP 和 RSYNC 三种方式的服务。

=====

3 . telnet

这是一个终端仿真程序,使你可以和远程登录服务器之间进行交互命令。它是网络系统管理员不可缺少的工具之一。系统管理员可以从任何地方登录到要维护的计算机上,对之进行维护,就像直接在控制台进行操作一样。还可以通过 Telnet 访问特定的服务器端口,查看服务器进程是否正常运行。

例 8-3 Telnet 的应用举例——电子公告牌 BBS 服务:
下面是访问清华大学 BBS 的屏幕显示。如图 2-8-1 所示。

d:\> telnet bbs .smth .edu .cn

正在连接到 bbs .smth .edu .cn ...

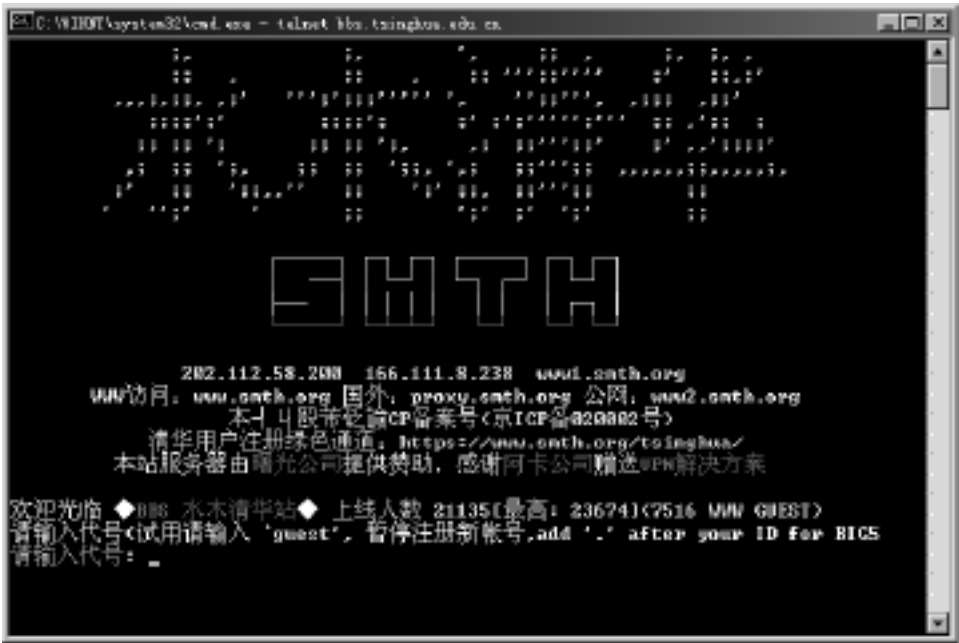


图 2-8-1 清华大学 BBS 的屏幕显示界面

然后用户可以用自己的账号登录。如果是第一次访问 BBS,则可用“ guest ”账号登录,对 BBS 进行浏览;或者用“ new ”账号登录,开始为自己申请一个 BBS 账号。

4 . ipconfig

ipconfig 命令能够显示系统的基本寻址信息,包括适配器名、MAC 地址、IP 地址、子网掩码和默认网关等。

ipconfig 最常用的选项:

ipconfig: 当使用 ipconfig 时不带任何参数选项,那么它为每个已经配置好的网卡显示 IP 地址、子网掩码和默认网关值。

ipconfig / all

当使用 all 选项时,ipconfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息(如 IP 地址等),并且显示内置于本地网卡中的物理地址(MAC)。如果 IP 地址是从 DHCP 服务器租用的,IPConfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

ipconfig / release 和 ipconfig / renew

这是两个附加选项,只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果我们输入 ipconfig / release,那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器(归还 IP 地址)。如果我们输入 ipconfig / renew,那么本地计算机便设法与 DHCP 服务器取得联系,并重新租用一个 IP 地址。ipconfig / release 将释放适配器上的 DHCP 租用信息,使 TCP/ IP 协议失效。大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。

例 8-4 D:\> ipconfig / all

```
Windows 2000 IP Configuration

Host Name . . . . . : station
Primary DNS Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : tsinghua .edu .cn

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . : tsinghua .edu .cn
    Description . . . . . : 3Com 3C920 Integrated Fast Ethernet
    Controller (3C905C-TX Compatible)

        Physical Address . . . . . : 00-06-5B-84-50-89
        DHCP Enabled . . . . . : Yes
        Autoconfiguration Enabled . . . . . : Yes
        IP Address . . . . . : 166 .111 .73 .197
        Subnet Mask . . . . . : 255 .255 .255 .0
        Default Gateway . . . . . : 166 .111 .73 .1
        DHCP Server . . . . . : 166 .111 .8 .7
        DNS Servers . . . . . : 166 .111 .8 .28
                                166 .111 .8 .29
        NetBIOS over Tcpip . . . . . : Disabled
        Lease Obtained . . . . . : 2005 年 3 月 16 日 9:03:32
        Lease Expires . . . . . : 2005 年 3 月 16 日 11:03:32
```

5 . tracert

确定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。一般用来检测故障的位置,你可以用 tracert IP 检查出在哪个环节上出了问题,Tracert 的使用很简单,只需要在 tracert 后面跟一个 IP 地址或 URL,它会进行相应的域名转换。

例 8-5

```
D:\>tracert 166.111.72.8
Tracing route to 166.111.72.8 over a maximum of 30 hops
  1  <10 ms  <10 ms  <10 ms  tu073001.ip.tsinghua.edu.cn [166.111.73.1]
  2    16 ms  <10 ms  <10 ms  166.111.72.8
Trace complete.
```

例 8-6

```
D:\>tracert www.baidu.com
Tracing route to www.cdnbaidu.com [202.108.250.249]
over a maximum of 30 hops:
  1  <10 ms  <10 ms  <10 ms  tu073001.ip.tsinghua.edu.cn [166.111.73.1]
  2  <10 ms  <10 ms  <10 ms  219.224.98.81
  3  <10 ms  <10 ms  <10 ms  219.224.97.1
  4    16 ms  <10 ms  <10 ms  219.224.96.5
  5    15 ms  <10 ms  <10 ms  202.112.38.9
  6    16 ms  <10 ms  <10 ms  202.112.36.254
  7  <10 ms  <10 ms    16 ms  202.112.62.46
  8  <10 ms    16 ms  <10 ms  202.38.123.18
  9    16 ms  <10 ms  <10 ms  202.38.123.10
 10   188 ms   172 ms   187 ms  219.158.28.73
 11   187 ms   172 ms   188 ms  219.158.11.89
 12    *      187 ms   203 ms  202.96.12.30
 13   188 ms    *      171 ms  202.106.192.18
 14   188 ms   187 ms   188 ms  202.108.46.14
 15   188 ms   171 ms   172 ms  202.108.250.29
 16    *      *      *      Request timed out.
 17   140 ms   156 ms   172 ms  202.108.250.249
Trace complete.
```

6 . ping

ping 是一个很有用的程序,它用于检验 TCP/ IP 是否成功安装。它向指定 IP 地址的主机发送 ICMP ECHO_REQUEST 包。该命令的一般格式为:ping [选项] 主机名/ IP 地址,命令中常用选项的含义如下:

- a 将 IP 地址解析为主机名。
- i 秒数 设定 TTL 域值。
- l 长度 指定长度,发送指定大小的请求回应分组。
- t 用于测试对某一特定主机的连接,直到用 Ctrl + C 停止。
- f 向网关提交“DO NOT FRAGMENT”命令。
- n 次数 这里的次数是记录发送和返回的分组所经过的路径。

例如:

Ping 127.0.0.1(内部回环测试)—检验 TCP/ IP 协议的操作、NIC 的收发功能。

- Ping 主机的 IP 地址—检验本地主机的 TCP/ IP 地址配置。
- Ping 默认网关地址—检验连接本地网络和其他网络的路由器是否可达。
- Ping 远端目的地的 IP 地址—检验与远端主机的连通性。

例 8-7

```
D: \> ping 166 .111 .73 .1
Pinging 166 .111 .73 .1 with 32 bytes of data:
Reply from 166 .111 .73 .1: bytes = 32 time < 10ms TTL = 30
Reply from 166 .111 .73 .1: bytes = 32 time < 10ms TTL = 30
Reply from 166 .111 .73 .1: bytes = 32 time < 10ms TTL = 30
Reply from 166 .111 .73 .1: bytes = 32 time < 10ms TTL = 30
Ping statistics for 166 .111 .73 .1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7 . netstat

netstat 命令的功能是显示网络连接、路由表和网络接口信息, 可以让用户得知目前都有哪些网络连接正在运作。该命令的一般格式为:

netstat [选项]

命令中各选项的含义如下:

- a 显示所有的连接和监听的端口。
- e 显示以太网统计数据, 这个选项可以和-S 选项一起使用。
- n 以数字形式来显示地址和端口数。
- r 显示路由选择表的内容。
- s 显示不同协议的统计数据。默认时, 显示 TCP、UDP 和 IP 的统计数据;-p 选项能用来指定一个特定的协议子集。

例 8-8 显示路由表: netstat -r

```
D: \> netstat -r
Route Table

=====
Interface List
0x1 .....MS TCP Loopback interface
0x1000003 .. .00 06 5b 84 50 89 .....3Com EtherLink PCI

=====
Active Routes:
Network  Destination      Netmask          Gateway           Interface         Metric
0 0 0 0      0 0 0 0          166 .111 .73 .1   166 .111 .73 .197 1
127 0 0 0    255 0 0 0        127 0 0 1        127 0 0 1        1
166 .111 .73 .0 255 255 255 0 166 .111 .73 .197 166 .111 .73 .197 1
166 .111 .73 .197 255 255 255 255 127 0 0 1        127 0 0 1        1
```

```
166 .111 .255 .255      255 .255 .255 .255      166 .111 .73 .197      166 .111 .73 .197      1
      224 .0 .0 .0      224 .0 .0 .0      166 .111 .73 .197      166 .111 .73 .197      1
255 .255 .255 .255      255 .255 .255 .255      166 .111 .73 .197      166 .111 .73 .197      1
Default Gateway:      166 .111 .73 .1
= = = = =
Persistent Routes:
None
```

例 8-9 在本地机上使用 netstat 命令。

```
D:\> netstat
Active Connections
Proto Local Address      Foreign Address    State
TCP   station:1347        station:microsoft-ds  TIME_WAIT
TCP   station:microsoft-ds  tu054022_ip.tsinghua.edu.cn:4406 ESTABLISHED
TCP   station:1229         166.111.8.11:30      ESTABLISHED
TCP   station:1230         166.111.8.76:31      ESTABLISHED
```

8 . nslookup

nslookup 命令的功能是查询一台机器的 IP 地址和其对应的域名。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器,就可以用这个命令查看不同主机的 IP 地址对应的域名。

该命令的一般格式为:

```
nslookup [IP 地址/ 域名]
```

例 8-10 在本地机上使用 nslookup 命令。

```
D:\> nslookup
Default Server: dns-a.tsinghua.edu.cn
Address: 166.111.8.28
>
```

在符号“ > ”后面输入要查询的 IP 地址或域名并回车即可。如果要退出该命令,输入 exit 并回车即可。

实验九

Socket 网络通信程序设计

9.1 实验目的

- (1) 掌握 TCP/ IP 网络 socket 机制的基本概念和方法。
- (2) 掌握 Linux 环境下的 Socket 程序设计方法,实现 TCP/ IP 网络环境下应用程序间的数据传输。

9.2 实验条件

有一台计算机装有 Red Hat 8.4,作为 Linux 服务器,同时在每台计算机上都安装有 UltraEdit-32,每个学生指定两台计算机,分别建立以自己学号命名的账号,在两台计算机上分别进行服务器和客户端的编程调试。

9.3 实验内容

1. 熟悉 Linux 系统

内容:由实验指导老师讲解上机的基本步骤,学生熟悉编程环境,编制简单的 C 程序。

- (1) 如何编辑源程序?
- (2) 如何编译连接,得到可执行文件?

2. Socket 编程基础

内容:熟悉基本的 Socket 函数,编制四种基本类型的服务器及相应的客户端程序。

- (1) 重复的无连接的服务器。
- (2) 重复的面向连接的服务器。
- (3) 并发的无连接的服务器。
- (4) 并发的面向连接的服务器。

要求:在服务器端运行服务器程序,在客户端运行客户程序,服务器向客户端发送一个字符串,客户端接受并显示该字符串后退出。

3. 利用已有的 Socket 调用设计一个网络实时交互游戏

内容:编制火柴棍游戏的服务器和客户端程序。

游戏由两人一组进行。原始状态下有三堆火柴棍,分别是 3,5,7 根。两个玩家轮流从中抽取火柴棍,抽得最后一根者判负。游戏规则: 每次只能从一堆火柴棍中抽取; 每次至少取一根,最多可以将一堆全部取走; 抽得最后一根火柴者(即本次操作后全部三堆火柴棍都已被取走),判负。

基本要求:

- (1) 游戏是二人通过网络交互式进行的。
- (2) 由于是在 Linux 环境下设计,不要求复杂的界面,可以用数字来表示每堆的火柴棍数目。要求游戏过程中有详细的提示,并有一定的容错性。
- (3) 游戏结束后,客户端退出,服务器继续运行,等待下一个玩家登录。

提高要求:

- (1) 完成超时判负功能,即一方长时间不操作,判定该玩家认输。
- (2) 解决可能出现的服务器死锁问题。(术语死锁是指一个或一组程序无法进行下去的状态,因为它们被阻塞并等待着一个永远不会发生的事件。简单来讲,服务器如果调用了 read 或 recv 来取来自客户端的下一个请求,但因某种原因,客户端未能发出这个请求,服务器进程将在该系统调用上被阻塞,从而使服务器不能回答请求。)

9.4 实验报告

实验完成后,应完成实验报告。报告内容为实验的总结报告和 Linux 环境下学习和使用 socket 网络编程的心得体会。报告应包括以下内容:

- (1) socket 网络通信机制的基本概念,程序设计方法。
- (2) 在实验过程中遇到的问题和解决方案。
- (3) 源程序文件功能说明;说明一共有几个文件,各自完成哪个实验或功能块。
- (4) 函数功能说明;对自己编写的函数,要做函数功能说明。按照函数原型,功能说明,参数说明的顺序介绍。
- (5) 打印所有源程序。

9.5 Linux 下常用的指令介绍

最重要的命令:man! man 是手册 (manual) 的意思,用来让使用者在使用时查询指令、系统呼叫、标准程式库函式、各种表格等的使用。在图形界面下,可以使用 xman,这是一个集成的帮助程序,使用更为方便。

1. 关于文件/目录处理的指令

ls: 显示某一个目录或是某一个文件的内容
cp: 复制文件
mv: 文件改名或移动
rm: 文件删除
mkdir: 建立目录

- cd: 切换工作目录
- pwd: 显示当前路径
- cat/ more: 查看文件内容
- 2 . 关于进程(process)处理的指令
 - ps: 显示目前系统状况
 - kill: 送一个信号给某个进程
- 3 . 网络指令
 - telnet: 登录到远端服务器
 - ftp: 网络文件传输
- 4 . 编译、连接指令
 - gcc: 编译,连接指令

9 .6 Linux 下常用套接字相关函数简介

socket	创建用于网络通信的描述符。
connect	连接远程对等实体(客户)。
write(send)	通过 TCP 连接外发数据。
read(recv)	从 TCP 连接中获得传入数据。
close	终止通信并释放描述符。
bind	将本地 IP 地址和协议端口号绑定到套接字上。
listen	将套接字置于被动模式,并设置在系统中排队的 TCP 传入连接的个数(服务器)。
accept	接收下一个传入连接(服务器)。
recv(read)	接收下一个传入的数据报。
recvmsg	接收下一个传入的数据报(recv 的变形)。
recvfrom	接收下一个传入的数据报并记录其源端点地址。
send(write)	发送外发的数据报。
sendmsg	发送外发的数据报(send 的变形)。
sendto	发送外发的数据报,往往是到预先记录下的端点地址。
shutdown	在一个或两个方向上终止 TCP 连接。
getpeername	在连接到达后,从套接字中获得远程机器的端点地址。
getsockopt	获得套接字的当前选项。
setsockopt	改变套接字的当前选项。
htonl	把长整数从本地字节顺序变换为网络字节顺序。
ntohl	把长整数从网络字节顺序变换为本地字节顺序。
htons	把短整数从本地字节顺序变换为网络字节顺序。
ntohs	把短整数从网络字节顺序变换为本地字节顺序。

9.7 Socket 网络通信编程实例

本节介绍 Socket 编程的一个例子。进行 Socket 编程,可供选择的编程语言很多,最常见的是 C 和 Java。所示程序用 C 语言编写,在 Linux 环境下运行(Red Hat 8.4 上编译、运行)。

在本例中,服务器程序在完成创建 socket,绑定端口,将套接字置于被动模式后开始监听,在无限循环中,服务器调用 accept 等待客户的连接请求。当新的连接请求到来时,系统为新的连接创建一个新套接字,然后创建一个新的进程来处理客户端的请求。为此,服务器调用 fork() 创建一个进程。新创建的子进程首先关闭原始套接字,然后进入回显服务子程序;父进程则关闭刚刚新建的新套接字,继续执行无限循环,即在 accept() 那里阻塞,等待下一个客户连接请求的到来。

客户端的程序相对要简单一些。对客户端来说,服务器是否支持并发并不影响自己的算法。和无连接的客户端程序相似,它也要先创建套接字,然后绑定到一个本机任意的未被使用的端口上。但接下来它将调用 connect 和服务器进行连接,如果成功地建立了与服务器的连接,客户将使用这个连接和服务器通信。

下面分别给出了服务器和客户端的源程序:

1. 服务器端程序

```

/ *
multiTcpServer.c - - - - - main, echoService
*/
#include <unistd.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <sys/signal.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/resource.h>
#include <sys/wait.h>
#include <sys/errno.h>
#include <netinet/in.h>
#define DEFAULT_PORT 2345      / * 服务器默认监听端口 */
#define MAX_QLEN 10           / * 最大连接队列数 */
#define BUFSIZE 1024          / * 读缓冲区大小 */
/ *
    main - - - 提供回显服务的 TCP 并发服务器端程序主函数
    usage: multiTcpServer [port]
*/
void echoService( int sock );

```



```
int main(int argc, char * argv[])
{
    int m_sock, s_sock;           /* m_sock: 主套接字, s_sock: 从套接字 */
    struct sockaddr_in server;     /* 存放服务器信息 */
    struct sockaddr_in client;     /* 存放客户端信息 */
    int port;                     /* 服务器监听端口号 */
    int qlen;                     /* 连接队列数 */
    int rval, length;
    switch( argc )
    {
        case 1:
            port = DEFAULT_PORT;  /* 不带参数运行, 使用默认端口号 */
            break;
        case 2:
            port = atoi(argv[1]);  /* 使用运行时指定的端口号 */
            break;
        default:
            perror( usage: multiTcpServer [port]\n );
            exit(1);
    }
    qlen = MAX_QLEN;  /* 连接队列数取最大值 */
    /* 创建套接字 */
    m_sock = socket(PF_INET, SOCK_STREAM, 0);
    if( m_sock < 0 )  /* 错误检测 */
    {
        perror( can't create socket\n );
        exit(1);
    }
    /* 填写服务器地址信息 */
    server.sin_family = AF_INET;
    server.sin_addr.s_addr = INADDR_ANY;
    server.sin_port = htons(port);
    /* 绑定到端口 */
    rval = bind( m_sock, (struct sockaddr *) &server, sizeof(server) );
    if ( rval < 0 ) /* 错误检测 */
    {
        perror( binding error\n );
        exit(1);
    }
    /* 开始监听 */
    rval = listen( m_sock, qlen );
    if( rval < 0 ) /* 错误检测 */
    {
        perror( listening error\n );
    }
}
```

```
        exit(1);
    }
    /* 服务器进入死循环,等待客户端联入 */
do
{
    /* 接受客户端连接请求 */
    length = sizeof( struct sockaddr_in );
    s_sock = accept( m_sock, (struct sockaddr* ) &client, &length );
    if( s_sock < 0 ) /* 错误检测 */
    {
        perror( accepting error\n );
        exit(0);
    }
    /* 调用 fork() 创建一个新的从进程处理客户的请求 */
    switch( fork() )
    {
        case - 1: /* 错误检测 */
            perror( fork error ! \n );
            exit(1);
        case 0: /* 子进程 */
            /* 关闭主套接字,进入服务子程序 */
            close( m_sock );
            echoService( s_sock );
            exit(0);
        default: /* 主进程 */
            /* 关闭从套接字,继续等待新的客户端连入 */
            close( s_sock );
    }
}
while (1); /* 循环结束 */
} /* 主函数结束 */
/*
    echoService - - - 提供回显服务的子函数
*/
void echoService( int sock )
{
    char buf[BUFSIZE];
    int rval;
    /* 循环接受客户端的输入,直到客户端输入 END 结束 */
do
{
    /* 接受客户端输入 */
    bzero(buf,sizeof(buf));
    rval = read( sock, buf, sizeof(buf) );
```

```

        if( rval<0 ) / * 错误检测 */
        {
            perror( reading error\n );
            exit(1);
        }
/ * 判断客户端是否输入 END,如是则结束服务 */
if( strcmp( buf, END ) == 0 )
    return;
else
{
    / * 将接受的字符串再回送给客户端 */
    rval = write(sock, buf, strlen(buf));
    if( rval<0 ) / * 错误检测 */
    {
        perror( writing error );
        exit(1);
    }
}
}
while(1); / * 循环结束 */
}

```

2 . 客户端程序

```

/ *
    tcpClient.c - - - - - main
*/
#include <sys/ types.h>
#include <sys/ socket.h>
#include <netinet/ in.h>
#include <netdb.h>
#include <stdio.h>
#define DEFAULT_PORT 2345 / * 服务器默认绑定端口 */
#define BUFSIZE 1024 / * 读缓冲区大小 */
/ *
    main - - - 回显服务的客户端程序(TCP)
    usage: tcpClient [xxx.xxx.xxx.xxx, [port]]
*/
int main(int argc, char * argv[])
{
    int sock; / * 套接字描述符 */
    struct sockaddr_in server; / * 存放服务器信息 */
    struct hostent * hp; / * 存放服务器地址 */
    int port; / * 服务器绑定端口号 */
    char buf[BUFSIZE];

```

```
int rval;
switch( argc )
{
    case 1:
        /* 不带参数运行,使用本机地址和默认端口号 */
        hp = gethostbyname( localhost );
        port = DEFAULT_PORT;
        break;
    case 2:
        /* 使用运行时指定的 ip 地址和默认端口号 */
        hp = gethostbyname(argv[1]);
        port = DEFAULT_PORT;
        break;
    case 3:
        /* 使用运行时指定的 ip 地址和端口号 */
        hp = gethostbyname(argv[1]);
        port = atoi(argv[2]);
        break;
    default:
        perror( usage: tcpClient [xxx.xxx.xxx.xxx, [port]]\n );
        exit(1);
}
if (hp == 0) /* 错误检测 */
{
    printf( %s:unknown host ,argv[1]);
    exit(1);
}
/* 创建套接字 */
sock = socket( PF_INET, SOCK_STREAM, 0 );
if( sock < 0 ) /* 错误检测 */
{
    perror( opening stream socket );
    exit(1);
}
server.sin_family = AF_INET;
bcopy((char *)hp -> h_addr, (char *)&server.sin_addr, hp -> h_length);
server.sin_port = htons(port);
/* 连接服务器 */
rval = connect(sock, (struct sockaddr *)&server, sizeof(server));
if(rval < 0) /* 错误检测 */
{
    perror( connecting stream socket );
    exit(1);
}
```

```
/*
    客户端接受键盘输入的字符串,发送给服务器后,再接受服务器返回的同样
    内容,并打印出来
*/
do
{
    scanf( %s , buf);
    rval = write(sock, buf, strlen(buf));
    if( rval< 0 )
    {
        perror( writing stream message );
        exit(1);
    }
    if( strcmp(buf, END ) == 0 )
        break;
    bzero(buf, sizeof(buf));
    rval = read(sock, buf, sizeof(buf));
    if( rval< 0 )
    {
        perror( reading stream message );
        exit(1);
    }
    printf( Echo from the host: %s\n , buf);
}
while(1); /* 循环结束 */
close(sock);
} /* 主函数结束 */
```

参 考 文 献

- 1 张曾科 . 计算机网络 第 2 版 北京:清华大学出版社,2005
- 2 谢希仁 . 计算机网络 第 4 版 北京:电子工业出版社,2003
- 3 Andrew S Tanenbaum 著 . 计算机网络 第 4 版 潘爱民译 . 徐明伟审 北京:清华大学出版社,2004
- 4 Douglas E Comer 著 . 用 TCP/ IP 进行网际互联, 第一卷 原理、协议与结构 第四版 .林瑶等译 .北京:电子工业出版社,2001
- 5 Douglas E Comer 著 . 计算机网络与因特网 . 徐良贤,唐英,王勋等译 .北京:机械工业出版社,2000
- 6 Cisco Systems 公司 Cisco Networking Academy Program 著 . 思科网络技术学院教程(第一、二学期)(第 3 版) .清华大学等译 .北京:人民邮电出版社,2004
- 7 Cisco Systems 公司 Cisco Networking Academy Program 著 . 思科网络技术学院教程(第三、四学期)(第 3 版) .天津大学等译 .北京:人民邮电出版社,2004
- 8 张建忠,徐敬东 . 计算机网络实验指导书 .北京:清华大学出版社,2005
- 9 黄叔武,张玉祥 . 计算机网络工程教程——题解与实验指导 北京:清华大学出版社,1999
- 10 吴功宜,吴英 . 计算机网络应用技术教程 . 北京:清华大学出版社,2003