高等院校计算机应用系列教材

网络安全基础与实践

谭江汇　罗小刚　周　亮　罗梁城　编著

清華大學出版社
北　京

内 容 简 介

本书全面而深入地介绍了网络安全的基础知识、核心概念、关键技术和实践应用。内容涵盖了计算机网络的基本概念、发展历程，以及网络安全的基本概念、发展历程、相关技术等多个方面。本书通过对这些关键领域的详细阐述，为读者提供了一个全面的网络安全知识体系，帮助读者理解并掌握网络安全的基本原理和应用实践。

本书内容丰富，结构合理，思路清晰，从网络基础开始，逐一介绍了网络相关的基础理论，讨论网络攻击技术和网络防御技术。此外，本书还涵盖了密码技术应用、网络安全协议，以及渗透测试和后渗透测试等内容，为读者提供了全面的网络安全知识和实践指导。

本书配套的电子课件、习题答案、教学大纲和实验指导书可以到 http://www.tupwk.com.cn/downpage 网站下载，也可以扫描前言中的二维码获取。

图书在版编目(CIP)数据

网络安全基础与实践 / 谭江汇等编著. -- 北京 :
清华大学出版社, 2025. 6. -- (高等院校计算机应用系列教材).
ISBN 978-7-302-69171-6

I. TP393.08

中国国家版本馆 CIP 数据核字第 2025UB9428 号

责任编辑：胡辰浩
封面设计：高娟妮
版式设计：恒复文化
责任校对：成凤进
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-83470000　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市天利华印刷装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**19.25　　**字　　数：**493 千字
版　　次：2025 年 7 月第 1 版　　**印　　次：**2025 年 7 月第 1 次印刷
定　　价：79.80 元

产品编号：102144-01

前　言

在信息技术飞速发展的今天，计算机网络已成为现代社会的基础设施，它不仅连接了全球各地的计算机系统，还促进了信息的快速流通和资源的共享。随着网络技术的不断进步，网络的规模和复杂性也在不断增长，网络安全也已经成为个人、企业和国家层面上不可忽视的重要议题。随着互联网技术的飞速发展，网络攻击手段日益复杂，数据泄露和网络犯罪事件频发，这使得网络安全防护变得尤为重要。本书旨在为读者提供一个全面的网络安全学习平台，帮助读者建立起系统的网络安全知识体系，掌握关键的网络安全技术和实践技能。

本书的编写团队由具有丰富教学经验和工程实践的教师组成。他们将理论与实践相结合，确保本书内容的前沿性和实用性。全书首先对计算机网络和网络安全的基本概念进行了介绍，包括计算机网络的结构、网络设备的选择、网络安全的重要性、面临的威胁以及网络安全的目标。随后，从如何应对网络威胁展开，深入探讨了防火墙技术，这也是网络安全中最为关键的技术之一。全书不仅介绍了防火墙的工作原理和类型，还详细讲解了如何配置和管理防火墙，以及如何在实际网络环境中应用防火墙技术。

本书共分为 10 章，内容涵盖了计算机网络的基础知识、路由交换技术、网络安全以及动态路由协议等。第 1 章介绍了计算机网络的基本概念、发展历史和功能，为读者奠定了学习的基础。第 2 章则深入探讨计算机网络协议，包括以太网帧格式、IP 数据报格式、ARP 协议、ICMP 协议和 TCP 协议等。第 3 章详细介绍路由交换基础，包括交换机的工作原理、路由原理和静态路由的配置等。第 4 章则聚焦于动态路由协议，特别是 RIP 和 OSPF 协议的工作原理和配置方法。

在网络安全方面，第 5 章和第 6 章分别讨论了防火墙和网络安全设备。第 7 章详细介绍网络安全体系和技术。第 8 章和第 9 章则详细介绍渗透测试和后渗透测试的相关知识，包括口令破解、中间人攻击和恶意代码攻击等。第 10 章则聚焦于入侵防御及流量分析，为读者提供了网络安全的高级知识和技能。

我们希望本书能够成为计算机网络领域的学习者和从业者的良师益友，帮助他们在网络技术的道路上不断前进。同时，我们也期待读者的反馈和建议，以便我们不断改进和完善本书内容。

除封面署名的作者外，参与本书编写的人员还有张智祥、李志远等人。由于作者水平有限，书中难免有不足之处，恳请专家和广大读者批评指正。在编写本书的过程中参考了相关文献，在此向这些文献的作者深表感谢。我们的电话是 010-62796045，邮箱是 992116@qq.com。

本书配套的电子课件、习题答案、教学大纲和实验指导书可以到 http://www.tupwk.com.cn/downpage 网站下载，也可以扫描下方的二维码获取。

作者

2025 年 2 月

目　录

∞ 第1章 ∞

概　　述

本章主要介绍计算机网络和网络安全的基础知识，包括计算机网络的功能和发展简史；计算机网络体系结构的分层原理和两种参考模型；网络安全的概念、基本要素等。

1.1 计算机网络概述

计算机网络是现代通信技术与计算机技术紧密结合的产物，从20世纪50年代末开始出现到现在，发展得非常快。到目前为止，我们可以将计算机网络定义为将分布在不同地理位置的具有独立功能的多台计算机及其外部设备，通过通信线路和通信设备连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现信息传递和资源共享的计算机系统。

计算机和外部设备的种类多种多样，并且新的产品还在不断涌现。目前，我们所熟知的有各种巨型、大型、中型、小型和微型计算机，以及平板电脑、智能手机、打印机、可穿戴设备、家用电器、智能传感器、PLC(可编程逻辑控制器)等设备。

1.1.1 计算机网络的功能

计算机网络的功能主要体现在以下四个方面。

(1) 信息交换：计算机之间进行信息交换是计算机网络的基本功能。数据通信是依照一定的通信协议，利用数据传输技术在两个计算机之间传递数据信息的一种通信方式和通信业务。利用数据通信技术可以实现计算机网络中各个节点之间的信息传递，如人们可以通过计算机网络传送电子邮件、发布新闻、预订酒店和机票、召开网络视频会议等。

(2) 资源共享：资源共享是人们建立计算机网络的主要目的之一。计算机网络的资源包括硬件资源、软件资源、数据资源、信道资源。硬件资源包括计算机、大容量存储设备、计算机外部设备(如打印机、扫描仪)等。软件资源包括各种应用软件、工具软件、系统开发所用的支撑软件、数据库管理系统等。数据资源包括数据库、办公文档资料、各类生产环节的数据等。信道资源即通信信道，是电信号的传输介质。

(3) 分布式处理：分布式处理是将一个复杂的大问题分解成多个小问题，分别交由计算机网络中的多个计算机共同处理。在此过程中，参与分布式处理的计算机能够根据各个计算机系

统的负荷情况进行动态调整，将负荷较重的计算机的处理任务传送到网络中的其他计算机系统中，以提高整个系统的利用率。同时各个计算机之间通过数据交换，形成了一种强大的整体计算能力。

(4) 提高系统的可靠性：对于关键部门的重要应用，可利用计算机网络中的冗余计算机节点实现系统的高可靠性。例如，工作中的一台计算机发生了故障，可以将任务方便地切换到另外一台计算机上继续工作。

1.1.2 计算机网络发展简史

计算机网络是现代通信技术与计算机技术紧密结合的产物。计算机网络的发展过程其实就是通信技术与计算机技术相结合的过程。计算机网络是伴随着计算机性能的提高和应用需求的提升而不断发展的，从产生到相对成熟，主要经历了以下四个阶段。它的发展促进了计算机技术、多媒体技术和通信技术的飞速发展。

1. 面向终端的计算机网络

面向终端的计算机网络又称为远程联机系统，是第一代计算机网络，它产生于 20 世纪 50 年代。第一代计算机网络主要有两种模式：具有通信功能的单机系统和具有通信功能的多机系统，如图 1-1 所示。

图 1-1 面向终端的计算机网络

20 世纪五六十年代，计算机价格昂贵、体积巨大、数量稀少，为了让更多的科技人员使用计算机，充分发挥计算机的工作效率，人们将一台计算机通过通信线缆与若干台终端连接起来构成一个网络，实现多人同时使用一台计算机来共享资源。严格意义上讲，这一阶段的网络并不能称为现代意义上的计算机网络，而应该称为远程终端联机，但这一阶段的研究成果为现代的计算机网络做好了技术准备，奠定了理论基础。这种系统的典型代表是美国军方在 1954 年研制的半自动地面防空系统(SAGE)，它将远程雷达与其他测量设备及基地的一台 IBM 计算机直接连接，实现集中的防空信息处理和控制。

2. 计算机—计算机网络

第二代计算机网络是在 20 世纪 60 年代中期发展起来的。这类网络是多台主机通过通信线路互联，以达到资源共享或者联合起来完成某项任务的目的。这就是早期以数据交换为主要目的的计算机网络，即所谓的计算机—计算机网络，如图 1-2 所示。这一阶段主要有两个标志性成果：一是提出分组交换技术；二是形成了 TCP/IP 的雏形。

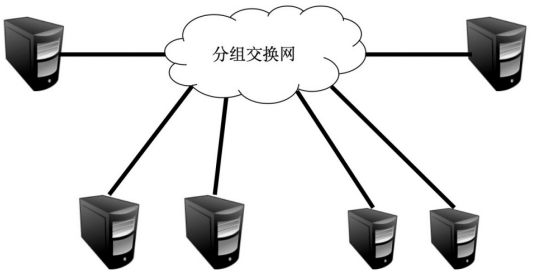

图 1-2　计算机—计算机网络

3. 标准化的计算机网络

20 世纪 70 年代末至 80 年代初，第二代计算机网络的发展使计算机资源进入了共享时代，加快了计算机应用的普及。但同时由于没有统一的网络标准，不同厂商研制出的计算机网络无法方便地互联，从而限制了计算机硬件、软件和数据的大范围共享。一个公司的多个分公司要实现信息共享，不得不采用同一厂商的计算机、网络设备和软件。因此，计算机网络的标准化成为当务之急。

20 世纪 80 年代中期，国际标准化组织(ISO)公布了 ISO7498，即 ISO OSI/RM 国际标准，该模型包括七个子层。另外，在 ARPANet 基础上，发展出了以 TCP/IP 为核心的 Internet 体系结构，该模型包括四个子层。因此，目前存在两个计算机网络体系结构的标准。法律上的国际标准为 ISO OSI/RM，但并没有得到广泛认可，而非法律意义上的国际标准 TCP/IP 却得到了广泛应用，这也使得 TCP/IP 成为事实上的国际标准。

4. 国际互联网和信息高速公路

20 世纪 90 年代后，计算机网络进一步朝着高速化、智能化、综合化和全球化方向发展。世界范围内建立了难以计数的局域网、城域网、广域网，进而形成了覆盖世界绝大多数国家的以 Internet 为代表的国际互联网。1993 年美国政府发布了“国家信息基础设施行动计划”的文件，其核心就是构建国家信息高速公路。在这之后，各个国家都建立起了自己的高速 Internet，而这些国家级 Internet 的互联构成了全球互联网，将计算机网络的应用渗透到社会的各个领域。

1.2　分层模型

我们在处理复杂问题时，通常采用的方法是将它分成一个一个小的简单的问题，逐一处理。对于网络亦如此，将网络进行层次划分，就可以将网络这个庞大而复杂的问题划分成若干较小的问题，从而解决计算机网络这个大问题。

1.2.1　分层思想

计算机网络层次结构划分依据以下原则：功能相似或紧密相关的模块应放在同一层；层与层之间应保持松散的耦合，使信息在层与层之间的流动减到最小。

对计算机网络进行层次划分的优点包括以下几个方面。

(1) 各层之间相互独立。高层不需要知道它的下一层是如何实现的，而仅需要知道该层通

过层间的接口所提供的服务。

(2) 灵活性好。当任何一层发生变化时，只要接口保持不变，则在这层以上或以下各层均不受影响。另外，当某层提供的服务不再需要时，甚至可将这层取消。

(3) 各层都可以采用适合自己的技术来实现，各层实现技术的改变不影响其他层。

(4) 易于实现和维护。整个系统已经被分解为若干个易于处理的部分，这种结构使一个庞大而又复杂系统的实现和维护变得容易控制。

(5) 有利于网络标准化。因为每一层的功能和所提供的服务都已经有了精确的说明，所以标准化变得较为容易。

1.2.2 OSI 参考模型

1. OSI 参考模型概述

为了充分发挥计算机网络的作用，使不同计算机厂家的网络能够连接且相互通信，这时就需要一个国际标准，遵守国际标准的网络才能互联互通。国际标准化组织(ISO)颁布的开放系统互联参考模型(OSI/RM)，自上而下分别是应用层、表示层、会话层、传输层、网络层、数据链路层和物理层，也就是七层网络通信模型，简称七层模型。

开放系统互联参考模型的分层思想使复杂的网络体系结构变得层次分明、结构清晰，整个网络的设计变成了对各层及层间接口的设计，这极大地便利了网络的设计和实现。网络中的每个节点都被划分为 7 个相同的层次结构；不同节点的相同层次拥有相同的功能；同一节点内各相邻层次间通过接口进行通信；每一个上级层次向下级层次提出服务请求，使用下层提供的服务；下层向上层提供服务；不同节点的对等层之间按对等层协议进行通信。

2. OSI 参考模型各层的功能

(1) 物理层：它处于 OSI 参考模型的最底层，利用传输介质为上层提供物理连接，负责处理数据传输率并监控数据出错率，以便透明地传送数据，这是物理层的主要功能。

(2) 数据链路层：在物理层提供比特数据流传输服务的基础上，数据链路层通过在通信的实体之间建立数据链路连接，传送以“帧”为单位的数据，使有差错的物理线路变成无差错的数据链路，保障点到点的可靠的数据传输。

(3) 网络层：为处在不同网络系统中的两个节点设备通信提供一条逻辑通道。其基本功能包括路由选择、拥塞控制和网络互联等。

(4) 传输层：向用户提供可靠的端到端服务，透明地传送报文。它向高层屏蔽了下层数据通信的细节，因而是计算机通信体系结构中最关键的一层，也是承上启下的一层。

(5) 会话层：主要功能是建立、管理和终止应用进程之间的会话和数据交换，这种会话关系是由两个或多个表示层实体之间的对话构成的。

(6) 表示层：保证一个系统应用层发出的信息能被另一个系统的应用层读出。如果有必要，表示层用一种通用的数据表示格式在多种数据表示格式之间进行转换。其主要功能包括数据格式变换、数据加密与解密，以及数据压缩与恢复等。

(7) 应用层：这是最靠近用户的一层，它为用户的应用程序提供网络服务，包括电子数据表程序、字处理程序和银行终端程序等。

1.2.3　TCP/IP 协议簇

尽管 OSI 参考模型得到了全世界的认同，但是互联网历史上和技术上的标准都是 TCP/IP (Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议)参考模型。

TCP/IP 起源于 20 世纪 60 年代末美国政府资助的网络分组交换研究项目。TCP/IP 是发展至今最成功的通信协议，用于当今最大的开放式网络系统 Internet。

TCP 和 IP 是两个独立且紧密结合的协议，负责管理和引导数据报文在 Internet 上的传输。二者使用专门的报文头定义每个报文的内容。TCP 负责和远程主机的连接，IP 负责寻址，使报文被送到其该去的地方。TCP/IP 也分为不同的层次，每一层负责不同的通信功能。但 TCP/IP 简化了层次(只有 4 层)，自上而下分别为应用层、传输层、网络层和网络接口层。表 1-1 是 OSI 参考模型和 TCP/IP 参考模型间的对应关系。

表 1-1　OSI 参考模型和 TCP/IP 参考模型间的对应关系

OSI 参考模型	TCP/IP 参考模型
应用层	应用层
表示层	
会话层	
传输层	传输层
网络层	网络层
数据链路层	网络接口层
物理层	

TCP/IP 协议簇则是一组用于在计算机网络上进行通信的协议。它是现代互联网通信的基础，由一系列相互关联的协议组成，确保数据在网络上的可靠传输和互连设备的相互通信。其中，关键协议主要包括：IP(Internet Protocol)、TCP(Transmission Control Protocol)、UDP(User Datagram Protocol)、ICMP(Internet Control Message Protocol)、ARP(Address Resolution Protocol)、DHCP(Dynamic Host Configuration Protocol)、DNS(Domain Name System)。

1.3　网络安全概述

随着计算机网络的发展，信息传递和信息共享越来越快速，人们的生活也因此变得越来越方便。大数据时代对人们的生活产生了非常重要的影响，网络已经成为人们生活和学习不可或缺的一部分。但是随着计算机网络技术的发展，网络为生产和生活带来效益的同时，也带来了诸多的挑战。要保证信息的安全和可靠，网络安全的重要性也就不言而喻。

1.3.1　网络安全的定义与意义

网络安全是指保护计算机网络、信息系统及其中的数据免受未经授权的访问、攻击、泄露或破坏的技术和实践。其核心目标是确保数据的机密性、完整性和可用性，以保障系统的正常

运行并防止敏感信息被篡改或泄露。在信息化社会中，网络安全涵盖从个人隐私保护到国家关键基础设施防护的广泛领域。它涉及身份认证、数据加密、防火墙、入侵检测、恶意软件防护等技术手段，以及完善的安全策略和应急响应体系。随着网络攻击手段日益多样化，网络安全的重要性日益凸显，它不仅关乎企业和个人的利益，也与国家安全和社会稳定息息相关，成为数字化发展的关键保障。

网络安全作为一个关系国家安全和社会稳定的重要因素，其重要性随着全球信息化发展的脚步而迅速提升。网络安全涉及计算机科学、网络技术、通信网络、密码学、信息安全及应用数学等多个学科的综合实践。因此，网络安全在信息化社会中具有至关重要的地位。

随着数字技术的普及，信息网络已渗透到个人生活、企业运营和国家基础设施中，保护数据和系统的安全性成了不可忽视的问题。对于个人而言，网络安全保护个人隐私，避免财产损失和身份盗用；对于企业而言，网络安全保障业务的连续性和客户信任；对国家而言，网络安全维护关键基础设施的安全，防范潜在的网络攻击威胁。网络安全已成为支持数字经济发展、维护社会稳定的关键要素。

1.3.2 网络安全的基本要素

网络安全的基本要素主要包括机密性(Confidentiality)、完整性(Integrity)和可用性(Availability)，即“CIA 三要素”。这三个要素是保障信息安全的核心目标，决定了网络系统和数据的安全性。此外，网络安全还包括认证、访问控制、加密、审计等关键支持要素。

(1) 机密性：机密性是指确保数据和信息仅能被授权的用户访问，防止未授权访问和信息泄露。通过身份验证、访问控制和数据加密等手段，可以保障数据在存储和传输过程中的私密性。例如，在银行系统中，客户的账户信息只有客户本人和被授权的工作人员可以查看。机密性是网络安全最基本的要求之一，尤其在金融、医疗等涉及敏感数据的领域至关重要。

(2) 完整性：完整性是指保证数据的准确性和一致性，防止数据被篡改或破坏。数据完整性不仅指静态数据的完整性(例如数据库中的记录未被恶意篡改)，还包括在传输过程中数据的完整性。通过数字签名、校验和、访问控制等措施，可以有效地保证数据的完整性。例如，在文件传输中使用哈希值校验，可以确保接收到的文件没有被篡改。数据完整性尤为重要，因为篡改数据会对决策、服务和用户信任造成极大影响。

(3) 可用性：可用性指信息系统、服务和数据在需要时能被授权用户访问，保证业务和操作的连续性。防止因拒绝服务攻击(DoS)、系统崩溃或人为破坏而造成系统不可用的情况，是实现可用性的关键。通过冗余设计、备份、灾难恢复、网络负载均衡等措施，可以提升系统的可用性。例如，金融机构通过异地备份来保障服务在灾难发生时仍然可用。可用性直接影响业务的连续性，是网络安全策略的关键目标之一。

此外，认证和授权是网络安全的支持要素，通过用户身份验证和访问权限控制来防止未授权的访问。加密技术在保护数据传输和存储的机密性中发挥着重要作用。审计和监控可以记录并追踪用户活动、检测异常行为，有助于及时发现安全威胁并采取应对措施。

1.3.3 常见的网络安全组件

以下是常见的计算机网络安全组件。这些组件在网络中扮演了重要角色，确保网络的运行

和通信是高效、安全的。

(1) 入侵检测系统(Intrusion Detection System，IDS)：负责监视网络流量，检测和报告潜在的安全威胁和攻击。

(2) 入侵防御系统(Intrusion Prevention System，IPS)：阻止潜在的网络攻击，具有主动的防御功能。

(3) 防病毒软件(Antivirus Software)：检测、阻止和删除计算机病毒和恶意软件。

(4) 虚拟专用网络(Virtual Private Network，VPN)：加密网络连接，确保数据在互联网上的安全传输。

(5) 安全认证设备(Authentication Devices)：包括令牌、生物识别设备等，用于确认用户身份。

(6) 加密设备(Encryption Devices)：用于对数据进行加密，确保数据在传输和存储过程中的安全性。

1.4 本章小结

本章从计算机网络的定义入手，介绍了计算机网络的基本功能，计算机网络的发展简史，计算机网络的分层模型。由此引入网络安全的概念、介绍网络安全的定义与意义，以及网络安全基本要素和常见网络安全设备概述，为后续章节做铺垫。

1.5 本章习题

1. 选择题

(1) 下列关于 OSI 参考模型的描述错误的是(　　)。

A. 定义了将两个层连接在一起的过程，提高了厂商之间的互操作性

B. 使一个系统可与位于世界上任何地方的、遵循同一标准的其他系统进行通信

C. 将复杂的功能分为多个更简单的组件

D. 定义了所有网络协议都适用的 8 个层

E. 提供了一种教学工具，可帮助网络管理员了解网络设备间的通信过程

(2) 将下列各层从高到低排列为正确的顺序：(　　)。

会话层(a)，表示层(b)，物理层(c)，数据链路层(d)，网络层(e)，应用层(f)，传输层(g)

A. c，d，e，g，a，b，f　　B. f，a，b，g，d，e，c

C. f，b，g，a，e，d，c　　D. f，b，a，g，e，d，c

3. 下面(　　)不是 TCP/IP 协议簇中应用层的网络协议。

A. HTTP　　B. FTP　　C. SMTP　　D. IP

2. 简答题

(1) 什么是计算机网络？
(2) 计算机网络的发展分为哪几个阶段？每个阶段有什么特点？
(3) 计算机网络的主要功能是什么？
(4) 网络应用层有哪些协议？一一列举并说明它们的主要用途。
(5) 计算机网络为什么采用层次化的体系结构？
(6) 网络安全的定义是什么？请简述网络安全的基本要素。

∞ 第 2 章 ∞

计算机网络协议

本章主要介绍计算机网络中数据通信最基本的内容，通过学习计算机网络中终端间的通信方式及原理，用户可掌握局域网数据传输结构以及传输的不同形式。本章还介绍以太网数据帧结构、IP 数据报格式，各类数据传输所用到的协议如 ARP 协议、ICMP 协议、TCP 协议、UDP 协议以及数据传输过程。

2.1 终端间的通信

终端间的通信，在计算机网络中也称为局域网通信。局域网(LAN)用于连接小的地理范围(如一个办公室、一幢大楼、一个单位)的计算机工作站、文件服务器、打印机和网络设备等，以实现内部的数据、文件、打印机等资源的共享。因此一般而言，网络为一个单位所拥有，且地理范围和站点数目均有限。

局域网技术主要涉及数据链路层，而数据链路层的数据传输单元被称为帧。所以我们首先需要了解通信中采用的帧格式，以及有哪些通信模式。

2.1.1 Ethernet_II 帧格式

局域网是以太网(Ethernet)的一部分，以太网最早是由美国的 Xerox 公司与前 DEC 公司设计的一种通信方式，当时命名为 Ethernet。之后 IEEE 802.3 委员会将其规范化。但是这两者对以太网帧的格式定义还是有所不同的。因此，IEEE 802.3 所规范的以太网有时又被称为 802.3 以太网。

我们先来看以太网的 Ethernet_II 帧格式，如图 2-1 所示，以太网帧前端有一个称为前导码(Preamble)的部分，它由 0、1 数字交替组合而成，表示一个以太网帧的开始，也是对端网卡能够确保与其同步的标志。前导码末尾是一个称为 SFD(Start Frame Delimiter，帧起始界定符)的域，它的值是“11”。在这个域之后就是以太网帧的本体。前导码与 SFD 合起来占 8 字节。

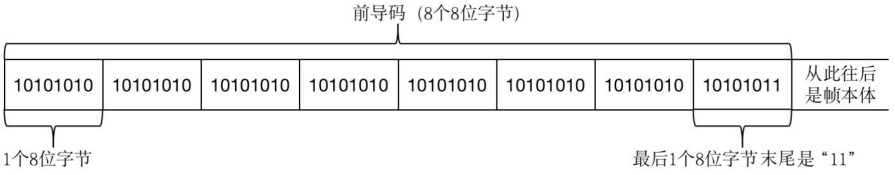

图 2-1　Ethernet_II 帧前导码

一般以太网中将最后的 2 比特称为 SDF，而 IEEE 802.3 中将最后的 8 比特称为 SDF。以太网帧本体的前端是以太网的首部，它总共占 14 字节，分别是 6 字节的目标 MAC 地址、6 字节的源 MAC 地址及 2 字节的上层协议类型。

注意：比特(位)、字节、8 位字节

◎ 比特(位)：二进制中最小的单位。每个比特(位)的值要么是 0，要么是 1。

◎ 字节：通常 8 个比特构成 1 字节。本书就以 8 比特作为 1 字节处理。然而在某些特殊的计算机中，1 字节有时包含 6 比特、7 比特或 9 比特。

◎ 8 位字节：8 比特也称为 8 位字节。强调 1 字节包含 8 比特时才使用。

如图 2-2 所示，Ethernet_II 帧格式中包括目标 MAC 地址、源 MAC 地址、类型，以及紧随帧头后面的数据。一个数据帧所能容纳的数据范围是 46~1500 字节。帧尾是 FCS(Frame Check Sequence，帧检验序列)，占 4 字节。在目标 MAC 地址中存放了目标工作站的物理地址。源 MAC 地址中则存放构造以太网帧的发送端工作站的物理地址。

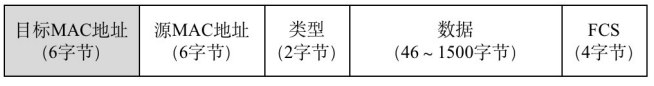

图 2-2　Ethernet_II 帧格式

类型通常跟数据一起传送，它包含用于标识协议类型的编号，即表明以太网的再上一层网络协议的类型。在这个字段的后面，则是该类型所标识的协议首部及其数据。

帧尾最后出现的是 FCS，可用于检查数据是否有所损坏。在通信传输过程中，如果出现电子噪声的干扰，可能会影响发送数据，导致乱码位的出现。因此，通过检查 FCS 字段的值可以将那些受到噪声干扰的错误帧丢弃。

FCS 中保存着整个帧除以生成多项式的余数。在接收端也用同样的方式进行计算，如果得到的 FCS 值相同，即可判定所接收的帧没有差错。

2.1.2　IEEE 802.3 帧格式

IEEE 802.3 帧格式与 Ethernet_II 帧格式类似，只是增加了 IEEE 802.3 的规范，使其相比一般以太网帧在帧的首部上稍有区别，如图 2-3 所示。一般以太网帧中表示类型的字段，在 IEEE 802.3 以太网中却表示帧的长度。此外，数据部分的前端还有 LLC 和 SNAP 等字段。而标识上一层协议类型的字段就出现在 SNAP 中。不过，SINAP 中指定的协议类型与一般以太网协议类型的意思基本相同。

图 2-3　IEEE 802.3 帧格式

2.1.3　数据通信模式

数据通信模式包括单播、组播和广播三种。

(1) 单播。在计算机网络中，单播通信是一种基本的通信模式，是终端间通信中最常见的通信方式，在计算机网络中广泛应用。单播通信是指封包在计算机网络中传输时目的地址为单一目标的传输方式。通常所使用的网络协议或服务大多采用单播传输，例如一切基于 TCP 的协议。

(2) 组播。在计算机网络中，组播通信是计算机网络中一种特殊的通信模式，用于将数据信息同时传递给一组目的地址。组播的使用策略是最高效的，因为消息在每条网络链路上只需传递一次，而且只有在链路分叉的时候，消息才会被复制。“组播”这个词通常用来指代 IP 组播。IP 组播是一种通过使用一个组播地址将数据在同一时间以高效的方式发往处于 TCP/IP 网络上的多个接收者的协议。此外，它还常用来与 RTP 等音视频协议相结合。

(3) 广播。与组播通信类似，广播通信也是计算机网络中的一种特殊通信模式，用于将数据从一个源设备发送到网络中的所有设备。在广播通信中，广播域是网络中能接收任一台主机发出的广播帧的所有主机集合。也就是说，如果广播域内的其中一台主机发出一个广播帧，同一广播域内所有的其他主机都可以收到该广播帧。

2.1.4　IP 数据报格式

了解 IP 数据报格式，主要是认识 IP 首部。数据在通信时，需要在数据的前面加入 IP 首部信息。IP 首部包含用于 IP 协议进行发包控制时的所有必要信息，首部固定长度为 20 字节。了解 IP 首部的结构，也就能够对 IP 所提供的功能有一个详细的把握。IP 数据报格式如表 2-1 所示。

表 2-1　IP 数据报格式

<table>
<tr><td>版本
Version(4)</td><td>首部长度
IHL (4)</td><td>优先级与服务类型
(8)</td><td colspan="2">总长度
Total length(16)</td></tr>
<tr><td colspan="3">标识
Identification(16)</td><td>标志
Flags (3)</td><td>片偏移
(13)</td></tr>
<tr><td colspan="2">生存时间
TTL(8)</td><td>协议
Protocol(8)</td><td colspan="2">首部校验和
(16)</td></tr>
<tr><td colspan="5">源地址
Source Address(32)</td></tr>
<tr><td colspan="5">目的地址
Destination Address(32)</td></tr>
<tr><td colspan="3">可选项
Options</td><td colspan="2">填充
Padding</td></tr>
<tr><td colspan="5">数据
Data</td></tr>
</table>

(1) 版本 Version：由 4 比特构成，表示 IP 的版本号。IPv4 的版本号即为 4，因此在这个字段上的值也是 4。此外，关于 IP 的所有版本已在表 2-2 中列出。

表 2-2　IP 的所有版本

版本	简称	协议
4	IP	Internet Protocol
5	ST	ST Datagram Mode
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX：The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA

注意：关于 IP 版本号，IPv4 的下一个版本是 IPv6。那么为什么要从版本 4 直接跳到版本 6 呢?这里需要提到的是，IP 版本号的含义与普通软件的版本号有所区别。普通的软件产品，版本号会随着更新逐渐增大，最新版本号即为最大号码。这是基于每款软件都由特定的软件公司或团体进行开发才能实现的。

(2) 首部长度(Internet Header Length，IHL)：由 4 比特构成，表明 IP 首部的长度。该字段的取值以 4 字节(32 比特)为单位。对于没有可选项的 IP 包，首部长度则设置为 5。也就是说，当没有可选项时，IP 首部的长度为 20(4×5=20)字节。

(3) 优先级与服务类型(8)：该字段用于表示数据包的优先级和服务类型。通过在数据包中划分确定的优先级，服务类型定义了如何处理数据。该字段一般不被使用。

(4) 总长度(16)：表示 IP 首部与数据部分合起来的总字节数。该字段长 16 比特。因此 IP 包的最大长度为 65535(2^{16}−1)字节，包括包头和数据。目前还不存在能够传输最大长度为 65535 字节的 IP 包的数据链路。不过，由于有 IP 分片处理，从 IP 的上一层的角度看，不论底层采用何种数据链路，都可以认为能够以 IP 的最大包长传输数据。

(5) 标识(16)：由 16 比特构成，用于分片重组。同一个分片的标识值相同，不同分片的标识值不同。通常，每发送一个 IP 包，它的值也逐渐递增。此外，即使标识值相同，如果目标地址、源地址或协议不同的话，也会被认为是不同的分片。

(6) 标志(3)：和标识符一起传递，指示不可以被分片或者最后一个分片是否发出(完整)。

(7) 片偏移(13)：由 13 比特构成，用来标识被分片的每一个分段相对于原始数据的位置。第一个分片对应的值为 0。由于片偏移域占 13 位，因此最多可以表示 8192(2^{13})个相对位置。单位为 8 字节，因此最大可表示原始数据 8×8192=65536 字节的位置。

(8) 生存时间(Time To Live，TTL)(8)：由 8 比特构成，它最初的意思是以秒为单位记录当前包在网络上应该生存的期限。然而，在实际中它是指可以中转多少个路由器。每经过一个路由器，TTL 会减少 1，变成 0 时丢弃该包，可以防止一个数据包在网络中无限循环地转发下去。

(9) 协议(8)：由 8 比特构成，表示 IP 首部的下一个首部隶属于哪个协议，即封装的上层哪个协议，比如 ICMP：1，TCP：6，UDP：17。

(10) 首部校验和(16)：由 16 比特(2 字节)构成，也称 IP 首部校验和。该字段只校验数据报的首部，不校验数据部分。它主要用来确保 IP 数据报不被破坏。校验和的计算过程，首先要将

该校验和的所有位置设置为 0，然后以 16 比特为单位划分 IP 首部并用 1 补数计算所有 16 位字的和。最后将所得到这个和的 1 补数赋给首部校验和字段。

(11) 源地址(32)：由 32 比特(4 字节)构成，表示发送端 IP 地址。

(12) 目的地址(32)：由 32 比特(4 字节)构成，表示接收端 IP 地址。

(13) 可选项：长度可变，通常只在进行实验或诊断时使用。该字段包含安全级别、源路径、路径记录和时间戳。

(14) 填充：填充字段也称填补物。在有可选项的情况下，首部长度可能不是 32 比特的整数倍。为此，通过向该字段填充 0，将首部长度调整为 32 比特的整数倍。

(15) 数据：数据字段的内容即上层数据。将 IP 上层协议的首部也作为数据进行处理。

2.2 ARP 协议

在数据传输中，只要确定了 IP 地址，就可以向这个目标地址发送 IP 数据报。然而，在底层数据链路层，进行实际通信时却有必要了解每个 IP 地址所对应的 MAC 地址。

ARP 是一种解决地址问题的协议，以目标 IP 地址为线索，用来定位下一个应该接收数据分包的网络设备对应的 MAC 地址。如果目标主机不在同一个链路上时，可以通过 ARP 查找下一跳路由器的 MAC 地址。不过 ARP 只适用于 IPv4，不能用于 IPv6。IPv6 中可以用 ICMPv6 替代 ARP 发送邻居探索消息。

2.2.1 广播与广播域

在认识 ARP 协议的具体原理之前，我们首先要知道广播和广播域的概念。因为 ARP 的工作机制需要用到广播和广播域。

在前面我们已经提到过广播的具体工作过程，它就是将广播地址作为目标地址的数据帧发送给广播域中的所有设备。广播域是指在网络中能接收到同一个广播的所有节点的集合(广播域越小越好，收到的垃圾广播越少，这样通信效率更高)。如图 2-4 所示，每个圈都是一个广播域，说明了交换机隔离不了广播域，路由器可以隔离广播域(物理隔离)。

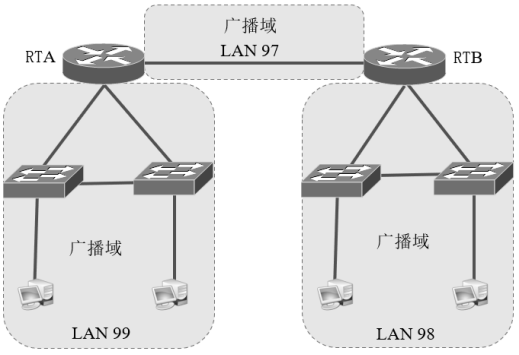

图 2-4　广播域示意图

2.2.2 ARP 协议原理

接下来，我们具体来看 ARP 协议的工作原理。首先 ARP 协议是一个地址解析协议，它属于内网协议，在内网工作，跑不出当前局域网，会被路由器隔离。那么 ARP 又是如何工作的呢？简单地说，ARP 是借助 ARP 请求与 ARP 响应两种类型的包确定目的 MAC 地址的，从而找到目标主机。如图 2-5 所示，假定主机 A 向同一链路上的主机 B 发送 IP 包，主机 A 的 IP 地址为 172.20.1.1，主机 B 的 IP 地址为 172.20.1.2，它们互不知道对方的 MAC 地址。

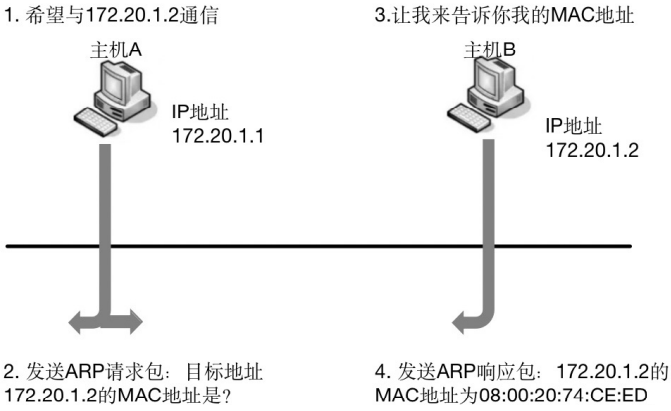

图 2-5　ARP 工作原理

主机 A 为了获得主机 B 的 MAC 地址，起初要通过广播发送一个 ARP 请求包，这个包中包含了想要了解其 MAC 地址的主机 IP 地址。也就是说，ARP 请求包中已经包含了主机 B 的 IP 地址 172.20.1.2。由于广播的包可以被同一个链路上所有的主机或路由器接收，因此 ARP 的请求包也就会被这同一个链路上所有的主机和路由器进行解析。如果 ARP 请求包中的目标 IP 地址与自己的 IP 地址一致，这个节点就将自己的 MAC 地址塞入 ARP 响应包返回给主机 A。

根据 ARP 可以动态地进行地址解析，因此，在 TCP/IP 的网络构造和网络通信中无须事先知道 MAC 地址究竟是什么，只要有 IP 地址即可。如果每发送一个 IP 数据报都要进行一次 ARP 请求以此确定 MAC 地址，那将会造成不必要的网络流量，因此，通常的做法是把获取到的 MAC 地址缓存一段时间。即把第一次通过 ARP 获取到的 MAC 地址作为 IP 对 MAC 的映射关系记忆到一个 ARP 缓存表中，下一次再向这个 IP 地址发送数据报时不需再重新发送 ARP 请求，而是直接使用这个缓存表当中的 MAC 地址进行数据报的发送。每执行一次 ARP，其对应的缓存内容都会被清除。不过在清除之前不需要执行 ARP，就可以获取想要的 MAC 地址。这样，在一定程度上也防止了 ARP 包在网络上被大量广播的可能性。

2.3 ICMP 协议

ICMP 是辅助 IP 协议的，是在 IPv4 中产生辅助作用的协议。架构 IP 网络时需要特别注意两点：确认网络是否正常工作，以及遇到异常时进行问题诊断。

例如，一个刚刚搭建好的网络，需要验证该网络的设置是否正确。此外为了确保网络能够

按照预期正常工作，一旦遇到什么问题，需要立即制止问题的蔓延。为了减轻网络管理员的负担，这些都是必不可少的功能。ICMP 正是提供这类功能的协议。

2.3.1　ICMP 的主要功能

ICMP 的主要功能包括：确认 IP 包是否成功送达目标地址，通知在发送过程当中 IP 包被废弃的具体原因，改善网络设置等。有了这些功能以后，就可以获得网络是否正常、设置是否有误以及设备有何异常等信息，从而便于诊断网络上的问题。

在 IP 通信中，如果某个 IP 包因为某种原因未能到达目标地址，那么这个具体的原因将由 ICMP 负责通知。如图 2-6 所示，主机 A 向主机 B 发送了数据包，由于某种原因，途中的路由器 2 未能发现主机 B 的存在，这时，路由器 2 就会向主机 A 发送一个 ICMP 包，说明发往主机 B 的包未能成功。ICMP 的这种通知消息会使用 IP 进行发送。因此，从路由器 2 返回的 ICMP 包会按照往常的路由控制，先经过路由器 1 再转发给主机 A。收到该 ICMP 包的主机 A 则分解 ICMP 的首部和数据域，以得知具体发生问题的原因。

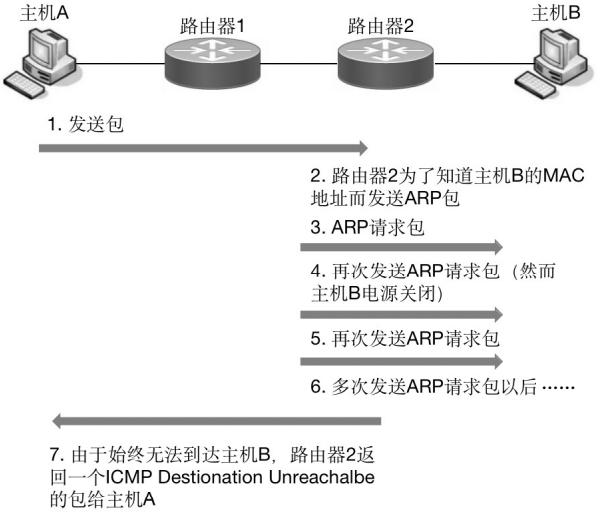

图 2-6　ICMP 目标不可达消息

2.3.2　ICMP 的基本使用

在使用过程中，ICMP 协议可以让路由器或者目的主机在 IP 数据报出现差错的时候通知源主机。下面介绍一个使用 ICMP 协议的常用命令：ping。

ping(Packet Internet Groper)，是一个应用层的通信协议，是 TCP/IP 协议的一部分，常用作网络诊断工具。作为一个因特网包探索器，ping 用来测试两个主机之间网络的连通性。它使用 ICMP 回送请求与回送回答报文。给目标 IP 地址的主机发送一个 ICMP 请求回显报文，要求对方返回一个同样大小的数据包，来确定两台网络机器是否连接相通，时延是多少。比如在 Windows 操作系统输入：Ping mail.sina.com.cn，屏幕会显示如下信息：

```
正在 Ping common7.dpool.sina.com.cn [49.7.36.27] 具有 32 字节的数据：
来自 49.7.36.27 的回复:字节 =32 时间 =26ms TTL=53
来自 49.7.36.27 的回复:字节=32 时间=28ms TTL=53
```

```
来自 49.7.36.27 的回复:字节=32 时间 =31ms TTL=53
来自 49.7.36.27 的回复:字节=32 时间 =27ms TTL=53

49.7.36.27 的 Ping 统计信息:
    数据包:已发送 =4,已接收 =4,丢失 =0(0% 丢失)
往返行程的估计时间(以毫秒为单位):
    最短=26ms,最长=31ms,平均 =28ms
```

“平均=28ms”是平均的响应时间，这个时间越小，说明连接这个地址的速度越快。如果想查看本地的 TCP/IP 协议是否设置好，输入命令：Ping 空格 127.0.0.1，如果接收和发送的数据都相等，那就是完好的。屏幕显示信息如下：

```
正在 Ping 127.0.0.1 具有 32 字节的数据：
来自 127.0.0.1 的回复:字节=32 时间 <1ms TTL=128
来自 127.0.0.1 的回复:字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复:字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复:字节=32 时间<1ms TTL=128

127.0.0.1 的 Ping 统计信息：
    数据包:已发送 =4,已接收 =4,丢失 =0(0% 丢失)
往返行程的估计时间(以毫秒为单位):
    最短=0ms,最长=0ms,平均=0ms
```

ICMP 的消息大致可以分为两类：一类是通知出错原因的错误消息，另一类是用于诊断的查询消息。表 2-3 列举了 ICMP 的消息类型。

表 2-3 ICMP 消息类型

类型(十进制数)	内容
0	回送应答(Echo Reply)
3	目标不可达(Destination Unreachable)
4	原点抑制(Source Quench)
5	重定向或改变路由(Redirect)
8	回送请求(Echo Request)
9	路由器公告(Router Advertisement)
10	路由器请求(Router Solicitation)
11	超时(Time Exceeded)
17	地址子网请求(Address Mask Request)
18	地址子网应答(Address Mask Reply)

2.4 TCP 协议

为了通过 IP 数据报实现可靠传输，需要考虑很多事情，例如数据的破坏丢包、重复以及分片顺序混乱等问题。若不能解决这些问题，可靠传输也就无从谈起。TCP 通过检验和、序列号、

确认应答、重发控制、连接管理以及窗口控制等机制实现可靠传输。

2.4.1　TCP 报文格式

首先我们来看 TCP 报文的格式。TCP 报文段也叫 TCP 分组，是 TCP 协议传输和接收数据的一种封装格式，只有按照该格式发送的数据才可以被 TCP 协议通信的双方正确接收与解析。TCP 报文的组成如表 2-4 所示。

表 2-4　TCP 报文格式

<table>
<tr><td colspan="5">源端口</td><td colspan="4">目的端口</td></tr>
<tr><td colspan="9">序号</td></tr>
<tr><td colspan="9">确认号</td></tr>
<tr><td>数据偏移</td><td>保留</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>窗口</td></tr>
<tr><td colspan="5">检验和</td><td colspan="4">紧急指针</td></tr>
<tr><td colspan="7">选项(长度可变)</td><td colspan="2">填充</td></tr>
<tr><td colspan="9">数据</td></tr>
</table>

TCP 报文组成具体介绍如下。

- 源端口：标识源端应用进程，即发送 TCP 分组的进程端口。
- 目的端口：标识目的端应用进程，即需要接收分组数据的进程端口号。
- 序号(seq)：在 SYN 标志未置 1 时，该字段指示了用户数据区中的第一个字节的序列号；在 SYN 标志置 1 时，该字段指示的是初始发送的序列号。
- 确认号(ACK)：用来确认本端 TCP 实体已经接收到的数据，其值表示期待对端发送的下一个字节的序号，实际上是在告诉对方，这个序号减 1 以前的字节已经正确接收。例如发送确认号为 1001，则表示前 1000 字节已经被确认接收。
- 数据偏移：以 32bit 为单位的 TCP 分组头的总长度，用于确定用户数据区的起始位置。
- RST：连接复位，对方要求重新连接。把携带 RST 标识的报文段称为复位报文段。
- SYN：请求建立连接，也是同步序号，当 SYN 置 1 时，表示建立连接，分组将发送 seq 为初始序列号(其值一般随机)。
- FIN：结束标志，表示关闭连接，当该字段置 1 时，表示分组将要关闭连接。
- ACK：确认号有效的标志，置 1 时表示确认号有效。
- URG：紧急指针有效的标志，置 1 时表示紧急指针有效。
- PSH：Push 操作，提示接收端应用程序立刻从 TCP 缓冲区把数据读走。

2.4.2　TCP 三次握手

TCP 连接的建立是通过三次握手的过程完成的。下面将具体讲解三次握手的过程。

如图 2-7 所示，第一次握手由主机 A(作为 client)向主机 B(作为 server)发送一个 TCP 数据报，

其中，TCP 分组的源端口为主机 A 发起通信建立的进程端口，而目的端口为主机 B 处理请求的进程端口号，比如 80 端口。在表示建立连接的 TCP 分组中，SYN 标志位置 1，则告知主机 B 发送该分组的目的是请求建立连接，并且当 SYN 置 1 时，该分组中的 seq 字段发送的是初始序列号 cilent_isn。

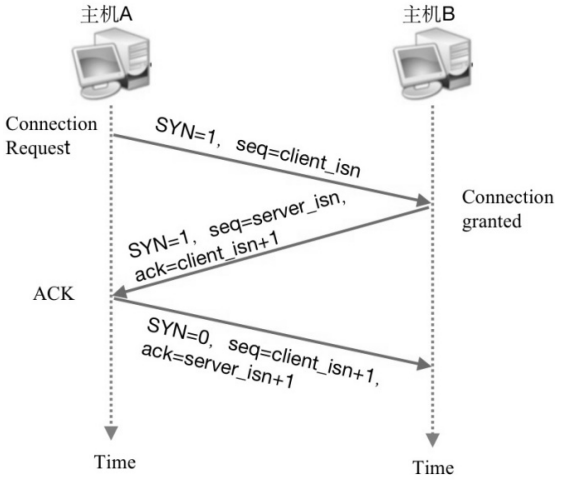

图 2-7　TCP 三次握手

第二次握手由主机 B 向主机 A 发出：主机 B 在成功接收了主机 A 第一次握手发送的 TCP 分组后，首先需要解析收到的 TCP 分组，发现 SYN 置 1 后，得知这个主机 A 发送分组的目的是建立连接，在确认完分组信息后，主机 B 也会向主机 A 发送一个 TCP 分组来代表第二次握手。

第三次握手由主机 A 向主机 B 发出：主机 A 在接收到主机 B 第二次握手的回复之后，同样会接收来自主机 B 的 TCP 分组并进行解读，由 SYN 为 1 解读该 TCP 分组的目的是继续建立连接，由分组中的 ACK 确认号了解到主机 B 已经成功接收了前 cilent_isn 字节的内容，并期望接收第 cilent_isn+1 字节的字节序号，同时确认来自主机 B 的初始序列号，并发送最后一个 TCP 分组给主机 B 来完成第三次握手。

采用三次握手是为了防止建立重复的连接而损耗资源或造成其他问题，确保双向通信的可靠性，最常见的是可以防止旧连接的重复初始化。比如在网络存在延迟的情况下，Client(客户端)之前发送的 SYN 包因网络延迟滞留，之后客户端重新发起连接，旧 SYN 包可能在新连接建立后到达 Server(服务器)。如果采用的是两次握手，若服务器收到旧 SYN 后回复 ACK，客户端因未发送过该 SYN，会忽略或拒绝该 ACK，导致服务器建立无效连接，浪费资源。那么三次握手就能解决该问题，当客户端收到服务器基于旧 SYN 的 SYN-ACK 时，会发现序列号与当前连接不匹配，从而发送 RST 包拒绝连接，避免无效连接建立。

2.4.3　TCP 四次挥手

上面我们知道了 TCP 三次握手的机制，以及采用三次握手的好处。接下来当连接需要关闭时，TCP 采用四次挥手的方式来关闭连接，如图 2-8 所示，具体过程如下。

第一次挥手：主机 A(client)因为不再有数据发送给主机 B(server)，所以向主机 B 发送 FIN 报文表示想要关闭连接，不会再发送数据了。FIN 报文中包含主机 A 的报文序号 M。

第二次挥手：主机 B 在接收了来自主机 A 的 FIN 报文后，得知主机 A 不再发送数据，将要关闭连接。但是，此时主机 B 或许还有部分数据没有回传给主机 A，主机 B 可能还要向主机 A 发送一部分数据才能关闭连接。所以主机 B 不会立即同意关闭连接，而是先发送表示确认信息的 ACK 报文，该 ACK 报文中包含了值为 M+1 的确认号。

第三次挥手：在主机 B 完成向主机 A 传送最后的数据后，此时不再有数据需要传输了。那么主机 B 也准备关闭连接，所以向主机 A 发送表示关闭连接的 FIN 报文，报文中包含了主机 B 的序号 N。

第四次挥手：在主机 A 也收到了主机 B 发送的 FIN 报文之后，得知服务器端也可以关闭连接了，此时再向主机 B 发送最后一次确认报文 ACK，使连接成功关闭，ACK 报文中的确认号为 N+1。期间主机 A 收到 FIN 返回 ACK 应答，会进入 TIME_WAIT 状态，在等待一段时间后，将状态置为 Closed，主机 B 收到应答后，状态置为 Closed。至此，连接关闭。

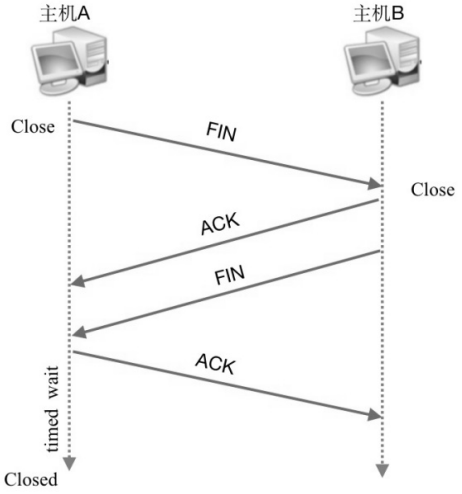

图 2-8　TCP 四次挥手

2.5 UDP 协议

UDP 是 User Datagram Protocol 的缩写。UDP 不提供复杂的控制机制，只是利用 IP 提供面向无连接的通信服务。它是在收到应用程序发来的数据的那一刻，立即按照原样发送到网络上的一种机制。即使是出现网络拥堵的情况下，UDP 也无法进行流量控制等避免网络拥塞的行为。此外，传输途中即使出现丢包，UDP 也不负责重发。甚至当出现包的到达顺序乱掉时也没有纠正的功能。UDP 有点类似于用户说什么听什么的机制，但是需要用户充分考虑好上层协议类型并制作相应的应用程序。因此，也可以说，UDP 按照“制作程序的那些用户的指示行事”。

由于 UDP 面向无连接，它可以随时发送数据，再加上 UDP 本身的处理既简单又高效，因此经常用于以下几个方面。

- 包总量较少的通信(DNS、SNMP 等)。

- 视频、音频等多媒体通信(即时通信)。
- 限定于 LAN 等特定网络中的应用通信。
- 广播和多播通信。

2.5.1 UDP 数据报格式

UDP 数据报分为首部和用户数据部分，整个 UDP 数据报作为 IP 数据报的数据部分封装在 IP 数据报中。UDP 数据报结构如表 2-5 所示。

表 2-5 UDP 数据报格式

源端口(16 位)	目的端口 16 位()
UDP 长度(16 位)	UDP 校验和(16 位)
数据(Data)	

UDP 首部有 8 字节，由 4 个字段构成，每个字段都是 2 字节。

- 源端口：源端口号，需要对方回信时选用，不需要时全部置 0。
- 目的端口：目的端口号，在终点交付报文的时候需要用到。
- 长度：UDP 的数据报的长度(包括首部和数据)，其最小值为 8(只有首部)。
- 校验和：检测 UDP 数据报在传输中是否有错，有错则丢弃。该字段是可选的，若源主机不想计算校验和，则直接令该字段全为 0。

当传输层从 IP 层收到 UDP 数据报时，根据首部中目的端口，把 UDP 数据报通过相应的端口上交给应用进程。如果接收方 UDP 发现收到的报文中的目的端口号不正确(即不存在对应于端口号的应用进程)，那么就丢弃该报文，并由 ICMP 发送“端口不可达”差错报文给对方。

2.5.2 UDP 传输过程

UDP 作为一个非连接的协议，传输数据之前源端和终端不需要建立连接，当它想传送时就简单地去抓取来自应用程序的数据，并尽可能快地把它扔到网络上，如图 2-9 所示。在发送端，UDP 传送数据的速度仅受应用程序生成数据的速度、计算机的能力和传输带宽的限制；在接收端，UDP 把每个消息段放在队列中，应用程序每次从队列中读一个消息段。

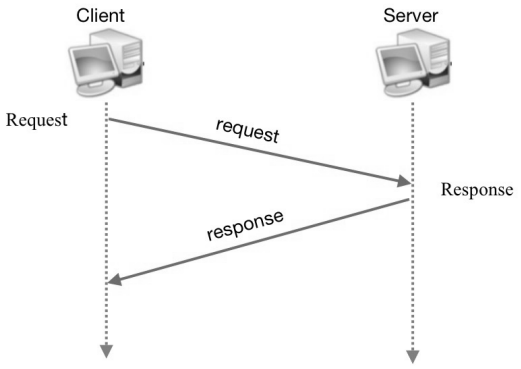

图 2-9 UDP 传输过程

由于传输数据不建立连接，因此也就不需要维护连接状态(包括收发状态等)，因此一台服务器可同时向多个客户机传输相同的消息。UDP 数据报的首部很短，只有 8 字节，相对于 TCP 的 20 字节的首部，开销很小。

UDP 的吞吐量也不受拥挤控制算法的调节，只受应用软件生成数据的速率、传输带宽、源端和终端主机性能的限制。

UDP 是面向报文的。发送方的 UDP 对应用程序交下来的报文，在添加首部后就向下交付给 IP 层，既不拆分，也不合并，而是保留这些报文的边界。因此，应用程序需要选择合适的报文大小。

我们经常使用 ping 命令来测试两台主机之间 TCP/IP 通信是否正常，其实 ping 命令的原理就是向对方主机发送 UDP 数据包，然后对方主机确认收到数据包，如果数据包到达的消息及时反馈回来，那么网络就是通的。

2.6 本章小结

本章从计算机通信数据传输过程和局域网数据传输结构出发，详细介绍了各层次结构涉及的通信协议，以及数据传输的三种模式：单播、组播、广播。通过本章的学习，读者能够对数据传输过程有基本的认识，区分不同的通信协议，了解相关协议的作用和原理。

2.7 本章习题

1. 选择题

(1) 从拓扑结构看，计算机网络是由(　　)组成的。

A. 网络节点和通信链路

B. 用户资源子网和通信子网

C. 硬件系统和网络软件系统

D. 以上答案都不对

(2) 终端间最常见的通信模式是(　　)。

A. 广播　　B. 多播　　C. 单播　　D. 任播

(3) 将 IP 地址转换为物理地址的协议是(　　)。

A. TCP　　B. ARP　　C. IP　　D. ICMP

(4) 在 TCP/IP 协议簇中，UDP 协议工作在(　　)。

A. 应用层　　B. 网络互联层　　C. 网络接口层　　D. 传输层

2. 问答题

(1) 请简要描述 ICMP 协议和 ARP 协议的作用。

(2) 请简要描述 IP 数据报首部结构。

(3) 请简要描述 TCP 三次握手和四次挥手的过程。