国家网络技术水平考试

二级学员教材

（内部试用版）

国家网络技术水平考试教材编委会

信息产业部国家信息化工程师认证考试管理中心

国家网络技术水平考试授权教材

国家网络技术水平考试
二级学员教材

（内部试用版）

国家网络技术水平考试教材编委会

信 息 产 业 部
国家信息化工程师认证考试管理中心

序

当前，我国信息化事业已经发展到一个新的阶段。经过不懈的努力，全民的信息化意识明显提高，信息网络应用日益普及，国家重大信息化系统工程取得实效。特别是党的十五届五中全会做出重要决策，将大力推进国民经济和社会信息化定为实施我国现代化建设的战略举措，极大地推动着全国信息化的进程。江泽民同志在中国共产党第十六次全国代表大会上所作的报告中也指出“信息化是我国加快实现工业化和现代化的必然选择”，要求我们“优先发展信息产业，在经济和社会领域广泛应用信息技术。”朱镕基同志主持召开的国家信息化领导小组第二次工作会议确定：推进信息化，必须坚持“统筹规划、资源共享，应用主导、面向市场，安全可靠、务求实效”的方针。同时特别强调，推进信息化必须做到基础工作先行，要加快信息化法规建设，制定国家信息技术标准体系，加强信息化知识普及和人才培养。这说明，信息化人才队伍建设不仅是当前信息化形势发展的迫切需要，而且也是保障完成今后信息化历史使命的一项基础性工作。

信息产业部国家信息化工程师认证考试(NCIE)正是为适应这一形势而启动的，在信息产业部的直接推动下，组织了由国务院信息化工作办公室、人事部、教育部、中科院、中国工程院、国家信息中心有关领导和著名院校、企业的院士、教授、专家参加的工作指导委员会。在工作指导委员会第一次会议上，决定首先实施我国自主品牌的国家网络技术水平考试(NCNE)。这是一件十分有意义的举措，在社会上引起了极大的反响。

认证考试管理中心通过引进国外先进教材和组织国内专家撰写的方式，陆续推出一系列技术领先、实用性强的网络技术认证考试教材、实验指导书和教学指导书。这些教材全面系统地介绍了教学大纲中规定的内容，既重视基本理论、基本知识的阐述，指导学生动手进行网络技术的实验，同时强调了学习的重点难点和应知应会并熟练掌握的基本技能，为学生学习和教师授课提供了详尽的指导。可以说这些教材既可作为国家网络技术水平考试的培训教材，也可作为信息化从业人员的参考手册。

我相信通过师生互动、教学相关，我们一定能培养出一大批优秀的网络技术人才。

我谨向国家信息化工程师认证考试的顺利启动表示祝贺，并希望国家信息化工程师认证考试在我国信息化人才建设工作中发挥重要的作用。

中国信息协会副会长
国家信息中心原主任 高新民

前　言

本书以 NCIE 国家网络水平考试二级教学大纲为基础，全面系统地介绍了大纲中规定的内容，为学员提供较为详尽的学习指导。

一、本书的主要内容

本书共分为两大部分，十九章节。前九章为第一部分，主要介绍了 TCP/IP 协议，DHCP 服务器配置，DNS 服务器配置，实现 Internet 信息服务，Windows 2000 路由服务，实现远程访问服务，网络故障诊断和排错，邮件服务器配置及 Windows 网络安全的知识。后十章为第二部分，主要介绍 Linux DNS 服务器，FTP 服务器，Apache 服务器配置，E-mail 服务器，Linux 路由实现，配置 DHCP 服务器，Linux 防火墙，Linux 安全，Linux 下的 VPN 及用 Webmin + SSL 管理系统的知识

二、本书的特点

本书从实际教学出发，将知识体系从易到难进行编排，本书最大的特点是通过大量实例来讲解知识点。本书中部分详细的实际操作为了教学的方便，安排在实验教材中，但并不影响对本书知识点的理解。

三、本书适用对象

本书适用于下列对象：

1. NCIE 国家网络技术水平考试二级认证教师和学员。
2. 其他网络技术培训教师和学员。
3. 大中专院校相关专业学生。
4. 系统管理员、网络管理员和广大网络技术爱好者。

本套丛书是在国家信息化工程师认证考试工作指导委员会的指导下，由国家网络技术水平考试教材编委会组织编写的。

由于编写时间仓促，本书中可能会有一些疏漏，希望广大认证教师及学员给予指正。可以发 E-mail 至：books@ncie.gov.cn。

如果您对国家网络技术水平考试的相关内容感兴趣，可以访问：

国家信息化工程师认证考试管理中心网站：http://www.ncie.gov.cn

国家网络技术水平考试教材编委会

2003 年 10 月

目　录

第 1 章　TCP/IP 协议

引言

现代生活离不开沟通，沟通离不开语言。给远方的亲人写信，书写工作总结，都需要语言的支持。网络也是一样，各种各样的服务，比如上网浏览网页，电子邮件，远程控制等，都离不开网络中的“通用语言”——TCP/IP 的支持。所以学习本章的目的就是要帮助大家深入了解 TCP/IP 协议，为学习本书的后续各章打下良好的基础。本章将分为三部分详细讲解 TCP/IP 协议：

- 协议简介；
- IP 寻址；
- TCP/IP 应用。

1.1　协议简介

1.1.1　TCP/IP 协议简介

微电子技术、计算机技术、通信技术的迅猛发展，促进了计算机网络的实现和发展。从 1969 年第一个分组交换计算机网 ARPANET 的出现，随着计算机硬件技术的飞速发展，计算机硬件价格的急骤下降，至今涌现了许多大型计算机网络。因此，如何实现不同网络及计算机间的互操作成为计算机联网的关键问题。经过近二十年的研究，到八十年代初，有了肯定的答案：这就是采用 TCP/IP 协议。在成为工业标准之前，TCP/IP 经历了近 12 年的实际测试。它最初是为了维护战争情况下通信联系和数据发送的快速实现而设计的一套 WAN 协议，在此之后，该协议的发展从政府部门传到 Internet 团体手中。而 Internet 又是 ARPNET，NFSNET，MILNET 等一组网络的集合，它用 TCP/IP 协议集来实现统一可交互操作的网络。这使得 TCP/IP 得以流行，成为事实的工业标准。

由于 TCP/IP 不是由某个公司维护和编写的，不存在像其他协议那样的兼容性问题。TCP/IP 的标准以 RFCs（Request For Comments）的形式出现并保证在 Internet 上随时公开，它详细说明了该组协议是怎样实现的。

人们为 TCP/IP 开发了许多实用程序，如文件传送协议（FTP）和终端仿真协议（Telnet）。使用这些程序的计算机之间的连接并不依赖于其上的操作系统。例如 Microsoft 的 FTP 客户可通过 Unix FTP 服务器来发送文件，而收发双方都不用担心兼容性的问题。

1.1.2　TCP/IP 协议栈的体系结构

TCP/IP 协议实际上是一组完整的网络协议。用与 OSI 同样的层次模型来描述 TCP/

IP 网络协议组，则 TCP 是提供传输层服务，而 IP 是提供网络层服务。此外，由于 TCP/IP 是一组协议的代名词，所以它还包含许多其他的协议，其层次结构图如图 1-1 所示。

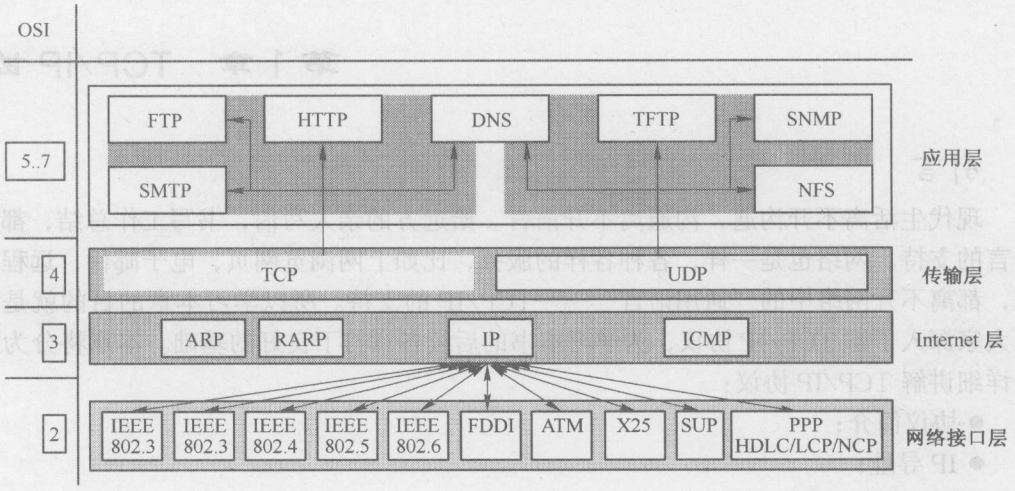

图 1-1　TCP/IP 层次结构图

其中网络接口层相当于 OSI 的第 1-2 层，表示 TCP/IP 的实现基础，如 Ethernet、Token Ring、Token Bus 等；

Internet 层负责提供基本的数据封包传送功能，让每一块数据包都能够到达目的主机（但不检查是否被正确接收），如网际协议（IP）。相当于 OSI 第 3 层，如表 1-1 所示。

表 1-1　INTERNET 层协议

协 议 名	功　能
IP	网际协议（Internet Protocol），负责主机间数据的路由和网络上数据的存储。同时为 ICMP、TCP、UDP 提供分组发送服务
ARP	地址解析协议（Address Resolution Protocol），此协议将网络地址映射到硬件地址
RARP	反向地址解析协议（Reverse Address Resolution Protocol），此协议将硬件地址映射到网络地址
ICMP	网间报文控制协议（Internet Control Message Protocol），此协议处理主机和路由器间的差错和传送控制

传输层提供了节点间的数据传送服务，如传输控制协议（TCP）、用户数据报协议（UDP）等，TCP 和 UDP 给数据包加入传输数据并把它传输到下一层中，这一层负责传送数据，并且确定数据已被送达并接收。相当于 OSI 第 4 层，如表 1-2 所示。

表 1-2　传输层的协议

协 议 名	功　能
TCP	传输控制协议（Transmission Control Protocol），这是一种提供给用户进程的可靠的全双工字节流面向连接的协议。它要为用户进程提供虚电路服务，并为数据可靠传输建立检查。大多数网络用户程序使用 TCP

续表

协 议 名	功 能
UDP	用户数据报协议（User Datagram Protocol），这是提供给用户进程的无连接协议，用于传送数据而不执行正确性检查

应用层负责应用程序间的沟通，如简单电子邮件传输协议（SMTP）、文件传输协议（FTP）、网络远程终端协议（Telnet）等。相当于 OSI 第 5－7 层，如表 1-3 所示。

表 1-3 应用层的协议

协 议 名	功 能
FTP	文件传输协议（File Transfer Protocol），允许用户以文件操作的方式（文件的增、删、改、查、传送等）与另一主机相互通信
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol），SMTP 协议为系统之间传送电子邮件
Telnet	终端协议（Telnet terminal Protocol），允许用户以虚终端方式访问远程主机。
HTTP	超文本传输协议（HyperText Transfer Protocol），是环球网 WWW 的基础，它使丰富多彩的 Internet 以文本和图形的方式展现给用户
TFTP	简单文件传输协议（Trivial File Transfer Protocol），FTP 的一种简化版本

整个 TCP/IP 协议的核心部分是传输层协议（TCP，UDP）、Internet 层协议（IP）。TCP/IP 协议建立了对网络的 TCP/IP 模型，与 OSI 的七层参考模型相比，TCP/IP 模型更简练和实用。传统的开放系统互连参考模型（OSI），是一种通信协议的 7 层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是便于分析和设计网络的各层面的功能。

1.2 TCP 与 UDP

了解了整体的 TCP/IP 模型后，我们重点来看 TCP 与 UDP 两个传输层协议。它们都可提供节点间的数据传送服务，TCP 是面向连接的协议，稳定性好；UDP 是无连接的协议，速度快。两者各有优缺点，具体的采用与选择由上层应用程序决定。

1.2.1 TCP——面向连接的协议

TCP 是面向连接的协议，可以提供可靠的数据传输。TCP 协议在数据传输过程中以组为单位发送数据包，而且还负责为数据包指定序列号，并为源计算机应用程序和目标计算机应用程序添加端口信息。

TCP 协议将数据包发送到网上并等待对方的确认信息，若在一定时间内没有收到对方的确认信息，则重发数据包。所以说 TCP 协议是面向连接的可提供可靠数据传输的协议。

TCP协议是通过三次握手（Tree-Way Handshake）来保证数据传输的可靠性。如图1-2所示，三次握手即：

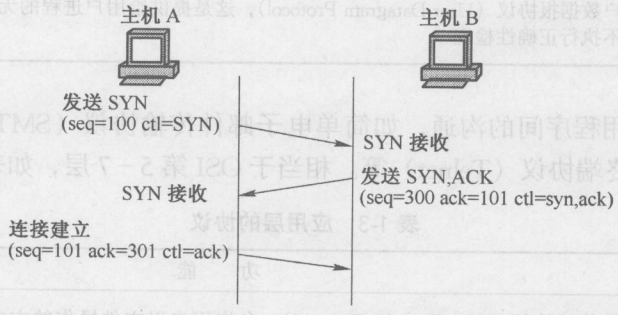

图 1-2　TCP 三次握手

1. 主机 A 选择一个序号 X 向主机 B 发出包含了该序号的请求；

2. 主机 B 回应主机 A 的请求，确认 X 并申明自己使用的序号 Y；

3. 主机 A 在其发送的第一个数据包中确认主机 B 使用的序号。

采用三次握手，源计算机与目的计算机之间的通信一般完成以下的三个过程：

1. 源计算机向目标计算机发出连接请求，协商建立连接和相互通信的规则；目标计算机响应源计算机的连接请求，如果协商成功，完成建立连接。

2. 源计算机根据双方协商的滑动窗口大小，向目标计算机发送数据包，即数据包大小由该窗口决定，目标计算机按顺序接收，并一一响应，确认是否正确接收了每一个数据包，如果出现错误或者丢失，则要求源计算机立即重传。

3. 数据传输完成，源计算机请求拆除连接，目标计算机响应，拆除连接。

1.2.2　UDP——无连接的协议

UDP 是一种无连接的协议，即不需要与目标主机进行连接确认，就会将数据包发送出去。所以 UDP 协议数据传输不如 TCP 可靠，但同时因为传输数据之前不需要连接，UDP 协议在传输大量小块数据时的速度明显要比 TCP 快，而且可进行多路广播。可以用于传输不重要的数据。

1.2.3　端口号

如果一台计算机只有一个 IP 地址，但同时开启多项服务或运行多个应用程序的时候，就需要对每个应用程序或服务进行单独标识。无论应用程序是选择 TCP 还是选择 UDP，这两种协议都会为每个应用程序产生的数据包打上端口号，用来标识数据包的所有者。

TCP/UDP 的端口号在 0～65535 之间，其中 1024 以下的端口已保留给常用的服务器端应用程序。

所以一个 IP 地址加一个端口号才能明确的表示出是哪一台计算机的哪个应用程序发出的数据。这样的一个 IP 地址加上一个 TCP 或 UDP 端口就称之为一个 Socket（套接

字），用来唯一识别一台计算机上的一个应用程序。

1.3 IP 地址

不论上层应用程序是选择 TCP 还是 UDP 作为其传输协议，都需要将 IP 地址信息打在数据包上，这样数据包才能被正确发送到目的地。这部分主要讲解 IP 寻址的工作原理和如何利用 IP 地址划分子网。

1.3.1 IP 地址的分类及寻址规则

IP 地址回顾

Internet 其实是一个典型的 TCP/IP 网络，而 TCP/IP 网上的设备或主机（也称为节点）都分配有一个唯一的地址，叫做 IP 地址。IP 地址属于三层逻辑地址，用来标识 TCP/IP 网络中的每一台设备。IP 地址采用分层结构，32 位，共 4 个 8 位组，采用网络位+主机位的形式，如 172.16.12.1。

IP 地址的分类

Internet 上的 IP 地址分配机构为了便于分配，最开始将全世界的 IP 地址划分为几大类。如表 1-4 所示。

表 1-4 IP 地址分类

地址类型	引导位	网络位地址范围	地址结构	主机位可用地址数
A类	0	1-126（127 保留）	网+主+主+主	16777214（2^{24}-2）
B类	10	128-191	网+网+主+主	65534（2^{16}-2）
C类	110	192-223	网+网+网+主	254（2^{8}-2）
D类	1110	224-239	组播地址	
E类	1111	240-	研究用地址	

注意：127.X.X.X 用于本地回送测试，不分配给任何一台主机。

IP 网络地址由 ICANN（The Internet Corporation for Assigned Names and Numbers）统一分配，以保证 IP 地址的唯一性。ICANN 根据组织的需求为其分配 A、B、C 类网络地址，具体主机的 IP 地址由得到某一网络地址的机构或组织自行决定如何分配。

而有一些用于企业内部网的 IP 地址分配，不会被任何 Internet 上的路由器转发，这类地址称为私有地址（Private address）。

私有地址包括：

10.0.0.0－10.255.255.255　　1 个 A 类地址

172.16.0.0－172.31.255.255　　16 个 B 类地址