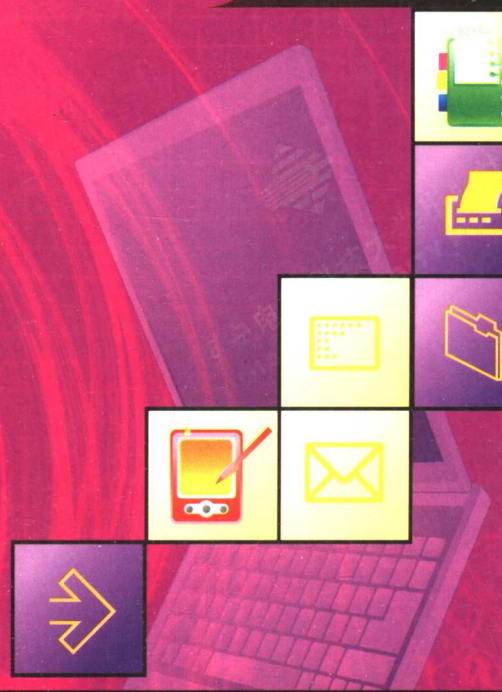
全国计算机技术与软件专业技术资格（水平）考试辅导用书

- 浓缩历年考试精华
- 命题专家权威解答
- 挖掘考试命题方略
- 真实检阅备考成效



网络管理员考试
历年试题分析与解答

计算机技术与软件专业技术资格（水平）考试研究组　编

2006

西安电子科技大学出版社
http://www.xduph.com

全国计算机技术与软件专业技术资格(水平)考试辅导用书

网络管理员考试历年试题分析与解答

计算机技术与软件专业技术资格(水平)考试研究组　编

西安电子科技大学出版社

内 容 简 介

本书收集了2002～2005年计算机技术与软件专业技术资格(水平)考试网络管理员考试(原网络程序员级)的全部试题，并给出了详尽的分析与解答。本书有助于准备参加计算机技术与软件专业技术资格(水平)考试的应试者复习有关内容，了解试题形式，提高应试能力。相信本书对于准备参加其他类似考试的读者，或者打算快速了解或复习有关计算机及其应用知识的读者都会有所帮助。

本书既可作为参加网络管理员级计算机技术与软件专业技术资格(水平)考试的考生备考的参考书，也可供大专院校师生和计算机爱好者学习参考。

图书在版编目(CIP)数据

网络管理员考试历年试题分析与解答/计算机技术与软件专业技术资格(水平)考试研究组编.
—西安：西安电子科技大学出版社，2005.9
全国计算机技术与软件专业技术资格(水平)考试辅导用书
ISBN 7-5606-1574-0
Ⅰ.网… Ⅱ.计… Ⅲ.计算机网络-工程技术人员-资格考核-解题 Ⅳ.TP393-44

中国版本图书馆CIP数据核字(2005)第109960号

策　　划　臧延新
责任编辑　杨宗周　臧延新
出版发行　西安电子科技大学出版社(西安市太白南路2号)
电　　话　(029)88242885　88201467　　邮　编　710071
http://www.xduph.com　E-mail:xdupfxb@pub.xaonline.com
经　　销　新华书店
印刷单位　陕西华沐印刷科技有限责任公司
版　　次　2005年9月第1版　2006年3月第2次印刷
开　　本　787毫米×1092毫米　1/16　印张　13.125
字　　数　310千字
印　　数　4001～10 000册
定　　价　20.00元
ISBN 7-5606-1574-0/TP·0901

XDUP 1865011-2

前　言

计算机技术与软件专业技术资格(水平)考试自1985年开考以来，经历了由多省市共同举行联合考试等过程，目前已发展成由国家人事部、信息产业部等部门领导下的国家级考试。国家级考试结果同获得专业技术职称相联系，使得考试更科学更合理，也更具有权威性和吸引力。这对提高我国计算机软件人员的技术水平，鼓励和激发计算机专业工作人员、在校学生钻研业务，提高全民的计算机应用水平都有很大的促进作用。

本书收集了2002～2005年计算机技术与软件专业技术资格(水平)考试网络管理员考试的全部试题，并给出了详尽的分析与解答。其目的是讲解或帮助读者复习有关的知识，希望本书有助于准备参加计算机技术与软件专业技术资格(水平)考试的应试者复习有关内容，了解试题形式，提高应试能力。同时，相信本书对于准备参加其他类似考试的读者或者打算快速了解或复习有关计算机及其应用知识的读者都有帮助。本书有如下特点：

1. 收集了这段时期的全部试题，而不是选编。

2. 每道试题都先对解题思路及方法给出详尽的分析，然后再给出正确的解答。

全书按考试年度分章，每章编排结构分为上午试题、上午试题解析、下午试题和下午试题解析。

作者在本书的编写过程中，参考了许多相关的书籍和资料，在此对这些参考文献的作者表示感谢。同时也非常感谢西安电子科技大学出版社在本书出版过程中所给予的大力支持和帮助。

尽管参加本书编写的人员是具有多年从事科研和教学工作的计算机专业领域的专业技术人员和学者，但是，书中难免会存在一些错漏和不妥之处，望读者指正，以利改进和提高。

编　者

2006年2月

目　　录

第 1 章　2002 年试题解析

1.1　2002 年上午试题

● 相对于 ISO/OSI 的 7 层参考模型的低 4 层，TCP/IP 协议集内对应的层次有 (1)，它的传输层协议 TCP 提供 (2) 数据流传送，UDP 提供 (3) 数据流传送，它的互联网层协议 IP 提供 (4) 分组传输服务；IEEE802 参考模型仿照了 ISO 的 OSI/RM，它的 (5) 对应于 OSI/RM 的数据链路层，两者的物理层相互对应。

(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. 面向连接的、不保证服务质量的
　　D. 无连接的、不保证服务质量的

(5) A. AAL 和 ATM　　B. LLC 和 MAC
　　C. CS 和 SAR　　D. TC 和 PMD

● 4B/5B 编码是将数字数据变换为数字信号的编码方法，其原理是用 (6) 位编码表示 (7) 位数据。该编码是 (8) 采用的编码方法，编码效率是 (9)，相对于曼彻斯特编码，效率提高了 (10)。

(6) A. 4　　B. 5　　C. 8　　D. 10

(7) A. 4　　B. 5　　C. 8　　D. 10

(8) A. 10 Mb/s 以太网　　B. 100BASE - T4 以太网
　　C. 1000 Mb/s 以太网　　D. FDDI(100BASE - FX)

(9) A. 50%　　B. 60%　　C. 75%　　D. 80%

(10) A. 30%　　B. 50%　　C. 60%　　D. 80%

● 在数字传输系统中传输的是 (11)，它所代表的原始数据是 (12)。对基于铜线的该种传输系统影响最大的噪声是 (13)，在这种传输系统中受延迟影响最大的是 (14)。在有线数字传输系统中，信号衰减的强度 p(分贝值)与传输距离 d 有关，可

以用于描述二者之间关系的是 (15) (其中 k 为某种常系数)。

(11) A. 数字数据 B. 模拟数据 C. 数字信号 D. 模拟信号

(12) A. 数字数据 B. 模拟数据
C. 数字数据或模拟数据 D. 混合的数字数据和模拟数据

(13) A. 热噪声 B. 脉冲噪声 C. 调制噪声 D. 串扰噪声

(14) A. 低速模拟信号 B. 低速数字信号
C. 高速模拟信号 D. 高速数字信号

(15) A. p=kd B. p=kd2 C. p=k D. 没有简单的公式

● 路由器是一种常用的网络互连设备，它工作在 OSI/RM 的 (16) 上，在网络中它能够根据网络通信的情况 (17) ，并识别 (18) 。相互分离的网络经路由器互连后 (19) 。通常并不是所有的协议都能够通过路由器，如 (20) 在网络中就不能被路由。

(16) A. 物理层 B. 数据链路层
C. 网络层 D. 传输层

(17) 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

(18) 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

(19) 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

(20) A. NetBEUI B. Apple Talk C. IPX D. IP

● 防火墙技术可以分为 (21) 等三大类型，防火墙系统通常由 (22) 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 (23) 网络内部的安全措施，也 (24) 进入防火墙的数据带来的安全问题。它是一种 (25) 网络安全措施。

(21) A. 包过滤、入侵检测和数据加密 B. 包过滤、入侵检测和应用代理
C. IP 过滤、线路过滤和入侵检测 D. IP 过滤、线路过滤和应用代理

(22) 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

(23) A. 可以替代 B. 不能替代 C. 是一种 D. 是外部和

(24) A. 物理隔离 B. 能够区分 C. 不能解决 D. 可以解决

(25) A. 被动的 B. 主动的
C. 能够防止内部犯罪的 D. 能够解决所有问题的

● PPP 是 Internet 中使用的 (26) ，其功能对应于 OSI 参考模型的 (27) ，以 (28) 协议为基础。PPP 使用面向 (29) 的填充方式，其理由之一是因为 (30) 。

(26) A. 串行 IP 协议 B. 分组控制协议 C. 点到点协议 D. 报文控制协议

(27) A. 数据链路层 B. 网络层 C. 传输层 D. 应用层

(28) A. TCP/IP B. NetBEUI C. SLIP D. HDLC

(29) A. 位 B. 字符 C. 透明传输 D. 帧

(30) A. 它的基础协议使用的是字符填充方式　　B. 它是以硬件形式实现的
　　C. 它是以软件实现的　　D. 这种填充效率高、灵活多样

● 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 (31) 或者 (32) 。

快速以太网仍然遵循 CSMA/CD，它采取 (33) 而将最大电缆长度减少到 100 m 的方式，使以太网的数据传输率提高到 100 Mb/s。为了支持不同的传输介质，快速以太网提供了三种技术标准，即 100BASE - T4、100BASE - TX 和 100BASE - FX，其中 100BASE - T4 使用 (34) ，100BASE - TX 使用 (35) 。

(31) 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

(32) 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

(33) 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

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

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

● IP 地址由 32 个二进制位构成，其组成结构为 IP 地址 = 网络地址 + 主机地址。分为五类(A 类至 E 类)，其中提供作为组播(Multicast)地址的是 (36) 。

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 (37) ；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 地址的共有 (38) 个。

采取子网划分后，IP 地址的组成结构为 (39) ，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，减少的地址数目为 (40) 。

(36) A. A 类地址　　B. C 类地址　　C. D 类地址　　D. E 类地址

(37) A. 127　　B. 126　　C. 255　　D. 128

(38) A. 16 384×65 536　　B. 16 384×65 534　　C. 16 382×65 534　　D. 16 382×65 536

(39) A. IP 地址 = 网络地址 + 子网地址 + 主机地址
　　B. IP 地址 = 网络地址 + 子网络接口地址 + 主机地址
　　C. IP 地址 = 网络地址 + 主机地址 + 子网络接口地址
　　D. IP 地址 = 网络地址 + 主机地址 + 子网地址

(40) A. 6　　B. 8　　C. 62　　D. 130

● Windows 系列操作系统在配置网络时应该遵循的基本顺序为 (41) ，安装了该类操作系统主机之间的资源共享与访问不能通过 (42) 协议实现。主机 A、B 安装了 Windows 98，A 可访问 B 的共享资源，而 B 不能访问 A，可能是由于 (43) 。

在配置 Windows 的 TCP/IP 协议时，如果希望该主机自动获得 IP 地址，或者将局域网中的主机名直接映射为 TCP/IP 协议中的域名，则所需要的服务分别为 (44) 。

通常情况下，Windows 网络系统的资源共享只能在局域网内部实现，但是有些情况下，用户可以在 Internet Explorer 浏览器的地址栏中输入“//ip_address”，实现对 IP 地址为“ip_address”主机的跨网段访问，防止这种不安全因素出现的最优方法为 (45) 。

(41) A. 网络适配器 → 网络协议 → 网络服务
B. 网络适配器 → 网络服务 → 网络协议
C. 网络服务 → 网络适配器 → 网络协议
D. 网络协议 → 网络适配器 → 网络服务

(42) A. TCP/IP　　B. IPX/SPX
C. NetBEUI　　D. DLC

(43) A. A 与 B 都安装了 NetBEUI 协议，但都没有安装“网络文件与打印共享”服务
B. A 与 B 都只安装了 TCP/IP 协议，但都没有安装“网络文件与打印共享”服务
C. A 只安装了 TCP/IP 协议，没有安装“网络文件与打印共享”服务；而 B 安装了 NetBEUI 协议，同时还安装了“网络文件与打印共享”服务
D. A 与 B 都只安装了 TCP/IP 协议，只有 B 安装了“网络文件与打印共享”服务

(44) A. BOOTP 与 DNS　　B. DHCP 与 WINS
C. DHCP 与 DNS　　D. BOOTP 与 WINS

(45) A. 在连接两个局域网的路由器上，禁止使用或中转 NetBEUI 协议
B. 在该主机 TCP/IP 协议属性配置中，终止“Microsoft 网络上的文件与打印机共享”服务与 TCP/IP 协议的绑定关系
C. 禁止该主机提供“网络文件与打印共享”服务
D. 禁止该主机使用 TCP/IP 协议

● 一台 PC 服务器，安装 Linux 并配置 DNS 服务，对服务器的测试与检查如下：

① 通过 (46) 命令测试 DNS，发现 DNS 工作正常；

② 检查文件 (47) ，发现内容为“order hosts”；

③ 检查本机的 DNS 解析配置文件 (48) ，发现内容为“domain pku. edu. cn nameserver 166. 111. 103. 1 nameserver 166. 111. 103. 2 search ”；

④ 检查 DNS 服务的配置文件，文件内容中有“ zone pku. edu. cn { type slave; file db. pku. edu. cn; master in (“202. 114. 102. 1”); }”，则表明该 DNS 服务器进程工作于 (49) 状态。

如果在该服务器上运行“ping ftp. pku. edu. cn”可以获得应答，而运行“ping ftp”无法获得目标主机的应答，(50) 是导致该现象的最直接原因。

(46) A. resolv　　B. ping
C. nslookup　　D. testdns

(47) A. /etc/resolv. conf　　B. /etc/host. conf
C. /etc/linux. conf　　D. /etc/sys. conf

(48) A. /etc/resolv. conf　　B. /etc/named. conf
C. /etc/dns. conf　　D. /var/named

(49) A. 解析服务器　　B. 缓冲服务器
C. 主域名服务器　　D. 备份域名服务器

(50) A. 本服务器指定了主域名服务器 166.111.102.1 作为自身的域名解析服务器，自身的 DNS 服务仅作为备份域名服务器，而主域名服务器中仅配置了 ftp.pku.edu.cn 的解析，没有配置“ftp”的解析

B. 在域名解析配置文件中，由于“search”后没有指定默认的域名搜索范围，故本机不能将“ftp”等同于“ftp.pku.edu.cn”

C. 本机对“ftp.pku.edu.cn”解析通过主域名服务器 166.111.102.1 完成，对“ftp”的解析由于在本域内，通过自身的域名解析进程完成，由于本机的 DNS 没有配置“ftp”，所以无法解析

D. 该服务器自身对域名的解析不是通过 DNS 完成的，而其他途径没有对“ftp”进行解析

● 磁盘服务器是基于盘体共享技术，并向网络提供共享的磁盘资源，它的效率由多种因素来决定，其中 (51) 是主要因素之一。

文件服务器是建立在磁盘服务器基础上，但与磁盘服务器有着本质区别。用户对磁盘服务器的读写是按 (52) 来读写，与 (53) 无关。而文件服务器可以根据 (54) 来确定从磁盘读出的信息量。设计文件服务器最基本的一个问题就是接口，它的作用是 (55) 。所以文件服务器不直接和用户接口，而是在文件服务器上建立一些更有用的功能，如文件系统、数据库服务器等，用户再和这些系统直接接口。

(51) A. 网络操作系统　　B. 网上数据传输速率
　　C. 用户应用程序　　D. 用户机上的操作系统

(52) A. 数据块　　B. 文件　　C. 目录　　D. 字节

(53) A. 读写速度　　B. 磁盘容量　　C. 数据结构　　D. 内存地址

(54) A. 目录大小　　B. 文件数量　　C. 目录数量　　D. 文件大小

(55) A. 将用户认识的文件符号名映像到服务器认识的文件标识号

B. 将用户不认识的文件符号名映像到服务器认识的文件标识号

C. 将服务器认识的文件标识号映像到用户认识的文件符号名

D. 将服务器不认识的文件标识号映像到用户认识的文件符号名

● 结构化布线系统中，所有的水平布线 UTP(非屏蔽双绞线)都是从工作区到各楼层配线间的。在工作区由 (56) 端接，在配线间由 (57) 端接。当布线结构需要调整时，可以通过布线配线系统来重新配置，具体调整手段是通过 (58) 实现。

结构化布线工程中常采用 4 对 UTP，它使用 (59) 等四种颜色标识，其对应的 I/O 信息模块有两种标准，即 T568A 和 T568B，它们之间的差别只是 (60) 。

(56) A. RJ45 接插头　　B. I/O 信息插座模块
　　C. 快接式跳线　　D. 网卡

(57) A. 配线架　　B. 接插件
　　C. 干线子系统　　D. 集线器或交换机

(58) A. 专用工具　　B. 连接块
　　C. 跳线　　D. 控制器

(59) A. 橙、蓝、紫、绿　　B. 紫、黑、蓝、绿
　　C. 黑、蓝、棕、橙　　D. 橙、绿、蓝、棕

(60) A. "1、2"对线与"3、6"对线位置交换
B. "4、5"对线与"7、8"对线位置交换
C. "1、2"对线与"4、5"对线位置交换
D. "3、6"对线与"7、8"对线位置交换

● 客户机/服务器(Client/Server)模式产生于20世纪 (61) 年代，它是基于 (62) 的要求而发展起来的。客户机/服务器模式的第一个软件产品是 (63) 系统，客户机/服务器模式通常在 (64) 环境下运行，客户端的软件具有 (65) 。

(61) A. 60 B. 70 C. 80 D. 90
(62) A. 操作系统 B. 网络通信 C. 计算机硬件 D. 数据库系统
(63) A. Sybase B. Informix C. SQL Server D. DB2
(64) A. 以大型机为中心的分时系统 B. 以服务器为中心的网络系统
C. 对等网络 D. 智能网络
(65) A. 专用性 B. 通用性
C. 浏览易操作性 D. 快速搜索特性

● In the following essay, each blank has four choices. Choose the most suitable one from the four choices and write down in the answer sheet.

Heterogeneous network environments consist of computer systems from (66) vendors that run (67) operating systems and communication protocols. An organization that (68) its computer resources is usually (69) the task of integrating its heterogeneous systems. Typically, each department or division has defined its own network needs (70) OS, LAN topology, communication protocols, applications, and other components.

(66) A. same B. similar C. different D. difference
(67) A. same B. similar C. different D. difference
(68) A. consolidates B. consists C. considerate D. consoles
(69) A. faced on B. faced with C. faced about D. faced up to
(70) A. in general B. in any term C. in set terms D. in terms of

● In the following essay, each blank has four choices. Choose the most suitable one from the four choices and write down in the answer sheet.

There are two types of key technology: private key and public key. Private-key encryption methods are called (71) ciphers, information is encrypted with (72) both the sender and receiver hold privately. Public-key encryption methods are called (73) ciphers, (74) created for each user, encryption key and decryption key are (75) .

(71) A. synchronous B. asynchronous
C. symmetric D. asymmetric
(72) A. a key B. two keys
C. three keys D. four keys

(73) A. synchronous　　B. asynchronous
　　C. symmetric　　D. asymmetric
(74) A. two related keys are　　B. a key is
　　C. two unrelated keys are　　D. three keys are
(75) A. same　　B. different　　C. difference　　D. some

1.2　2002 年上午试题解析

试题(1)～(5)解析：

本题主要测试 ISO/OSI 的参考模型、TCP/IP 协议集、TCP/IP 分层模型的概念和它们之间的关系，以及 ISO/OSI 的参考模型与 IEEE 802 参考模型之间的关系。

国际标准组织(ISO)为使网络协议系统的设计实现标准化而建立的开放系统互连模型(OSI)分为 7 层，由低层到高层依次为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，但在实际应用中，每一个协议的分层模型与 ISO/OSI 的参考模型不太相同。TCP/IP 是 Internet 采用的协议，也是全世界采用最广泛的工业标准。它是一个协议系列，目前已包含了 100 多个协议，用来将各种计算机和数据通信设备组成实际的计算机网络。ISO/OSI 的参考模型、TCP/IP 协议集和 TCP/IP 分层模型之间的对应关系如图 1－1 所示。

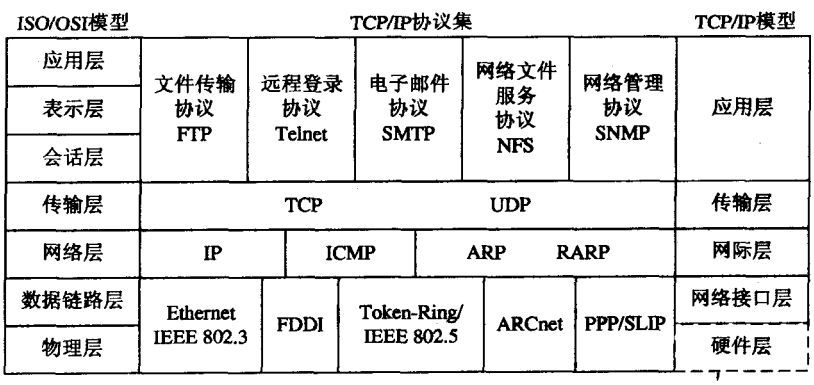


图 1－1　各模型之间的对应关系

TCP/IP 分层模型由 4 个层次构成，即应用层、传输层、网际层和网络接口层，其各层的功能简述如下：

(1) 应用层。应用层处在分层模型的最高层，用户调用应用程序来访问 TCP/IP 互联网络，以享受网络上提供的各种服务。应用层的协议有 NFS、Telnet、SMTP、DNS、SNMP、FTP 等，应用程序负责发送和接收数据。每个应用程序可以选择所需要的传输服务类型把数据按照传输层的要求组织好，再向下层传送，传送时可选择需要的传送类型，或者是数据报，或者是字节流。

(2) 传输层。传输层的基本任务是提供应用程序之间的通信服务。这种通信又叫端到端的通信。传输层既要系统地管理数据信息的流动，还要提供可靠的传输服务，以确保数据准确而有序地到达目的地。为了这个目的，传输层协议软件需要进行协商，让接收方回

送确认信息及让发送方重发丢失的分组。在传输层与网际层之间传递的对象是传输层分组。传输层分组分为两种协议：TCP 协议和 UDP 协议。

TCP 的特性有：面向数据流的处理方式，即 TCP 采用连续方式对数据进行处理，以每次接收一个字节的方式来接收数据，而不是按预先格式化的数据块的方式来接收；完全的可靠性，即 TCP 通过面向连接的传输方式，以及一些差错控制、流量控制的手段，确保了数据不会丢失，同时 TCP 还能对接收到的 IP 数据报进行重新排序，解决了数据乱序的问题；全双工通信，即 TCP 连接允许数据在任何一个方向流动，并允许任何一个应用程序在任何时刻发送数据；流量控制，即 TCP 的流量控制特性确保数据传输的速度不会超过或低于目的计算机接收数据的能力。

与 TCP 相比较，UDP 是一种不可靠的、无连接的协议，它的错误检测功能要弱得多。可以这样说，TCP 有助于提供可靠性，而 UDP 则有助于提高传输的高速率性。例如，必须支持交互式会话的应用程序(如 FTP 等)往往使用 TCP 协议；而自己进行错误检测或不需要错误检测的应用程序(如 DNS，SNMP 等)则往往使用 UDP。

(3) 网际层。网际层又称 IP 层，主要处理机器之间的通信问题。它接收传输层的请求，传送某个具有目的地址信息的分组。IP 所提供的服务通常被认为是无连接的和不可靠的(不保证服务质量)。事实上，在网络性能良好的情况下，IP 传送的数据能够完好无损地到达目的地。至于不可靠的服务是指目的系统不对成功接收的分组进行确认，IP 只是尽可能地使数据传输成功。但是只要需要，上层协议必须实现用于保证分组成功提供的附加服务。

(4) 网络接口层。网络接口层又称数据链路层，处于 TCP/IP 协议层之下，负责接收 IP 数据包，并把数据包通过选定的网络发送出去。网络接口层包含设备驱动程序，该层也可能是一个复杂的使用自己的数据链路协议的子系统。

在 IEEE 802 局域网(LAN)标准中，只定义了物理层和数据链路层两层，并根据 LAN 的特点，把数据链路层分成逻辑链路控制(LLC，Logical Link Control)子层和介质访问控制(MAC，Medium Access Control)子层；还加强了数据链路层的功能，把网络层中的寻址、排序、流控和差错控制等功能放在 LLC 子层来实现。图 1－2 为 LAN 协议的层次与 OSI/RM 参考模型的对应关系。

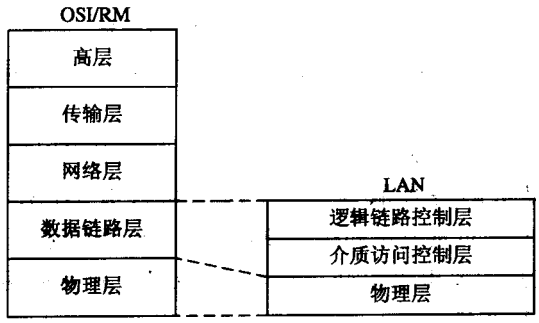


图 1－2 LAN 协议的层次与 OSI/RM 参考模型的对应关系

解答：(1) B (2) C (3) A (4) D (5) B

试题(6)～(10)解析：

本题主要测试 FDDI 采用 4B/5B 编码的原理、效率以及该编码与曼彻斯特编码的比较。

光纤中传送的是光信号，有光脉冲表示 1，无光脉冲表示 0。这种简单编码的缺点是没有同步功能。在同轴电缆或双绞线作为传输介质的局域网中，通常采用曼彻斯特编码方式。它利用中间的跳变作为同步信号。这样对每一位数据单元产生两次瞬变，使带宽的利用率降低。例如，200 MHz 的元器件只能得到 100 Mb/s 的数据传输速率，这对高速的 FDDI 来说，效率太低了。

FDDI 采用一种新的编码技术，称为 4B/5B 编码，如表 1.1 所示。在这种技术中，每次对 4 位数据进行编码。每 4 位数据编码成 5 位符号，用光信号的存在或不存在来代表 5 位符号中的每一位是 1 还是 0。也就是说使用 5 位编码表示 4 位数据，这种编码技术使效率提高 80%。100 Mb/s 的数据传输速率只需 125 MHz 的元器件就可完成。

表 1.1　4B/5B 编码技术

十六进制数	4 位二进制数	4B/5B 编码
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111
8	1000	10010
9	1001	10011
10	1010	10110
11	1011	10111
12	1100	11010
13	1101	11011
14	1110	11100
15	1111	11101

5 比特编码的 32 种组合中，实际只使用了 24 种，其中的 16 种用作数据符号，其余 8 种用作控制符号(如帧的起始和结束符号等)。上表列出 4B/5B 编码的数据符号部分，所有 16 个 4 位数据符号，经编码后的 5 位码中“1”码至少为 2 位，按 NRZI 编码原理，信号中就至少有两次跳变，因此接收端可得到足够的同步信息。

IEEE 802.3 标准中使用的曼彻斯特编码只有 50%的效率，因为每一比特都要求线路上有两次状态变化(即 2 Baud)。如果采用曼彻斯特码，那么 100 Mb/s 传输速率就要求 200M Baud 的调制速率，也即 200 MHz。换言之，曼彻斯特编码需要发送数据的 2 倍带宽。所以 4B/5B 编码相对于曼彻斯特编码，效率提高了 30%。

解答：(6) B (7) A (8) D (9) D (10) C

试题(11)～(15)解析：

本题主要测试数字传输系统的特点、性能。

模拟数据和数字数据都可以用模拟信号或数字信号来表示和传输。在一定条件下，可以将模拟信号转变为数字信号，或将数字信号转变为模拟信号。模拟信号是连续变化的电磁波，显然模拟信号的取值可以有无限多个，是某些物理量的测量结果，这种信号可以以不同的频率在各种介质上传输。数字信号是一系列的电脉冲，像计算机的输出，数字仪表的测量结果等。它可用恒定的正电压和负电压直接表示二进制的“1”和“0”。这种电脉冲可以按照不同的位速率在有线介质上传输。

数据通过介质传送时必须转换为一定形式的信号(模拟信号或数字信号)，因此通信归结到底是在一定的传输介质上传送电信号，从而实现传送数据，达到交换信息的目的。数据传输是指用电信号把数据从发送端传送到接收端的过程。数据传输分为模拟传输和数字传输两种形式。

传输信道为数据信号从发送端传送到接收端提供了物理通路。传输信道可以是同轴电缆、光纤、双绞线等有线线路，也可以是卫星和地面微波站等构成的无线线路。

数字数据通常直接用两种电平来表示，即用二进制形式的数字脉冲信号来表示。但为改变其传播特性，常常对二进制数据进行编码。数字数据也可以用模拟信号表示，但此时要利用调制解调器(Modem)进行信号的转换。在线路的发送端，通过一个载波信号把一串二进制电压脉冲转换为模拟信号，所产生的信号占有以该载波频率为中心的某一频谱，并且能在适合于此种载波的媒体上传播。大多数通用的调制解调器都用语音频谱来表示数字数据，因此能使数字数据在普通的音频电话上传播。在线路的另一端，调制解调器再把模拟信号还原，解调成原来的数字信号。

模拟信号和数字信号都可以在合适的传输媒体上进行传播，但二者之间还是有差别的。模拟传输是在线路上直接传输模拟信号的方式。模拟信号传送一定距离后，由于信号的幅度衰减而失真。为了实现长距离传输，需在沿途加若干放大器将信号放大。但放大信号的同时也放大了噪声。同样引起误差，且这种误差是沿途累加的，那么信号就会越来越畸形(失真)。尽管如此，对于模拟数据，例如声音，即使有多位变形，仍然能够听清和理解。但是，对于数字数据，这种误差将会使数据传输产生错误，有时会导致传输的信息无法使用。对于基于铜线的数字传输系统，影响最大的噪声是脉冲噪声，受延迟最大的是高速数字信号。

数字传输是在线路上用数字信号进行传输的方式。这种方式可以直接传输二进制数据

或编码的二进制数据，也可以传输数字化了的模拟数据，如数字化的图像等。数字传输中也会由于信号幅度衰减而危及数据的完整性，因此，数字信号只能在一个有限距离内传输。为了获得更大的传输距离，可以使用中继器。中继器接收衰减了的数字信号，把数字信号恢复为 1 和 0 的标准电平，然后重新传输这些新的信号。这样就有效地克服了衰减。中继器比较简单，它的引入不会产生积累误差，这也是现代通信趋向采用数字传输方式来传输模拟数据的原因。无论在价格方面还是在质量方面，数字传输都比模拟传输优越，数字传输是今后数据通信的发展方向。

双绞线是综合布线工程中最常用的一种传输介质。双绞线由两根具有绝缘保护层的铜导线组成。把两根绝缘的铜导线按一定密度互相绞在一起，可降低信号干扰的程度，每一根导线在传输中辐射的电波会被另一根线上发出的电波抵消。双绞线性能指标之一便是衰减(Attenuation)，衰减是沿链路的信号损失度量。衰减 p 与线缆的长度 d 有关系，随着长度的增加，信号衰减也随之增加，即 p=kd(k 为某种常系数)。

解答：(11) C　(12) C　(13) B　(14) D　(15) A

试题(16)～(20)解析：

本题主要测试路由器的作用、支持的协议以及工作的层次。

路由器(Router)是一种常用的网络设备，它在网络互连中主要有两种用途，一种是几个路由器将近距离(如校园内)的几个局域网互连，现在这种用途已被局域网交换机所取代；另一种是一个局域网通过路由器接入广域网，实现大范围、远距离的网络互连。路由器工作在 OSI 参考模型的网络层，在网络层协议上实现多个网络之间的互连。基于路由器的网络互连模型如图 1－3 所示。

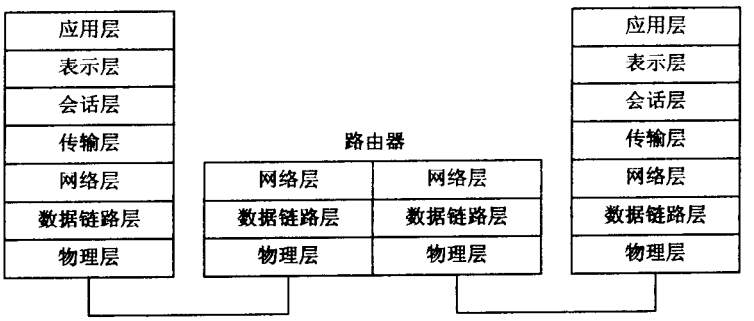


图 1－3　路由器协议层与 OSI RM 的对应关系

路由器具有很强的异种网互连能力，互连的网络最低两层协议可以互不相同，通过驱动软件接口到第三层上而得到统一。对于互连网络的第三层协议，如果相同，可使用单协议路由器进行互连；如果不同，则应使用多协议路由器。多协议路由器同时支持多种不同的网络层协议，并可以设置为允许或禁止某些特定的协议。所谓支持多种协议是指该路由器能对多种协议的数据包进行转发，当然其前提是这些协议必须具有路由信息，且路由器支持该协议。例如，在 Windows NT 网络上，Windows NT 提供的 RIP for IP Router 便是一种多协议的路由器，它可对 TCP/IP 和 IPX/SPX 包进行转发。尽管 Windows NT 也支持 NetBEUI 协议，但由于 NetBEUI 协议不含路由信息，因此，NetBEUI 数据包是不可路由的。

通常把网络层地址信息叫做网络逻辑地址，把数据链路层地址信息叫做物理地址。路由器最主要的功能是选择路径。在路由器的存储器中维护着一个路径表，记录各个网络的逻辑地址，用于识别其他网络。在互连网络中，当路由器收到从一个网络向另一个网络发送的信息包时，将丢弃信息包的外层，解读信息包中的数据，获得目的网络的逻辑地址，使用复杂的程序来决定信息经由哪条路径发送最合适，然后重新打包并转发出去。路由器的功能包括过滤、存储转发、路径选择、流量管理、介质转换等。一些增强功能的路由器还可有加密、数据压缩、优先、容错管理等功能。由于路由器工作于网络层，它处理的信息量比网桥要多，因而处理速度比网桥慢。

解答：(16) C (17) A (18) B (19) D (20) A

试题(21)～(25)解析：

本题主要测试防火墙的分类、组成以及作用。

防火墙(Firewall)技术可以分为 IP 过滤、线路过滤和应用层代理等三大类型。目前越来越多的防火墙技术混合使用这些技术，以获得最大的安全性和系统性能。

防火墙系统通常由过滤路由器和代理服务器组成。过滤路由器是一个多端口的 IP 路由器，它能够拦截和检查所有出站和进站的数据。它首先打开 IP 包，取出包头，根据包头的信息(如 IP 源地址，IP 目标地址)确定该包是否符合包过滤规则(如对包头进行语法分析，阻止或允许包传输或接收)，并进行记录。对于符合规则的包，则应该进行转发，否则应进行报警并丢弃该包。代理服务防火墙使用了与包过滤器不同的方法。代理服务器使用一个客户程序与特定的中间节点(防火墙)连接，然后中间节点与期望的服务器进行实际连接。与包过滤器所不同的是，使用这种类型的防火墙，内部与外部网络之间不存在直接连接。因此，即使防火墙发生了问题，外部网络也无法获得与被保护的网络的连接。代理提供了详细的注册和审计功能，这大大提高了网络的安全性，也为改进现有软件的安全性能提供了可能。它是基于特定协议的，如 FTP，HTTP 等。为了通过代理支持一个新的协议，必须改进代理服务器以适应新协议。双宿主主机防火墙、被屏蔽主机、堡垒主机、被屏蔽子网等均属于代理型防火墙。

在网络层，防火墙被用来处理信息在内外网络边界的流动，它可以确定来自哪些地址的信息可以通过或者禁止哪些目的地址的主机。在传输层，这个连接可以被端到端的加密，也就是进程到进程的加密。在应用层，它可以进行用户级的身份认证、日志记录和账号管理等。

防火墙是建立在内外网络边界的过滤封锁机制，内部的网络被认为是安全的和可信赖的，而外部网络(通常是指 Internet)被认为是不安全的和不可信赖的。防火墙的作用就是防止不希望的、未经授权的通信进出被保护的内部网络，通过边界控制强化内部网络的安全策略。防火墙的实现有多种形式，但原理很简单，可以把它想象为一对开关，其中一个用来阻止传输，另一个用来允许传输。不同的防火墙侧重点不同。防火墙技术简单说就是一套身份认证、加密、数字签名和内容检查集一体的安全防范措施。所有来自 Internet 的传输信息和内部网络发出的传输信息都要穿过防火墙，由防火墙进行分析，以确保它们符合站点设定的安全策略。以提供一种内部节点或网络与 Internet 的安全屏障，它是一种被动的网络安全措施。在实际的攻击中，攻击者常常是同时使用多种攻击手段，以取得完全控制被攻击主机的目的。所以，为了确保信息不被窃取或系统免受攻击，防火墙应该具有