

考点分析



第6章 计算机网络

计算机网络知识是软件设计师考试的一个必考点，每次考试的分数基本在5分左右。

6.1 考点分析

本节把历次考试中计算机网络方面的试题进行汇总，得出本章的考点，如表6-1所示。

表6-1 计算机网络试题知识点分布

考试时间	分数	考查知识点
10.11	4	100BASE-TX（1）、组播（2）、双绞线制作（1）
11.05	5	子网掩码（2）、远程管理（1）、TCP/IP端口（1）、带宽（1）
11.11	5	代理服务器（1）、ARP（1）、网络服务组件（1）、OSI参考模型（1）、QoSA标准（1）
12.05	5	多模光纤（1）、CDMA（2）、网络命令（1）、XML（1）
12.11	5	ARP（2）、802.11（1）、子网（2）
13.05	5	路由器概念（1）、ARP表（1）、C类网络（1）、网络命令（1）、DHCP（1）
13.11	5	FTP协议（1）、HTML语法（1）、POP3协议（1）、网络设计原则（1）、网络的需求分析（1）
14.05	6	UDP和HTTP协议（2）、电子邮件协议（1）、PING命令（2）、虚拟目录（1）

根据表6-1,我们可以得出计算机网络的考点主要有：

- （1）网络体系结构：包括OSI参考模型、TCP/IP协议族中的各种协议。
- （2）传输介质与设备：包括双绞线、光纤，各种网络使用的介质，以及常见的网络设备。
- （3）组网技术：包括网络设计原则、网络的需求分析，以及各种接入技术。
- （4）网络管理：包括代理服务器、常用的网络命令等。
- （5）网络应用：包括各种常见的网络应用技术。

对这些知识点进行归类，然后按照重要程度进行排列，如表6-2所示。其中的星号（*）代表知识点的
重要程度，星号越多，表示越重要。

在本章的后续内容中，我们将对这些知识点进行逐个讲解。

表6-2 计算机网络各知识点重要程度

知识点	10.11	11.05	11.11	12.05	12.11	13.05	13.11	13.05	合计	比例	重要程度
网络体系结构	2	3	2	1	4	3	3	3	21	52.50%	★★★★★
传输介质与设备	2				1	1			4	10.00%	★★
网络管理			2	1		1		2	6	15.00%	★★★
组网技术		1		2			2		5	12.50%	★★
网络应用		1	1	1				1	4	10.00%	★★

版权方授权希赛网发布，侵权必究

上一节 本书简介 下一节

网络体系结构

6.2 网络体系结构

在网络体系结构方面，主要考查OSI参考模型和TCP/IP协议族。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

第6章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

OSI参考模型

6.2.1 OSI参考模型

OSI/RM最初是用来作为开发网络通信协议族的一个工业参考标准，作为各个层上使用的协议国际标准化的第一步而发展来的。严格遵守OSI模型，不同的网络技术之间可以轻而易举地实现互操作。整个OSI/RM模型共分7层，从下往上分别是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

1.物理层

物理层的所有协议就是人为规定了不同种类传输设备、传输媒介如何将数字信号从一端传送到另一端，而不管传送的是什么数据。它是完全面向硬件的，它通过一系列协议定义了通信设备机械的、电气的、功能的、规程的特征。

（1）机械特征：规定线缆与网络接口卡的连接头的形状、几何尺寸、引脚线数、引线排列方式、锁定装置等一系列外形特征。

（2）电气特征：规定了在传输过程中多少伏特的电压代表"1",多少伏特代表"0".

（3）功能特征：规定了连接双方每个连接线的作用，用于传输数据的数据线，用于传输控制信息的控制线，用于协调通信的定时线，用于接地的地线。

（4）规程特征：具体规定了通信双方的通信步骤。

2.数据链路层

数据链路层在物理层已能将信号发送到通信链路中的基础上，负责建立一条可靠的数据传输通道，完成相邻结点之间有效地传送数据的任务。正在通信的两个站在某一特定时刻，一个发送数据，一个接收数据。数据链路层通过一系列协议将实现以下功能：

（1）封装成帧：把数据组成一定大小的数据块，称之为帧。然后以帧为单位发送、接收、校验数据。

（2）流量控制：对发送数据的一方，根据接收站的接收情况，实时地进行传输速率控制，以免出现发送数据过快，接收方来不及处理而丢失数据的情况。

（3）差错控制：对接收数据的一方，当接收到数据帧后对其进行检验，如果发现错误，则通知发送方重传。

（4）传输管理：在发送端与接收端通过某种特定形式的对话来建立、维护和终止一批数据的传输过程，以此对数据链路进行管理。

就发送端而言，数据链路层将来自上层的数据按一定规则将比特流送到物理层处理；就接收端而言，它通过数据链路层将来自物理层的比特流合并成完整的数据帧供上层使用。最典型的数据链路层协议是IEEE开发的802系列规范，在该系列规范中将数据链路层分成了两个子层，分别是逻辑链路控制层（LLC）和介质访问控制层（MAC）。LLC层负责建立和维护两台通信设备之间的逻辑通信

链路。MAC层就像交通指挥中心控制汽车通行的车道一样，控制多个信息复用一个物理介质，提供对网卡的共享访问与网卡的直接通信。网卡在出厂前会被分配唯一的由12位十六进制数表示的MAC地址，MAC地址可提供给LLC层来建立同一个局域网中两台设备之间的逻辑链路。

IEEE802规范目前主要包括以下内容：

- (1) 802.1:802协议概论。
- (2) 802.2:逻辑链路控制层 (LLC) 协议。
- (3) 802.3:以太网的CSMA/CD (载波监听多路访问/冲突检测) 协议。
- (4) 802.4:令牌总线 (Token Bus) 协议。
- (5) 802.5:令牌环 (Token Ring) 协议。
- (6) 802.6:城域网协议。
- (7) 802.7:宽带技术协议。
- (8) 802.8:光纤技术协议。
- (9) 802.9:局域网上的语音/数据集成规范。
- (10) 802.10:局域网安全互操作标准。
- (11) 802.11:无线局域网 (WLAN) 标准协议。

3.网络层

网络层用于从发送端向接收端传送分组，负责确保信息到达预定的目标。它存在的主要目的就是解决以下问题：

(1) 通信双方并不相邻。在计算机网络中，通信双方可能是相互邻接的，但也可能并不是邻接的。这样，当一个数据分组从发送端发送到接收端的过程中，就可能在这个中间要经过多个其他网络结点，这些结点暂时存储"路过"的数据分组，再根据网络的"交通状况"选择下一个结点将数据分组发出去，直到发送到接收方为止。

(2) 由于OSI参考模型是出现在许多网络协议之后的，它就必须为使用这些已经存在的网络协议的计算机网络之间的相互通信做出贡献。事实上，网络层的一些协议解决了这样的异构网络的互联问题。

工作在网络层上的协议主要有IP协议和IPX协议。

4.传输层

传输层实现发送端和接收端的端口到端口的数据分组传送，负责保证实现数据包无差错、按顺序、无丢失和无冗余地传输。在传输层上，所执行的任务包括检错和纠错。它的出现是为了更加有效地利用网络层所提供的服务。它主要体现在以下两方面：

- (1) 将一个较长的数据分成几个小数据包发送。
- (2) 解决通信双方不只有一个数据连接的问题。

工作在传输层的协议有TCP协议、UDP协议和SPX协议。

5.会话层

会话层主要负责管理远程用户或进程间的通信。该层提供如名字查找和安全验证等服务，允许两个程序能够相互识别并建立和维护通信连接。会话层还提供数据同步和检查点功能，这样当网络失效时，会对失效后的数据进行重发。在OSI参考模型中，会话层的规范具体包括通信控制、检查点设置、重建中断的传输链路、名字查找和安全验证服务。

6.表示层

表示层以下的各层只关心从源地到目的地可靠地传输数据，而表示层则关心的是所传送信息的语义与语法。它负责将收到的数据转换为计算机内的表示方法或特定的程序的表示方法。也就是说，它负责通信协议的转换、数据的翻译、数据的加密、字符的转换等工作。在OSI参考模型中表示层的规范具体包括数据编码方式的约定和本地句法的转换。各种表示数据的格式的协议也属于表示层，例如：MPEG、JPEG等。

7.应用层

应用层就是直接提供服务给使用者的应用程序的层，比如电子邮件、在线交谈程序都属于应用层的范畴。应用层可实现网络中一台计算机上的应用程序与另一台计算机上的应用程序之间的通信，而且就像在同一台计算机上一样。在OSI参考模型中应用层的规范具体包括各类应用过程的接口和提供用户接口。

8.模型的工作模式

当接收数据时，数据是自下而上传输；当发送数据时，数据是自上而下传输。在网络数据通信的过程中，每一层要完成特定的任务。当传输数据的时候，每一层接收上一层格式化后的数据，对数据进行操作，然后把它传给下一层。当接收数据的时候，每一层接收下一层传过来的数据，对数据进行解包，然后把它传给上一层。从而实现对等层之间的逻辑通信。OSI模型并未确切描述用于各层的协议和服务，它仅仅告诉我们每一层该做些什么。

为了便于复习，我们对OSI参考模型各层的主要功能进行了总结和归纳，如表6-3所示。

表6-3 七层的主要功能

层的名称	主要功能	详细说明
应用层	处理网络应用	直接为端用户服务，提供各类应用过程的接口和用户接口。例如 HTTP、Telnet、FTP、SMTP、NFS 等
表示层	数据表示	使应用层可以根据其服务解释数据的涵义。通常包括数据编码的约定、本地句法的转换。例如 JPEG、ASCII、GIF、DES、MPEG 等
会话层	互连主机通信	负责管理远程用户或进程间的通信，通常包括通信控制、检查点设置、重建中断的传输链路、名字查找和安全验证服务。例如：RPC、SQL 等
传输层	端到端连接	实现发送端和接收端的端到端的数据分组传送，负责保证实现数据包无差错、按顺序、无丢失和无冗余的传输。其服务访问点为端口。代表性协议有 TCP、UDP、SPX 等
网络层	分组传输和路由选择	通过网络连接交换传输层实体发出的数据，解决路由选择、网络拥塞、异构网络互联的问题。服务访问点为逻辑地址（网络地址）。代表性协议有 IP、IPX 等
数据链路层	传送以帧为单位的信息	建立、维持和释放网络实体之间的数据链路，把流量控制和差错控制合并在一起。为 MAC（媒介访问层）和 LLC（逻辑链路层）两个子层。服务访问点为物理地址（MAC 地址）。代表性协议有 IEEE 802.3/2、HDLC、PPP、ATM 等
物理层	二进制位传输	通过一系列协议定义了通信设备的机械的、电气的、功能的、规程的特征。代表性协议有 RS232、V.35、RJ-45、FDDI 等

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

TCP/IP协议族

6.2.2 TCP/IP协议族

TCP/IP不是一个简单的协议，而是一组小的、专业化协议。TCP/IP最大的优势之一是其可路由性，也就意味着它可以携带被路由器解释的网络编址信息。TCP/IP还具有灵活性，可在多个网络操作系统或网络介质的联合系统中运行。然而由于它的灵活性，TCP/IP需要更多的配置。TCP/IP协议族可被大致分为应用层、传输层、网际层和网络接口层四层。

1.应用层

TCP/IP的应用层大致对应于OSI模型的应用层和表示层，应用程序通过本层协议利用网络。这些协议主要有FTP、TFTP、HTTP、SMTP、DHCP、NFS、Telnet、DNS、SNMP等。

FTP (File Transport Protocol,文件传输协议) 是网络上两台计算机传送文件的协议，是通过Internet把文件从客户机复制到服务器上的一种途径。

TFTP (Trivial File Transfer Protocol,简单文件传输协议) 是用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。TFTP协议设计的时候是进行小文件传输的。因此它不具备通常的FTP的许多功能，它只能从文件服务器上获得或写入文件，不能列出目录，不进行认证，它传输8位数据。

HTTP (Hypertext Transfer Protocol,超文本传输协议) 是用于从WWW服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示等。

SMTP (Simple Mail Transfer Protocol,简单邮件传输协议) 是一种提供可靠且有效电子邮件传输的协议。SMTP 是建模在FTP文件传输服务上的一种邮件服务，主要用于传输系统之间的邮件信息并提供来信有关的通知。

DHCP (Dynamic Host Configuration Protocol,动态主机配置协议) 分为两个部分，一个是服务器端，而另一个是客户端。所有的 IP 网络设定数据都由 DHCP 服务器集中管理，并负责处理客户端的 DHCP 要求；而客户端则会使用从服务器分配下来的IP环境数据。DHCP 透过"租约"的概念，有效且动态的分配客户端的 TCP/IP 设定。DHCP分配的IP地址可以分为三种方式，分别是固定分配、动态分配和自动分配。

NFS (Net File System,网络文件系统) 是FreeBSD支持的文件系统中的一种，允许一个系统在网络上与他人共享目录和文件。通过使用NFS,用户和程序可以像访问本地文件一样访问远端系统上的文件。

Telnet (远程登录协议) 是登录和仿真程序，它的基本功能是允许用户登录进入远程主机系统。以前，Telnet是一个将所有用户输入送到远方主机进行处理的简单的终端程序。它的一些较新的版本在本地执行更多的处理，于是可以提供更好的响应，并且减少了通过链路发送到远程主机的信息数量。

DNS (Domain Name System,域名系统) 用于命名组织到域层次结构中的计算机和网络服务。在Internet上域名与IP地址之间是一一对应的，域名虽然便于人们记忆，但机器之间只能互相认识IP地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS就是进行域名解析的服务器。DNS 通过用户友好的名称查找计算机和服务。当用户在应用程序中输入DNS名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如IP地址。

SNMP (Simple Network Management Protocol,简单网络管理协议) 是为了解决Internet上的路由器管理问题而提出的，它可以在IP,IPX,AppleTalk,OSI以及其他用到的传输协议上被使用。SNMP事实上是指一系列网络管理规范的集合，包括协议本身、数据结构的定义和一些相关概念。

目前SNMP已成为网络管理领域中事实上的工业标准，并被广泛支持和应用，大多数网络管理系统和平台都是基于SNMP的。

2.传输层

TCP/IP的传输层大致对应于OSI模型的会话层和传输层，主要包括TCP和UDP,这些协议负责提供流控制、错误校验和排序服务。所有的服务请求都使用这些协议。

TCP (Transport Contrl Portocol,传输控制协议) 是整个TCP/IP协议族中最重要的协议之一，它在IP协议提供的不可靠数据服务的基础上，采用了重发技术，为应用程序提供了一个可靠的、面向连接的、全双工的数据传输服务。TCP协议一般用于传输数据量比较少，且对可靠性要求高的场合。

UDP (User Datagram Protocol,用户数据包协议) 是一种不可靠的、无连接的协议，可以保证应用程序进程间的通信，与同样处在传输层的面向的TCP相比较，UDP是一种无连接的协议，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。UDP协议一般用于传输数据量大，对可靠性要求不是很高，但要求速度快的场合。

3.网际层

TCP/IP的网际层对应于OSI模型的网络层，包括IP、ICMP、IGMP以及 ARP和RARP.这些协议处理信息的路由以及主机地址解析。

IP (Internet Protocol,网际协议) 所提供的服务通常被认为是无连接的和不可靠的，因此把差错检测和流量控制之类的服务授权给了其他的各层协议，这正是TCP/IP能够高效率工作的一个重要保证。网际层的功能主要由IP来提供。除了提供端到端的分组分发功能外，IP还提供了很多扩充功能。例如：为了克服数据链路层对帧大小的限制，网络层提供了数据分块和重组功能，这使得很大的IP数据包能以较小的分组在网上传输。

网际层的另一个重要服务是在互相独立的局域网上建立互连网络，即网际网。网间的报文来往根据它的目的IP地址通过路由器传到另一网络。

ARP (Address Resolution Protocol,地址解析协议) 用于动态地完成IP地址向物理地址的转换。物理地址通常是指主机的网卡地址 (MAC地址) ，每一网卡都有唯一的地址。

RARP (Reverse address resolution protocol,反向地址解析协议) 用于动态完成物理地址向IP地址的转换。

ICMP (Internet Control Message Protocol,网际控制报文协议) 是一个专门用于发送差错报文的协议，由于IP协议是一种尽力传送的通信协议，即传送的数据可能丢失、重复、延迟或乱序传递，所以IP协议需要一种避免差错并在发生差错时报告的机制。

IGMP (Internet Group Management Protocol,网际组管理协议) 允许Internet主机参加多播，也即是IP主机用作向相邻多目路由器报告多目组成员的协议。多目路由器是支持组播的路由器，向本地网络发送IGMP查询。主机通过发送IGMP报告来应答查询。组播路由器负责将组播包转发到所有网络中组播成员。

4.网络接口层

TCP/IP的网络接口层大致对应于OSI模型的数据链路层和物理层，TCP/IP协议不包含具体的物理层和数据链路层，只定义了网络接口层作为物理层的接口规范。网络接口层处在TCP/IP协议的最底层，主要负责管理为物理网络准备数据所需的全部服务程序和功能。该层处理数据的格式化以及将数据传输到网络电缆，为TCP/IP的实现基础，其中可包含IEEE802.3的CSMA/CD、IEEE802.5的

TokenRing等。

5.端口

在TCP/IP网络中，在传输层中，所有的服务都包含端口号，它们可以唯一区分每个数据包包含哪些应用协议。端点系统利用这种信息来区分包中的数据，尤其是端口号使一个接收端计算机系统能够确定它所收到的IP包类型，并把它交给合适的高层软件。

端口号和设备IP地址的组合通常称作插口（socket）。任何TCP/IP实现所提供的服务都用知名的1~1023之间的端口号。这些知名端口号由Internet号分配机构（Internet Assigned Numbers Authority, IANA）来管理。例如：SMTP所用的TCP端口号是25, POP3所用的TCP端口号是110, DNS所用的UDP端口号为53, WWW服务使用的TCP端口号为80. FTP在客户与服务的内部建立两条TCP连接，一条是控制连接，端口号为21, 另一条是数据连接，端口号为20.

256~1023之间的端口号通常都是由Unix系统占用，以提供一些特定的Unix服务。也就是说，提供一些只有Unix系统才有的、而其他操作系统可能不提供的服务。

在实际应用中，用户可以改变服务器上各种服务的保留端口号，但要注意在需要服务的客户端也要改为同一端口号。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

IP地址和子网掩码

6.2.3 IP地址和子网掩码

连接到Internet上的每台计算机都必须有一个唯一地址，称为IP地址。IP地址是一个4字节（共32bit）的数字，被分为4段，每段8位，段与段之间用句点分隔。为了便于表达和识别，IP地址是以十进制形式表示（例如212.152.200.12），每段所能表示的十进制数最大不超过255. IP地址由两部分组成，即网络号和主机号。网络号标识的是Internet上的一个子网，而主机号标识的是子网中的某台主机。

1. IP地址的分类

IP地址可分为5类，分别是A类、B类、C类、D类和E类，大量使用的仅为A, B, C三类。

（1）A类地址：最前面1位为0, 然后用7位来标识网络号，24位标识主机号。即A类地址的第一段取值介于1~126之间。A类地址通常为大型网络而提供，全世界总共只有126个可能的A类网络，每个A类网络最多可以连接224-2台主机（2个保留地址）。

（2）B类地址：最前面2位是10, 然后用14位来标识网络号，16位标识主机号。因此，B类地址的第一段取值介于128~191之间，第一段和第二段合在一起表示网络号。B类地址适用于中等规模的网络，全世界大约有16000个B类网络，每个B类网络最多可以连接216-2台主机（2个保留地址）。

（3）C类地址：最前面3位是110, 然后用21位来标识网络号，8位标识主机号。因此，C类地址的第一段取值介于192~223之间，第一段、第二段合在一起表示网络号。最后一段标识网络上的主机号。C类地址适用于校园网等小型网络，每个C类网络最多可以有28-2台主机（2个保留地址）。

（4）D类地址：最前面4位为11110, D类地址不分网络地址和主机地址，它是一个专门保留的地

址。它并不指向特定的网络，目前D类地址被用在多点广播中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

(5) E类地址：最前面5位为11110,E类地址也不分网络地址和主机地址，为将来使用保留。

有几个特殊的情况。主机号全为1的地址用于广播，叫作广播地址。网络号全为0,则后面的主机号表示本网地址。主机号全为0,此时的网络号就是本网的地址。网络号全为1的地址和32位全为0的地址为保留地址。

2.子网掩码

子网指一个组织中相连的网络设备的逻辑分组。一般子网可表示为某地理位置内（某大楼或相同局域网中）的所有机器。将网络划分成一个个逻辑段（即子网）的目的是便于更好地管理网络，同时提高网络性能，增强网络安全性。另外，将一个组织内的网络划分成各个子网，只需要通过单个共享网络地址，即可将这些子网连接到因特网上，从而减缓了因特网IP地址的耗尽问题。

掩码是一个32位二进制数字，用点分十进制来描述，缺省情况下，掩码包含两个域，分别为网络域和主机域。这些内容分别对应网络号和本地可管理的网络地址部分，通过使用掩码可将本地可管理的网络地址部分划分成多个子网。

例如：假设某个IP地址为176.68.160.12/22,则表示使用22位作为网络地址，那么主机地址就占10位。因此，此子网的主机数可以有 $2^{10}-2=1022$ 个。该IP地址是个B类地址，默认掩码为255.255.0.0（B类地址的前16位为网络地址）。但这个地址中前22位作为网络地址，则子网掩码第三个字节的前6位为子网域，用1表示；剩余的位数为主机域，用0表示。即11111100 00000000,将这个二进制信息转换成十进制作为掩码的后半部分，则可得出完整掩码为255.255.252.0。

3.IPv6

我们前面介绍的IP地址协议的版本号是4（简称为IPv4），它的下一个版本就是IPv6.IPv6正处在不断发展和完善的过程中，它在不久的将来将取代目前被广泛使用的IPv4。

与IPv4相比，IPv6具有以下几个优势：

(1) IPv6具有更大的地址空间。IPv4中规定IP地址长度为32位，而IPv6中IP地址的长度为128位。

(2) IPv6使用更小的路由表。IPv6的地址分配一开始就遵循聚类原则，这使得路由器能在路由表中用一条记录表示一个子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度。

(3) IPv6增加了组播支持以及对流的支持，这使得网络上的多媒体应用有了长足发展的机会，为服务质量（QoS,Quality of Service）控制提供了良好的网络平台。

(4) IPv6加入了对自动配置的支持。这是对DHCP协议的改进和扩展，使得网络（尤其是局域网）的管理更加方便和快捷。

(5) IPv6具有更高的安全性。在使用IPv6网络中用户可以对网络层的数据进行加密并对IP报文进行校验，极大地增强了网络的安全性。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

6.3 传输介质与设备

在传输介质与网络设备方面，主要考查包括双绞线、光纤，各种网络使用的介质，以及常见的网络设备。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

第6章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

传输介质

6.3.1 传输介质

网络传输介质是指在网络中传输信息的载体，常用的传输介质分为有线传输介质和无线传输介质两大类。

无线传输介质是指在两个通信设备之间不使用任何物理连接，而是通过空间传输的一种技术。

无线传输介质主要有微波、红外线和激光等。它们的抗干扰性都比较差。

有线传输介质是指在两个通信设备之间实现的物理连接部分，它可将信号从一方传输到另一方，有线传输介质只有双绞线、同轴电缆和光纤三种。

1. 双绞线

(1) 物理特性：双绞线由按规则螺旋结构排列的2根或4根绝缘线组成。一对线可以作为一条通信电路，各个线对螺旋排列的目的是使各线对之间的电磁干扰最小。

(2) 传输特性：双绞线最普遍的应用是语音信号的模拟传输。使用双绞线通过调制解调器传输模拟数据信号时，数据传输速率目前单向可达56Kbps,双向达33.6Kbps,24条音频通道总的数据传输速率可达230Kbps.使用双绞线发送数字数据信号，一般总的数据传输速率可达2Mbps.

(3) 连通性：双绞线可用于点对点连接，也可用于多点连接。

(4) 地理范围：双绞线用于远程中继线时，最大距离可达15 km;用于10Mbps局域网时，与集线器的距离最大为100 m.

(5) 抗干扰性：在低频传输时，其抗干扰能力相当于同轴电缆。在10~100 kHz时，其抗干扰能力低于同轴电缆。

(6) 价格：双绞线的价格低于其他传输介质，并且安装、维护方便。

对于双绞线，用户最关心的是表征其性能的几个指标。这些指标包括衰减、近端串扰、阻抗特性、分布电容、直流电阻、衰减串扰比、回波损耗等。

2. 同轴电缆

(1) 物理特性：同轴电缆也由两根导体组成，有粗细之分，它由套置单根内导体的空心圆柱体构成。内导体是实芯或者是绞的；外导体是整体的或纺织的。内导体用规则间距的绝缘环或硬的电媒体材料来固定，外导体用护套或屏蔽物包着。

(2) 传输特性：50Ω专用于数字传输，一般使用曼彻斯特编码，数据速率可达2Mbps.CATV电缆可用于模拟和数字信号。对模拟信号，高达300~400MHz的频率是可能的。对数字信号，已能达

到50Mbps。

(3) 连通性：同轴电缆可用于点对点连接，也可用于多点连接。

(4) 地理范围：典型基带电缆的最大距离限于数公里，而宽带网络则可以延伸到数十公里的范围。

(5) 抗干扰性：同轴电缆的结构使得它的抗干扰能力较强，同轴电缆的抗干扰性取决于应用和实现。一般对较高频率来说，它优于双绞线的抗干扰性。

(6) 价格：安装质量好的同轴电缆的成本介于双绞线和光纤之间、维护方便。

3. 光纤

(1) 物理特性：光学纤维是一种直径细（2~125μm）的柔软、能传导光波的介质，能够传导光波的媒体。各种玻璃和塑料可用来制造光学纤维。光缆具有圆柱形的形状，由三个同心部分组成：纤芯、包层、护套。

(2) 传输特性：光纤利用全内反射来传输经信号编码的光束。分多模和单模方式，多模的带宽为200MHz~3GHz/km；单模的带宽为3GHz~50GHz/km。

(3) 连通性：光纤最普通的使用是在点到点的链路上。

(4) 地理范围：光纤信号衰减极小，它可以在6km~8km的距离内不使用中继器实现高速率数据传输。

(5) 抗干扰性：不受电磁干扰和噪声的影响。

(6) 价格：目前光纤系统比双绞线系统和同轴电缆系统贵，但随着技术的进步，它的价格会下降来与其他传输介质竞争。

光纤分为单模光纤和多模光纤。单模光纤一般光纤跳线用黄色表示，接头和保护套为蓝色；传输距离较长，窄芯线，需要激光源，耗散小，高效。多模光纤一般光纤跳线用橙色表示，也有的用灰色表示，接头和保护套用米色或者黑色；传输距离较短，宽芯线，聚光好，耗散大，低效。

一般来说，多模光纤要比单模光纤便宜。如果对传输距离或传送数据的速率要求不严格，那么多模光纤在大多情况下都可以表现得很好。单模光纤虽然成本高，但是具有散射小的特点，可以应用在长距离传输或者需要高速数据速率的场合。

为了便于记忆，我们把有线传输的介质归纳成表6-4。

表6-4 有线传输介质比较

传输介质	类 型	距 离	速 度	特 点
同轴电缆	细缆 RG58	185m	10M	安装容易，成本低，抗干扰性较强
	粗缆 RG11	500m	10M	安装较难，成本低，抗干扰性强
	粗缆 RG-59	>10km	100~150M	传输模拟信号（CATV），也叫宽带同轴电缆，常使用 FDM（频分多路复用）
屏蔽双绞线（STP）	3 类/5 类	100m	16/100M	相对 UTP 笨重，令牌环网常用，现在 7 类布线系统又开始使用
无屏蔽双绞线（UTP）	3/4/5/超 5/6 类	100m	16/20/100/155/200M	价格便宜，安装容易，适用于结构化综合布线，得到了广泛应用，随着网卡技术的发展，在短距离内甚至可以达到 1Gbps
光纤	多模	2km	100~1000M	电磁干扰小，数据速度高，误码率小，低延迟
	单模	2~10km	1~10G	与多模光纤比，特点是高速度、长距离、高成本、细芯线，常使用 WDM（波分复用）提高带宽

在有关传输介质方面，我们还需要掌握各种以太网所使用的介质类型，如表6-5所示。

表6-5 以太网常用传输介质

名 称	传输介质	最大段长度	每段节点数	优 点
10Base5	粗同轴电缆	500m	100	早期电缆，废弃
10Base2	细同轴电缆	185m	30	不需集线器
10Base-T	非屏蔽双绞线	100m	1024	最便宜的系统
10Base-F	光纤	2000m	1024	适合于楼间使用
100Base-T4	非屏蔽双绞线	100m		3 类线，4 对
100Base-TX	非屏蔽双绞线	100m		5 类线，全双工
100Base-FX	光纤	2000m		全双工、长距离
1000Base-SX	光纤	550m		多模光纤
1000Base-LX	光纤	5000m		单模或多模光纤
1000Base-CX	屏蔽双绞线	25m		2 对 STP
1000Base-T	非屏蔽双绞线	100m		5 类线，4 对

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

网络设备

6.3.2 网络设备

常见的网络设备简介如下：

1.网卡

网卡也称为网络适配器或者网络接口卡（ Network Interface Card,NIC ）。网卡及其驱动程序事实上已基本实现了网络协议中底部两层的功能。具体负责主机向媒体收/发信号，实现帧一级协议的有关功能。

2.集线器

集线器（ Hub ）也称为线集中器，工作于数据链路层，它收集多个端口来的数据帧并广播出去。集线器把结点都集中到总线上相互连接在一起，也可以使Hub之间相互用双绞线进一步互联互通。例如：可以先把每间小房间里的计算机先连接在相应的一个hub上，再把这些Hub互相连接而构成一个LAN网络Hub也可分为共享式Hub、堆栈式Hub和交换式Hub.共享式Hub和堆栈式Hub整体作为一个网段；而交换式Hub的每一个端口都允许作为一个网段，速度非常快。

3.重发器

重发器也称为中继器或转发器，这是一种在物理层上因特网段的小设备。因为信号在传输媒体的线路上传输一段距离后必然会发生衰减或者畸变，通过重发器放大增强信号并进行转发就可以保证信号可靠传输。采用重发器把两条（或更多条）干线连接起来的方法，使这两个干线段成为同一个局域网。重发器连接的两个网段，必须是同一种类型的局域网。

4.网桥

网桥也称为桥接器（ Bridge ），这是一种在数据链路层把同段互相连接起来的设备。在网桥中可以进行两个网段之间的数据链路层的协议转换。网桥最重要的功能是对数据进行过滤的能力。即在网桥中保存着所连接的每个网段上所有站点的地址。当收到一个帧时，可以只让必要的数据信息通过网桥或者只向相应的网段转发。

5.交换机

交换机也称为交换器。一台具有基本功能的以太网交换机的工作原理相当于一个具有很多个端

口的多端口网桥，即是一种在LAN中互连多个网段，并可进行数据链路层和物理层协议转换的网络互联设备。当一个以太网的信息帧到达交换机的一个端口时，交换机根据在该帧内的目的地址，采用快速技术把该帧迅速地转发到另一个相应的端口（相应的主机或网段）。目前在以太网交换机中最常用的高速切换技术有直通式和存储转发式两类。

交换机可以分位二层交换机、三层交换机和多层交换机。二层交换机工作在数据链路层，起到多端口网桥的作用，主要用于局域网互连。三层交换机工作在网络层，利用IP地址进行交换，相当于带路由功能的二层交换机。多层交换机工作在高层（传输层以上），这是带协议转换的交换机。

6.路由器

在广域网通信过程中，需要采用一种称为路由的技术，根据地址来寻找到达目的地的路径，路由器就是实现这个过程的网络设备。路由器在属于不同网络段的广域网和局域网间根据地址建立路由，将数据送到最终目的地。路由器工作于网络层，它根据IP地址转发数据包，处理的是网络层的协议数据单元。路由器通过逻辑地址进行网络间的信息转发，可完成异构网络之间的互连互通，只能连接使用相同网络层协议的子网。

按应用范围的不同，路由协议可分为两类：在一个AS（Autonomous System,自治系统）内的路由协议称为内部网关协议（Interior Gateway Protocol,IGP），AS之间的路由协议称为外部网关协议（Exterior Gateway Protocol,EGP）。所谓自治系统是指一个互连网络，就是把整个Internet划分为许多较小的网络单位，这些小的网络有权自主地决定在本系统中应采用何种路由选择协议。常用的内部网关协议有RIP-1、RIP-2、IGRP、EIGRP、IS-IS和OSPF.其中前4种路由协议采用的是距离向量算法，IS-IS和OSPF采用的是链路状态算法。对于小型网络，采用基于距离向量算法的路由协议易于配置和管理，且应用较为广泛，但在面对大型网络时，不但其固有的环路问题变得更难解决，所占用的带宽也迅速增长，以至于网络无法承受。因此对于大型网络，采用链路状态算法的IS-IS和OSPF较为有效，并且得到了广泛的应用。

7.网关

网关也称为网间连接器、信关或联网机，是网络层以上的中继系统。用网关连接两个不兼容的系统要在高层进行协议转换，因此，网关也称为协议转换器。

8.调制解调器

调制解调器同样也是应用在广域网上，作为末端系统和通信系统之间信号转换的设备。分为同步和异步两种，分别连接路由器的同步口和异步口，同步用于专线、帧中继、X.25等高速网络连接，异步用于PSTN的低速连接。调制解调器工作于物理层，它的主要作用是信号变换，即把模拟信号变换成数字信号，或把数字信号变换成模拟信号。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

6.4 组网技术

本知识点重点在于掌握网络设计的原则、网络的需求分析，以及各种组网技术（包括广域网、

网络系统建设

6.4.1 网络系统建设

企业内部网络的建设已经成为提升企业核心竞争力的关键因素。企业网已经越来越多地被人们提到，利用网络技术，现代企业可以在供应商、客户、合作伙伴、员工之间实现优化的信息沟通。这直接关系到企业能否获得关键的竞争优势。企业网络要求具有资源共享功能、通信服务功能、多媒体功能、远程VPN拨入访问功能。所以在进行企业网络的需求分析时，对企业的需求、应用范围、基于的技术等，要从企业应用来进行分析。

先期的网络规划对网络建设和使用至关重要。网络规划的任务就是为即将建立的网络系统提出一套完整的设想和方案，对建立一个什么形式、多大规模、具备哪些功能的网络系统做出全面科学的论证，并对建立网络系统所需的人力、财力和物力投入等做出一个总体的计划。

1. 网络设计的原则

在网络设计方面，应着重考虑以下几个要素，它们也是网络设计和网络建设的基本原则。

(1) 采用先进，成熟的技术。在规划网络、选择网络技术和网络设备时，应重点考虑当今主流的网络技术和网络设备。只有这样，才能保证建成的网络有良好的性能，从而有效地保护建网投资，保证网络设备之间、网络设备和计算机之间的互联，以及网络的尽快使用、可靠运行。

(2) 遵循国际标准，坚持开放性原则。网络的建设应遵循国际标准，采用大多数厂家支持的标准协议及标准接口，从而为异种机、异种操作系统的互连提供极大的便利和可能。

(3) 网络的可管理性。具有良好可管理性的网络，网管人员可借助先进的网管软件，方便地完成设备配置、状态监视、信息统计、流量分析、故障报警、诊断和排除等任务。

(4) 系统的安全性。一般的网络包括内部的业务网和外部网。对于内部用户，可分别授予不同的访问权限，同时对不同的部门(或工作组)进行不同的访问及连通设置。对于外部的因特网，要考虑网络“黑客”和其他不法分子的破坏，防止网络病毒的传播。有些网络系统，如金融系统对安全性和保密性有着更加严格的要求。网络系统的安全性包括两个方面的内容：一方面是外部网络与本单位网络之间互联的安全性问题，另一方面是本单位网络系统管理的安全性问题。

(5) 灵活性和扩充性。网络的灵活性体现在连接方便，设置和管理简单、灵活，使用和维护方便。网络的可扩充性表现在数量的增加、质量的提高和新功能的扩充。网络的主干设备应采用功能强、扩充性好的设备，如模块化结构、软件可升级，信息传输速度快、吞吐量大。可灵活选择快速以太网、千兆以太网、FDDI、ATM网络模块进行配置，关键元件应具有冗余备份的功能。

(6) 系统的稳定性和可靠性。选择网络产品和服务器时，最重要的一点应考虑它们的稳定性和可靠性，这也是我们强调选择技术先进、成熟产品的重要原因之一。关键网络设备和重要服务器的选择应考虑是否具有好的电源备份系统、链路备份系统，是否具有中心处理模块的备份，系统是否具有快速、良好的自愈能力等。不应追求那些功能大而全但不可靠或不稳定的产品，也不要选择

那些不成熟和没有形成规范的产品。

(7) 经济性。网络的规划不但要保质保量按时完成,而且要减少失误、杜绝浪费。

(8) 实用性。网络设计一定要充分保护网络系统现有资源。同时要根据实际情况,采用新技术和新装备,还需要考虑组网过程要与平台建设及开发同步进行,建立一个实用的网络。力求使网络既满足目前需要,又能适应未来发展,同时达到较好的性能/价格比。

2.网络建设的步骤

一个网络从立项、设计、采购、建设、调试到投入运行,是一项复杂的系统工程。如何减少失误、保护投资、提高效益,是网络建设过程中需要重点考虑的问题。网络的设计和实现必须有一整套完整的实施方法和步骤。良好的系统设计方法是保证系统成功的前提,一般要遵循如下步骤:

(1) 网络用户需求调查分析

网络需求分析的目的是充分了解组建网络应当达到的目标(包括近期目标和远期目标)。进行用户需求调研,需掌握以下几个方面的内容。

了解联网设备的地理分布,包括联网设备的数目、位置和间隔距离,用户群组织,以及特殊的需求和限制。

联网设备的软硬件,包括设备类型、操作系统和应用软件等。

所需的网络服务,如电子邮件、WWW服务、视频服务、数据库管理系统、办公自动化、CMIS系统集成等。

实时性要求,用户信息流量等。

本阶段的成果是提出网络用户需求分析报告。

(2) 系统可行性分析

系统可行性分析的目的在于说明组建网络在技术、经济和社会条件等方面的可行性,以及评述为了合理地达到目标而可能选择的各种方案,并说明和论证最终选择的方案。本阶段的成果是提出可行性分析报告,供领导决策。

(3) 网络总体设计

网络总体设计就是根据网络规划中提出的各种技术规范 and 系统性能要求,以及网络需求分析的要求,制订出一个总体计划和方案。网络总体设计包括以下主要内容:

网络流量分析、估算和分配。

网络拓扑结构设计。

网络功能结构设计。

本阶段的成果是确定一个具体的网络系统实施的总体方案,即网络的物理结构和逻辑关系结构。

(4) 网络详细设计

网络详细设计实质上就是分系统进行设计。一个网络由很多部分组成,我们把每个部分称为一个系统(或子系统),这样便于进行设计,能确保设计的精度。对于一个局域网而言,网络的详细设计包括以下内容:

网络主干设计。

子网设计。

网络的传输介质和布线设计。

网络安全和可靠性设计。

网络接入互连网设计。

网络管理设计，包括网络管理的范围、管理的层次、管理的要求，以及网络控制的能力。

网络硬件和网络操作系统的选择。

（5）设备配置、安装和调试

根据网络系统实施的方案，选择性能价格比高的设备，通过公开招标等方式和供应商签定供货合同，确定安装计划。

网络系统的安装和调试主要包括系统的结构化布线、系统安装、单机测试和互联调试等。在设备安装调试的同时开展用户培训工作。用户培训和系统维护是保证系统正常运行的重要因素，使用户尽可能地掌握系统的原理和使用技术，以及出现故障时的一般处理方法。

（6）网络系统维护

网络组建完成后，还存在着大量的网络维护工作，包括对系统功能的扩充和完善，各种应用软件的安装、维护和升级等。另外，网络的日常管理也十分重要，如配置和变动管理、性能管理、日志管理和计费管理等。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

网络分类

6.4.2 网络分类

不同传输距离的网络可以分为局域网、城域网、广域网三种。局域网的相关技术是基于处理近距离传输而设计和发展而来的，而广域网的相关技术是基于处理远距离传输而设计和发展而来的，城域网则是为一个城市网络设计的相关技术。

1. 局域网

局域网（Local Area Network, LAN），是基于传输距离较短的前提下所发展的相关技术的集合，用于将小区域内的各种计算机设备和通信设备互联在一起组成资源共享的通信网络。在局域网中常见的传输媒介有：双绞线、细/粗同轴电缆、微波、射频信号、红外线等。其主要特点：

（1）距离短：0.1km~25km,可以是一个建筑物内、一个校园内或办公室内。

（2）速度快：4Mbps~1Gbps,从早期的4Mbps、10Mbps、100Mbps发展到现在的1000Mbps（1Gbps），而且现在还在不断向前发展。

（3）高可靠性：由于距离很近，传输相当可靠，有极低的误码率。

（4）成本较低：由于覆盖的地域较小，因此传输媒介、网络设备的价格都相对比较便宜，管理也比较简单。

根据不同的技术采用具体的实现方法，局域网有以太网（Ethernet）、令牌环网络（Token Ring）、Apple Talk网络、ArcNet网络几种类型。现在，几乎所有的局域网都是基于以太网实现的。当然，随着应用需求的不断提高，也对局域网技术提出了新的挑战。为了迎合新的需求，科学家们也进行了不懈的研究，出现了一批像FDDI一样的新技术，使局域网技术得到了长足发展。

2. 广域网

广域网 (Wide Area Network,WAN) 是基于传输距离较长的前提下所发展的相关技术的集合, 用于将大区域范围内的各种计算机设备和通信设备互联在一起组成一个资源共享的通信网络。其主要特点如下。

(1) 长距离: 是跨越城市、甚至是联通全球远距离连接。

(2) 低速率: 一般情况下, 广域网的传输速率是以Kbps为单位的。当然随着应用的需要, 引起技术的不断创新, 现在也出现了许多像ISDN、ADSL这样的高速广域网, 其传输速率也能达到Mbps, 当然费用也大大提高了。

(3) 高成本: 相对于城域网、局域网来说, 广域网的架设成本是很昂贵的, 当然它所带来的经济效益也是极大的。就像现在的Internet,就给世界带来了前所未有的大发展。

WAN一般用电话线路, 当然也可以用其他的媒介如光纤、卫星来建立。目前, 经常采用的几种电话线路技术如下:

(1) 公用交换电话网 (PSTN) : 在大多数家庭中使用。

(2) 综合业务数字网 (ISDN) : 最常用的是宽带ISDN,被分为三条信道, 两条用于数据传输, 一条用于控制, 称为2B+D,每条B信道速率为64Kbps,而D信道则为16Kbps。

(3) T1线路: 主要用于商业应用, 其传输速率达到1.544Mbps。

WAN由通信子网与资源子网两个部分组成, 通信子网通常由通信节点和通信链路组成。通信节点往往就是一台计算机。它一方面提供通信子网与资源子网的接口, 另一方面对其他节点又是一个存储转发节点。作为网络接口节点, 它能提供信息的接口, 并对传输以及网络信息进行控制。通信子网中, 软件必须遵循网络协议, 实现对链路及节点存储器的管理, 还必须提供与主处理器、终端集中器及信息交换的接口。资源子系统是连在网上的各种计算机、终端和数据库等。这不仅指硬件, 也包括软件和数据资源。通信子网主要使用分组交换技术, 根据网络通信原理, 局域网与广域网的互联一般是通过第三层设备路由器实现的。

3.城域网

城域网 (Metropolitan Area Network,MAN) 的覆盖范围介于局域网和广域网之间, 城域网的主要技术是DQDB (Distributed Queue Dual Bus,分布式队列双总线), 即IEEE802.6.DQDB是由双总线构成, 所有的计算机都连接在上面。所谓宽带城域网, 就是在城市范围内, 以IP和ATM电信技术为基础, 以光纤作为传输媒介, 集数据、语音、视频服务于一体的高带宽、多功能、多业务接入的多媒体通信网络。

版权方授权希赛网发布, 侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

接入网技术

6.4.3 接入网技术

本节主要介绍常见的网络接入技术。

1.电话接入技术

利用普通电话线接入是成本最低、应用最广的接入技术, 如表6-6所示。

值得注意的一点是，ADSL现在比较成熟的标准包括两种：全速率ADSL标准G.DMT（上行1.5Mbps,下行8Mbps,要求用户安装POTS分离器，复杂且价格昂贵，适用小型办公室）；G.Lite（上行512Kbps,下行1.5Mbps,省去复杂的POTS分离器，成本较低且易于安装，适用普通家庭）。

表6-6 电话线接入技术

2.同轴电缆接入

随着有线电视网的双向改造之后，就催生了Cable MODEM接入的技术。它的基础是HFC（混合光纤-同轴电缆）技术。在同轴电缆接入的技术方案中，用户端需要使用一个称为Cable MODEM（电缆调制解调器）的设备，它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身，它无须拨号，可提供随时在线的永远连接。其上行速度已达10Mbps以上，下行速率更高。

3.光纤接入

随着光纤通信技术的平民化以及高速以太网的发展，现在许多宽带智能小区就是采用以千兆以太网技术为主干，充分利用光纤通信技术完成接入的。实现高速以太网的宽带技术常用的方式是FFTx+LAN,即光纤+局域网。根据光纤深入用户的程度，可以分为：FFTC（Fiber To The Curb,光纤到路边），FFTZ（Fiber To The Zone,光纤到小区），FFTB（Fiber To The Building,光纤到楼），FFTF（Fiber To The Floor,光纤到楼层），FTTH（Fiber To The Home,光纤到户）。

4.移动电话接入

移动通信技术经历了三个发展时期：第一代移动通信系统是模拟通信，采用的是FDMA（频分多址）调制技术，其频谱利用率低；第二代移动通信系统是现在常用的数字通信系统，采用的是TDMA（时分多址）的数字调制方式，对系统的容量限制较大；而新近出现的第三代移动通信（3G）技术则采用了CDMA（码分多址）数字调制技术，能够提供大容量、高质量、综合业务、软切换的要求。

（1）WCDMA:这是基于GSM网发展出来的3G技术规范，该标准提出了在GSM基础上的升级演进策略："GSM（2G）→GPRS→EDGE→WCDMA（3G）"。

（2）CDMA2000:这是由窄带CDMA（CDMA-1S95）技术发展而来的宽带CDMA（3G）技术，该标准提出了在CDMA-1S95基础上的升级演进策略："CDMA1S95（2G）→CDMA20001x→CDMA20003x（3G）"。CDMA20003x与CDMA20001x的主要区别在于应用了多路载波技术来提高速度。

（3）TD-SCDMA:时分同步CDMA,是由我国大唐电信公司提出的3G标准，该标准提出不经过2.5代的中间环节，直接向3G过渡，非常适用于GSM系统向3G升级。TD-SCDMA将智能无线、同步CDMA和软件无线电等技术融入其中，在频谱利用率、对业务支持的灵活性、频率灵活性及成本等方面具有独特优势。

（4）OCDMA:OCDMA技术在原理上与码分复用技术相似。OCDMA通信系统给每个用户分配一个唯一的光正交码的码字作为该用户的地址码。在发送端，对要传输的数据用地址码进行光正交编码，然后实现信道复用；在接收端，用与发送端相同的地址码进行光正交解码。

5.接口层协议

在连接到Internet及远程访问时，需要使用相应的接口层协议，常见的协议包括以下几个：

（1）SLIP协议：提供了串行通信线路上封装IP数据包的简单方法。但有三个不足：事先需要知

道对方的IP地址，不支持动态IP地址分配；只支持IP协议；没有校验字段，需上层进行差错控制。

(2) PPP协议：有效的点对点通信协议，采用HDLC封装，可用于不同传输媒体，解决了SLIP的限制：远程服务器可以为本地客户机提供一个动态IP地址；支持IP、IPX、OSI等多种网络协议；具有差错检测功能，提供一组网络控制协议。

(3) PPPoE协议：它利用了PPP的优点、结合以太网的优势，可实现多台客户机同时接入Internet。它继承了以太网的快速和PPP拨号的简捷、用户验证、IP分配等方面的优势。

6.RAS网络

在实现远程访问服务时，需要在服务器端设置一台RAS服务器，并通过Modem池来为多个客户提供服务，客户端需要使用PPP协议与RAS建立连接。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

第6章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

网络管理

6.5 网络管理

网络管理具有故障管理、配置管理、计费管理、性能管理和安全管理五大管理功能。在网络管理方面，主要考查包括代理服务器、常用的网络命令等。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

第6章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

代理服务器

6.5.1 代理服务器

代理服务器是介于浏览器和Web服务器之间的一台服务器，当用户通过代理服务器上网浏览时，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送给用户的浏览器。

代理服务器的作用主要体现在以下5个方面：

(1) 提高访问速度。因为客户要求的数据存于代理服务器的硬盘中，因此下次这个客户或其他客户再要求相同目的站点的数据时，就会直接从代理服务器的硬盘中读取，代理服务器起到了缓存的作用，对热门站点有很多客户访问时，代理服务器的优势更为明显。

(2) 可以起到防火墙的作用。因为所有使用代理服务器的用户都必须通过代理服务器访问远程站点，因此在代理服务器上就可以设置相应的限制，以过滤或屏蔽掉某些信息。这是局域网网管对局域网用户访问范围限制最常用的办法，也是局域网用户为什么不能浏览某些网站的原因。拨号用户如果使用代理服务器，同样必须服从代理服务器的访问限制，除非你不使用这个代理服务器。

(3) 通过代理服务器访问一些不能直接访问的网站。因特网上有许多开放的代理服务器，客户在访问权限受到限制时，而这些代理服务器的访问权限是不受限制的，刚好代理服务器在客户的访问范围之内，那么客户通过代理服务器访问目标网站就成为可能。国内的高校多使用教育网，不能出国，但通过代理服务器，就能实现访问因特网，这就是高校内代理服务器热的原因所在。

(4) 安全性得到提高。无论是上聊天室还是浏览网站，目的网站只能知道用户来自于代理服务器，而用户的真实IP就无法测知，这就使得用户的安全性得以提高。

(5) 共享IP地址。由于IP地址比较紧张，通过代理服务器，可以节约一些IP地址。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

第6章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

网络管理工具

6.5.2 网络管理工具

现在网络管理平台有很多，而真正具有OSI定义的网管五大功能的系统却不多，典型的系统包括HP的Open View、IBM的Net View和Tivoli、SUN的SunNet、Cabletron的SPECTRUM.Cisco Work则是最适用于Cisco网络设备密集的网络的实用性网络管理系统。

在进行网络维护时，我们经常需要监视网络数据流并对其进行分析，这也称为网络监视，而常见的网络监视器包括Ethereal,NetXRay和Sniffer。

(1) Ethereal:提供了对TCP,UDP,SMB,telnet,ftp等常用协议的支持，覆盖了大部分应用需求。

(2) NetXRay:主要是用做以太网上的网管软件，能够对IP,NetBEUI,TCP/UDP等协议进行详细分析。

(3) Sniffer:它是使网络接口处于混杂模式，以截获网络内容。它是最完善、应用最广泛的一种网络监视器。

另外，在操作系统中有两个十分常用的网络管理工具：

(1) ping命令：基于ICMP协议，用于把一个测试数据包发送到规定的地址，如果一切正常则返回成功响应，并且可以从时戳中获得链路的状态信息。它常用于以下几个情形：

验证TCP/IP协议是否正常安装：ping 127.0.0.1,如果正常返回，说明安装成功。其中127.0.0.1是回送地址。

验证IP地址配置是否正常：ping本机IP地址。

查验远程主机：ping远端主机IP地址。

(2) tracert:检查到达的目标IP地址的路径并记录结果。tracert命令显示用于将数据包从计算机传递到目标位置的一组IP路由器，以及每个跃点所需的时间。如果数据包不能传递到目标，tracert命令将显示成功转发数据包的最后一个路由器。

(3) netstat:用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

(4) IPConfig:显示当前的TCP/IP配置。这些信息一般用来检验人工配置的TCP/IP设置是否正

确。

[版权方授权希赛网发布，侵权必究](#)

[上一节](#) [本书简介](#) [下一节](#)

第 6 章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

网络应用

6.6 网络应用

在网络应用方面，主要考查XML、OGSA等新技术的基本概念和应用。

[版权方授权希赛网发布，侵权必究](#)

[上一节](#) [本书简介](#) [下一节](#)

第 6 章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

可扩展标记语言

6.6.1 可扩展置标语言

可扩展置标语言（Extensible Markup Language, XML）是一套定义语义置标的规则，这些置标将文档分成许多部分并对这些部分加以标识。它也是元置标语言，用于定义其他与特定领域有关的、语义的、结构化的置标语言的句法语言。XML同HTML（Hypertext Markup Language, 超文本置标语言）一样，都来自SGML（Standard Generalized Markup Language, 即标准通用置标语言）。

虽然XML与HTML都是置标语言，但它们在结构和应用上有很大的区别。

HTML是一种格式化的语言，一个HTML文本可以看作一个格式化的程序。HTML（及类似的）语言定义了一套固定的置标，用来描述一定数目的元素。如果置标语言中没有所需的置标，用户也就没有办法了。另外，用该语言描述的程序或文本具有“内容+格式”的双重属性。一个HTML在不同平台、不同浏览器上的表现是一模一样的。而一段符合XML语法规则的文本则是一段“纯”的数据，它的结构由其他的称为DTD（Document Type Description）的文本来描述；而它的处理则可能是任何其他支持XML的容器或程序，例如：IE浏览器依据相关的CSS或XSL文件来显示XML数据；开发人员可以用来自Microsoft、IBM、Sun、BEA、Inprise等厂商的任何支持XML的开发工具开发自己的XML处理程序。

与HTML相比的另一不同是XML是一种元置标语言。它可以被用于定义其他的置标语言。例如：在Peter Murray-Rust的Chemical Markup Language（化学置标语言，简称为CML）中的MOL.DTD文件中描述了词汇表和分子科学的句法。对于其他领域也有其他的DTD, 用户还可以创建自己的DTD。

1.XML的组织

一个实用的XML文档必须满足两点：组织良好的（well-formed）和有效的（valid）。下例试

图描述一个记事条 (note) :

```
<?xml version="1.0"?>
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

这就是一份可以接受的XML文档。由于使用了一些人们易于理解的置标如<note>、<body>等, 我们觉得这些数据十分易读和有意义。

这也是一个组织良好的XML文档, 即它满足以下三项基本规则:

- (1) 文档以XML定义<?xml version="1.0"?>开始。
- (2) 有一个包含所有其他内容的根元素, 如上面例子中的<note>和</note>置标符。
- (3) 所有元素必须合理地嵌套, 不允许交叉嵌套。

组织良好的XML可以对应为一棵逻辑树。没有组织好的文档在HTML中可能不算什么, 因为浏览器已经被设计成可以处理这种问题。但是在XML中却是致命的, 因为应用程序将拒绝处理没有组织好的文件。

XML文档光组织良好是不够的。例如如下的"记事条"数据:

```
<?xml version="1.0"?>
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
</note>
```

这段数据是组织良好的, 但却不会产生什么实用价值, 因为它不含关键的"内容" (<body>) ! 因此, 我们还必须要有一个文档对XML数据文档的内容作出规定, 这种文档就是文档类型描述DTD. 例如, 关于note的DTD可以这么写:

```
<?xml version="1.0"?>
<!DOCTYPE note [
  <!ELEMENT note ( to,from,heading,body ) >
  <!ELEMENT to ( #PCDATA ) >
  <!ELEMENT from ( #PCDATA ) >
  <!ELEMENT heading ( #PCDATA ) >
  <!ELEMENT body ( #PCDATA ) >
]>
```

!DOCTYPE note第二行的节点是XML文档中的"note"类型; 第三行说明元素"note"有四个元素"to,from,heading,body";第四行定义了"to"元素的类型为"#PCDATA";第五行定义了"from"元素的类型为"#PCDATA"等。

DTD可以看做对XML数据的语法结构的描述。不同的人就能够使用共同的DTD来交换数据, 应

用程序可以使用这个标准的DTD来验证接收到的数据是有效的。当然也可以使用一个DTD来验证自己的XML数据。

除DTD外，还有一种方式来定义有效的XML 文档，那就是W3C与XML标准一起定义的XML模式（XML Schema），它们与 DTD 相比有几个优势：

（1）XML模式使用XML语法。换句话说，XML模式是一个XML文档。这意味着可以象处理任何其他文档一样处理模式。例如：可以编写一个XSL样式表，该样式表将 XML 模式转换成具有自动生成的JavaScript代码的 Web 表单，其中的JavaScript代码可以验证输入的数据。

（2）XML模式支持数据类型。尽管DTD确实支持数据类型，但这些数据类型是从发布的角度开发的。XML模式支持DTD中的所有原始数据类型，还支持整数、浮点数、日期、时间、字符串、URL和其他对数据处理和验证有用的数据类型。

（3）XML模式是可扩展的。除了XML模式规范中定义的数据类型以外，还可以创建自己的数据类型，并且可以基于其他数据类型派生出新的数据类型。

（4）XML模式有更强的表达能力。例如：我们可以用 XML模式定义任何 <state> 属性值不得超过2个字符，而用DTD则无法做这些事。

2.CSS与XSL

XML文档最终是要通过一定的应用程序来表现的，例如：浏览器。用浏览器来表现XML就要经过CSS或XSL这一媒介，它们都是样式语言，描述了XML数据与HTML置标的映射关系。或者说，XSL是对XML文档进行"排版"的语言。

（1）CSS

级联样式单（Cascading Style Sheets,CSS）可以在某种程度上把HTML文档中的排版格式信息与其他数据信息分离开。

一个CSS样式单就是一组规则，样式再根据特定的一套规则级联起来。每个规则给出此规则所适用的元素的名称，以及此规则要应用于那些元素的样式。例如，如下清单是一首诗的CSS样式单：

```
POEM { display: block }
TITLE { display: block; font-size: 16pt; font-weight: bold }
POET { display: block; margin-bottom: 10px }
STANZA { display: block; margin-bottom: 10px }
VERSE { display: block }
```

此样式单有五个规则。每个规则有一个选择符--规则所应用的元素的名称--和一组适用于此元素实例的属性。第一个规则说明POEM元素应以块的形式（Display:block）显示其内容。第二个规则说明TITLE元素应以16磅（font-size:16pt）、粗体（font-weight:bold）将其内容显示在块中（Display:block）。第三个规则说明POET元素应通过自身显示在块中（Display:block），并且与紧随其后的下一块相距10个像素（margin-bottom:10px）。第四个规则与第三个相同，所不同的只是前者应用于STANZA元素。最后，第五个规则只简单地说明VERSE元素也是显示在自己的块中。

定义了如上的CSS以后，HTML文档就可以用"POEM"、"TITLE"来说明真正的"数据"了。

（2）XSL

可扩展的样式语言（Extensible Style Language,XSL）是专门用于XML文档的样式单语言，可以把XSL当成一种能够把XML转变成HTML的语言，一种能够筛选和排序XML文档中数据的语言，一

种能够根据XML的数据数值格式化XML数据的语言（例如把负数显示成红色）。XSL文档本身就是结构完整的XML文档。

（3）CSS与XSL比较

CSS只能改变特定元素的格式，也只能以元素为基础。但XSL样式单可以重新排列元素并对元素进行重排序。这种样式单可以隐藏一些元素而显示另外一些元素。更进一步说，还可以选择应用样式的置标，不仅是基于置标的，而且还基于置标的内容和特性，还基于置标在文档中相对于其他元素的位置，以及基于各种其他的准则。

CSS的优越性在于具有广泛的浏览器支持。但是XSL更为灵活和强大，可更好地适用于XML文档。而且带XSL样式单的XML文档可以很容易地转换为带CSS样式单的HTML文档。

如果只是要对一些“固定”数据进行“排版”，可以使用“HTML+CSS”方式；如果这些数据是与某些应用程序相关，独立于程序存在的，并且要独立于程序来使用，则应该充分使用XML技术，采用“HTML+XML+XSL”。

3.XML编程接口

本节将介绍XML的多种编程接口，这些接口为开发人员使用XML文档提供了统一的接口。有许多API可以使用，本节介绍最流行和广泛使用的API中的四种：DOM、API、JDOM和JAXP。

（1）DOM

DOM（Document Object Model,文档对象模型）由W3C制定和管理，定义了与平台和语言无关的接口，以便允许程序和脚本动态访问和修改文档内容、结构及样式。它提供了一组表现HTML和XML文档的标准对象集合以及这些对象如何组合的标准模型，一组访问和操作这些对象的标准接口。DOM的目标是提供一个可以通用于各种程序语言、操作系统和应用程序的API,所以DOM具有极高的兼容性，不论CORBA、COM、Java、C++等都可以使用同样的DOM接口。也因为这种跨平台的需求，DOM在定义时就采用了CORBA标准，因此它可以为各种语言提供完全相同的接口。

DOM是一套为合法的Well-Formed文件设计的API（应用程序接口），它同时定义了这些文件的逻辑结构、访问及操作方法。在DOM的规范里，文件的定义很广泛，其中包括了HTML和XML。所以，DOM也可以用来操作XML及HTML文件，也可以用DOM建立文件、浏览文件结构以及增加或删除文件的某些内容。

XML将数据组织为一棵树，DOM就是对这棵树的一个对象描述。通俗地说，就是通过解析XML文档，为XML文档在逻辑上建立一个树模型，树的节点是一个个对象。我们通过存取这些对象就能够存取XML文档的内容。DOM的基本对象有5个，分别是Document、Node、NodeList、Element和Attr。

（2）SAX

SAX（Simple API for XML,XML简单应用程序接口）是一种基于事件的模型，可用于避免构造整个文档的树状结构。如果文档特别庞大或仅对其中一部分感兴趣，SAX就显得特别有用了。SAX事件由解析器在进入或离开文档、元素、属性、目录子树时产生。该模型可在不关注文档完整结构的情况下测定其特征或相关数据。

SAX是一个基于事件XML解析器定义的、可以免费获得的、与平台和语言无关的API,它允许程序和脚本动态的访问和更新文档内容、结构和风格。所以，它作为一个中间件层用来把XML文档中的数据解释成相应的Java事件。SAX是一种事件驱动的接口。它的基本原理是由接口的用户提供符合定义的处理函数，XML分析时遇到特定的事件，就去调用处理器中特定事件的处理函数。SAX需要用户

提供以下三个处理器类的实现：

DocumentHandlerXML:文件事件的处理器。

DTDHandler:DTD中事件的处理器。

ErrorHandler:出错处理器。

(3) JDOM

JDOM是一个开源项目，它基于树形结构，利用纯Java的技术对XML文档实现解析、生成、序列化以及多种操作。JDOM 直接为Java编程服务。它利用Java语言的诸多特性（方法重载、集合概念以及映射），把SAX和DOM的功能有效地结合起来。在使用设计上尽可能地隐藏原来使用XML过程中的复杂性。

JDOM 的主要特性是它极大地减少了必须编写的代码数量，JDOM 应用程序的长度通常是DOM 应用程序的三分之一，大约是SAX应用程序的一半。JDOM并不做所有的事，但对于大多数要做的解析可能正好适合。

(4) JAXP

尽管DOM、SAX和JDOM为大多数常见任务提供了标准接口，但仍有些事情是它们不能解决的。例如：在Java程序中创建DOMParser对象的过程因DOM解析器的不同而不同。为了修正这个问题，Sun发布了JAXP（Java API for XML Parsing,用于XML解析的Java API）。该API为使用DOM、SAX和XSL处理XML文档提供了公共接口。

JAXP提供的诸如DocumentBuilderFactory 和 DocumentBuilder之类的接口为不同的解析器提供了一个标准接口。还有一些方法可以允许你控制底层的解析器是否可以识别名称空间以及是否使用DTD或模式来验证XML文档。

为了选择合适的接口类型，需要理解所有接口的设计要点，而且需要理解应用程序用XML文档来做什么。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

开放式网格服务体系

6.6.2 开放式网格服务体系

开放式网格服务体系（Open Grid Services Atchitecture,OGSA）被称为是下一代的网格体系结构，是Web服务（Web Seviles）和网格（Grid）技术结合的产物，提供一组遵守特定的约定并定义明确的接口，是实体之间产生、管理和交换信息的机制。OGSA已成为网格基础框架的标准，它利用Web服务的标准接口定义机制、多协议绑定、本地与远端的透明性，利用网络服务的语义、可靠性和安全模型、生命周期管理、发现和其他服务，以及多主机运行环境来建构自己的框架。

简单地讲，网格是把整个Internet整合成一台巨大的超级计算机，实现各种资源的全面共享。当然，网格并不一定非要这么大，也可以构造地区性的网格，如中关村科技园区网格、希赛内部网格、局域网网格，甚至家族网格和个人网格等等。网格根本的特征不是它的规模，而是资源共享，

消除资源孤岛。

OGSA最早形成气候是在高性能计算机领域，因为高性能计算机资源最稀缺，一般的企业用户现在只是刚刚发现。今天不仅有计算网格，还有数据网格、信息网格、GIS网格、基因网格等等。随着应用潜力的挖掘，还会有更多的网格冒出来。

OGSA最突出的思想就是以服务为中心。在OGSA框架中，将一切都抽象为服务，包括计算机、程序、数据、仪器设备等。这种观念有利于通过统一的标准接口来管理和使用网格。Web服务提供了一种基于服务的框架结构，但是，Web服务面对的一般都是永久服务，而在网格应用环境中，大量的临时性的短暂服务，比如一个计算任务的执行等。考虑到网格环境的具体特点，OGSA 在原来Web服务概念的基础上，提出了网格服务（Grid Service）的概念，用于解决服务发现、动态服务创建、服务生命周期管理等与临时服务有关的问题。

基于网格服务的概念，OGSA 将整个网格看作是网格服务的集合，但是这个集合不是一成不变的，是可以扩展的，这反映了网格的动态特性。网格服务通过定义接口来完成不同的功能，服务数据是关于网格服务实例的信息，因此网格服务可以简单地表示为“网格服务=接口/行为+服务数据”。

以网格服务为中心模型具有如下好处：

（1）由于网格环境中所有的组件都是虚拟化的，因此，通过提供一组相对统一的核心接口，所有的网格服务都基于这些接口实现，就可以很容易地构造出具有层次结构的、更高级别的服务，这些服务可以跨越不同的抽象层次，以一种统一的方式来对待。

（2）虚拟化也使得将多个逻辑资源实例映射到相同的物理资源上成为可能，在对服务进行组合时不必考虑具体的实现，可以以底层资源组成为基础，在虚拟组织（Virtual Organization）中进行资源管理。通过网格服务的虚拟化，可以将通用的服务语义和行为，无缝地映射到本地平台的基础设施上。

在OGSA中提供了三种运行环境，分别是简单运行环境、虚拟运行环境以及组操作环境。这三种环境的关系是从简单到复杂，包含的服务从具体到抽象。用户直接提出的服务要求，一般都比较抽象和复杂，但是这些要求可以转化为多个相对基本的要求或者服务，这样层层分解，直到找到基本可以满足的服务为止。

网格技术和Web服务技术是OGSA的关键技术，有关这些技术的详细内容，请读者阅读《系统分析师技术指南（2007版）》（张友生主编，清华大学出版社）。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

6.6.3 电子政务

电子政务作为电子信息技术与管理的有机结合，成为当代信息化的最重要的领域之一。所谓电子政务，就是应用现代信息和通信技术，将管理和服务通过网络技术进行集成，在因特网上实现组织结构和 workflows 的优化重组，超越时间和空间及部门之间的分隔限制，向社会提供优质和全方位的、规范而透明的、符合国际水准的管理和服务。

事实上，电子政务的主要模式有GtoG模式、GtoE模式、GtoB模式和GtoC模式4种，由于数字2的英文two与to同音，因此，上述4种模式也写成G2G模式、G2E模式、G2B模式和G2C。

(1) G2G:政府 (Government) 之间的电子政务，称为G2G,它是指政府内部、政府上下级之间、不同地区和不同职能部门之间实现的电子政务活动。G2G模式是电子政务的基本模式，具体的实现方式可分为：政府内部网络办公系统、电子法规、政策系统、电子公文系统、电子司法档案系统、电子财政管理系统、电子培训系统、垂直网络化管理系统、横向网络协调管理系统、网络业绩评价系统、城市网络管理系统等十个方面，亦即传统的政府与政府间的大部分政务活动都可以通过网络技术的应用高速度、高效率、低成本地实现。

(2) G2E:政府 (Government) 与政府公务员 (即政府雇员Employee) 之间的电子政务，主要是利用Intranet建立起有效的行政办公和员工管理体系，为提高政府工作效率和公务员管理水平服务。G2E电子政务是政府机构通过网络技术实现内部电子化管理的重要形式，也是G2G、G2B和G2C电子政务模式的基础。

(3) G2B:政府 (Government) 与企业 (Business) 之间的电子政务。即政府通过网络进行采购与招标，快捷迅速地为企业提供各种信息服务；企业通过网络进行税务通报、办理证照、参加政府采购、对政府工作的意见反馈等；政府向企业事业单位发布的各种方针、政策、法规、行政规定等。对政府来说，G2B电子政务的形式主要包括以下几种：电子采购与招标、电子税务、电子证照办理、电子外经贸管理、中小企业服务、综合信息服务等。

(4) G2C:政府 (Government) 与公民 (Citizen) 之间的电子政务，是政府通过电子网络系统为公民提供各种服务。G2C电子政务所包含的内容十分广泛，主要的应用包括：公众信息服务、电子身份认证、电子税务、电子社会保障服务、电子民主管理、电子医疗服务、电子就业服务、电子教育、培训服务、电子交通管理等。G2C电子政务的目的是除了政府给公众提供方便、快捷、高质量的服务外，更重要的是可以开辟公众参政、议政的渠道，畅通公众的利益表达机制，建立政府与公众的良性互动平台。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

电子商务

6.6.4 电子商务

电子商务，顾名思义是指在Internet网上进行商务活动。其主要功能包括网上的广告、订货、付款、客户服务和货物递交等销售、售前和售后服务，以及市场调查分析、财务核计及生产安排等多项利用Internet开发的商业活动。电子商务的一个重要技术特征是利用Web的技术来传输和处理商业信息。

电子商务有广义和狭义之分。狭义的电子商务也称作电子交易 (e-commerce)，主要是指利用Web提供的通信手段在网上进行的交易。而广义的电子商务包括电子交易在内的利用Web进行的全部商业活动，如市场分析、客户联系、物资调配等等，亦称作电子商业 (e-business)。这些商务活动可以发生于公司内部、公司之间及公司与客户之间。

电子商务不仅仅是买卖，也不仅仅是软硬件的信息，而是在Internet、企业内部网（Intranet）和企业外部网（Extranet），将买家与卖家、厂商和合作伙伴紧密结合在了一起，因而消除了时间与空间带来的障碍。

电子商务也有几种模式：B2B、B2C、C2C,这里的B表示企业Business,C表示顾客Customer.

（1）B2B:企业与企业之间通过因特网进行产品、服务及信息的交换。例如，阿里巴巴就是一个典型B2B平台。除了在线交易和产品展示，B2B业务更重要的意义在于，将企业内部网，通过B2B网站与客户紧密结合起来，通过网络的快速反应，为客户提供更好的服务，从而促进企业的业务发展。

（2）B2C:即商家对消费者。也就是通常所说的"网上购物网站",企业、商家可充分利用电子商城提供的网络基础设施、支付平台、安全平台、管理平台等共享资源有效地、低成本地开展自己的商业活动。例如，希赛网的第一书店、学赛网的视频等，都属于B2C服务。

（3）C2C:即个人对个人的交易行为。C2C商务平台就是通过为买卖双方提供一个在线交易平台，使卖方可以主动提供商品上网拍卖，而买方可以自行选择商品进行竞价。在C2C方面，淘宝网、拍拍网、eBay、易趣等都做得不错。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

第6章：计算机网络

作者：希赛教育软考学院 来源：希赛网 2014年05月20日

万维网

6.6.5 万维网

WWW（万维网）是一个支持交互式访问的分布式超媒体系统。超媒体系统（在超文本的基础上，结合语音、图形、图像、动画等信息）直接扩充了传统的超文本系统（非线性的、用"链接"整合的信息结构）。Web文档用HTML来撰写。除了文本外，文档还包括指定文档版面与格式的标签。在页面中可以包含图形、音频、视频等各种多媒体信息。

在WWW中，依赖于标准化的统一资源定位器URL地址来定位信息的内容。在进行页面访问时采用超文本传送协议HTTP,其服务端口就是HTTP服务端口（80端口）。首先，浏览器软件与HTTP端口建立一个TCP连接，然后发送GET命令，Web服务器根据命令取出文档，发送给浏览器；浏览器释放连接，显示文档。

在上网时在浏览器地址栏中输入的地址称为URL（Uniform Resource Locator,统一资源定位符），也就是我们常说的网址。例如，<http://www.educity.cn/>

[ruankao/2007rk.htm](http://www.educity.cn/ruankao/2007rk.htm),其中www.educity.cn是域名，后面部分是我们要访问的文件所在的目录和文件名。

版权方授权希赛网发布，侵权必究

[上一节](#) [本书简介](#) [下一节](#)

电子邮件

6.6.6 电子邮件

电子邮件 (E-mail) 是现在数据量、使用量最大的一个因特网应用, 它用来完成人际之间的信息通信。与它相关的有以下三个协议:

- (1) SMTP:简单邮件传送协议, 用于邮件的发送, 工作在25号端口上。
- (2) POP3:邮局协议V3.0,用于接收邮件, 工作在110号端口上。
- (3) IMAP:邮件访问协议, 是用于替代POP3协议的新协议, 工作在143号端口上。

E-mail地址的格式是"用户名@域名",例如edu@educity.cn.

Outlook Express和Foxmail是常见的2个电子邮件客户端软件, 用来收发邮件。如果要在电子邮件中传送一个文件, 则应通过附件功能。

电子邮件系统在中心服务器(邮件服务器) 上给用户分配电子邮箱, 也就是在服务器的硬盘上, 划出一块区域, 相当于邮局, 在这块存储区内又分成许多小区, 就是邮箱。发送方发送邮件时, 邮件发送到发送服务器, 再由发送服务器将其送到接收方的收信服务器中相应的邮箱, 接收方随时读取或下载到本地。

版权方授权希赛网发布, 侵权必究

[上一节](#) [本书简介](#) [下一节](#)

DNS

6.6.7 DNS

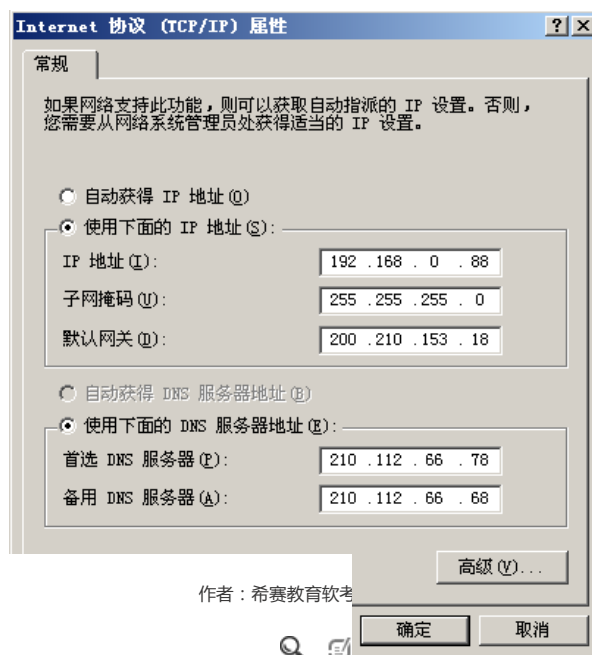
网络用户希望用有意义的名字来标识主机, 而不是IP地址。为了解决这个需求, 应运而生了一个域名服务系统DNS (工作在53号端口)。它是运行在TCP协议之上, 负责将域名转换成实际相对应的IP地址, 从而在不改变底层协议的寻址方法的基础上, 为使用者提供一个直接使用符号名来确定主机的平台。

DNS是一个分层命名系统, 名字由若干个标号组成, 标号之前用圆点分隔。最右边的是主域名, 最左边的是主机名, 中间的是子域名。

注意: 通常我们在写域名时, 最后是不加一个"."的, 其实这只是一个缩写, 最后一个"."代表的是"根", 如果采用全域名写法, 还需要加上这个小点。这在配置DNS时就会需要。

除了以上讲述的名字语法规则和管理机构的设立, 域名系统中还包括一个高效、可靠、通用的分布式系统用于名字到地址的映射。将域名映射到IP地址的机制由若干个称为名字服务器 (name server) 的独立、协作的系统组成。

例如, 如果我们要访问学赛网软考学院中的软考报考指南, 则要访问的URL为http://www.educity.cn/ruankao/index.htm, 其中www.educity.cn表示所访问网站的域名。假设www.educity.cn的IP地址为213.210.118.88, 域名记录存储在IP地址为213.210.112.34的域名服务器中。某主机的TCP/IP属性配置如图6-4所示。



DNS

IP地址属性设置

图6-1表明，如果通过局域网连接Internet,需要设置TCP/IP协议的属性，其中需要指定3个IP地址，即本机地址、默认网关地址和DNS的地址。所谓网关，是完成Internet连接共享，局域网内的其他机器则通过它来实现对Internet的访问。

图6-1所示的主机要访问www.educity.cn,则首先查询IP地址为210.112.66.78的域名服务器。如果连接不成功，才会连接备用DNS服务器210.112.66.68。

版权方授权希赛网发布，侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

IIS

6.6.8 IIS

IIS (Internet Information Server,因特网信息服务) 是一种Web (网页) 服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络 (包括因特网和局域网) 上发布信息成了一件很容易的事。

1.IIS的添加和运行

进入"控制面板",依次选"添加/删除程序→添加/删除Windows组件",将"Internet信息服务 (IIS)"前的小钩去掉 (如有)，重新勾选中后按提示操作即可完成IIS组件的添加。用这种方法添加的IIS组件中将包括Web、FTP、NNTP和SMTP等全部4项服务。

当IIS添加成功之后，再进入"开始→设置→控制面板→管理工具→Internet服务管理器 (Internet信息服务)"以打开IIS管理器，对于有"已停止"字样的服务，均在其上单击鼠标右键，选"启动"来开启。

2.建立Web站点

例如，本机的IP地址为192.168.0.1,自己的网页放在D:\educity目录下，网页的首页文件名为

index.htm,现在想根据这些建立自己的Web服务器。

对于此Web站点,我们可以用现有的"默认Web站点"来做相应的修改后,就可以轻松实现。先在"默认Web站点"上单击右键,选"属性",以进入名为"默认Web站点属性"设置界面。

(1) 修改绑定的IP地址:转到"Web站点"窗口,再在"IP地址"后的下拉菜单中选择所需用到的本机IP地址"192.168.0.1".

(2) 修改主目录:转到"主目录"窗口,再在"本地路径"输入(或用"浏览"按钮选择)好自己网页所在的"D:\educity"目录。

(3) 添加首页文件名:转到"文档"窗口,再按"添加"按钮,根据提示在"默认文档名"后输入自己网页的首页文件名"index.htm".

(4) 添加虚拟目录:主目录在"D:\educity"下,而我们想输入"192.168.0.1/test"的格式就可调出"E:\csai"中的网页文件,这里面的"test"就是虚拟目录。在"默认Web站点"上单击右键,选"新建→虚拟目录",依次在"别名"处输入"test",在"目录"处输入"E:\csai"后再按提示操作即可添加成功。

3.对IIS服务的远程管理

(1) 在"管理Web站点"上单击右键,选"属性",再进入"Web站点"窗口,选择好"IP地址".

(2) 转到"目录安全性"窗口,单击"IP地址及域名限制"下的"编辑"按钮,点选中"授权访问"以能接受客户端从本机之外的地方对IIS进行管理;最后单击"确定"按钮。

(3) 则在任意计算机的浏览器中输入如"http://192.168.0.1:3598"(3598为其端口号)的格式后,将会出现一个密码询问窗口,输入管理员帐号名(Administrator)和相应密码之后就可登录成功,在浏览器中对IIS进行远程管理了。在这里可以管理的范围主要包括对Web站点和FTP站点进行的新建、修改、启动、停止和删除等操作。

版权方授权希赛网发布,侵权必究

上一节

本书简介

下一节

VOD

6.6.9 VOD

视频点播(Video on Demand,VOD)也称为交互式电视点播系统,亦即根据用户的需要播放相应的视频节目。一个VOD系统主要由3部分构成,分别是服务端系统、网络系统和客户端系统。

1.服务端系统

服务端系统主要由视频服务器、档案管理服务器、内部通信子系统和网络接口组成。档案管理服务器主要承担用户信息管理、计费、影视材料的整理和安全保密等任务。内部通信子系统主要完成服务器间信息的传递、后台影视材料和数据的交换。网络接口主要实现与外部网络的数据交换和提供用户访问的接口。视频服务器主要由存储设备、高速缓存和控制管理单元组成,其目标是实现对媒体数据的压缩和存储,以及按请求进行媒体信息的检索和传输。视频服务器与传统的数据服务器有许多显著的不同,需要增加许多专用的软硬件功能设备,以支持该业务的特殊需求。例如:媒体数据检索、信息流的实时传输以及信息的加密和解密等。对于交互式的VOD系统来说,服务端系统还需要实现对用户实时请求的处理、访问许可控制、VCR(Video Cassette Recorder)功能(如

快进、暂停、重绕等)的模拟。

2.网络系统

网络系统包括主干网络和本地网络两部分。因为它负责视频信息流的实时传输,所以是影响连续媒体网络服务系统性能极为关键的部分。同时,媒体服务系统的网络部分投资巨大,故而在设计时不仅要考虑当前的媒体应用对高带宽的需求,而且还要考虑将来发展的需要和向后的兼容性。当前,可用于建立这种服务系统的网络物理介质主要有CATV(有线电视)的同轴电缆、光纤和双绞线。而采用的网络技术主要有快速以太网、FDDI和ATM技术。

3.客户端系统

目前,根据不同的功能需求和应用场景,主要有3种VOD系统,分别是NVOD、TVOD和IVOD。

(1) NVOD (Near Video On Demand):称为就近式点播电视,多个视频流依次间隔一定的时间启动发送同样的内容。例如,12个视频流每隔10分钟启动一个发送同样的两小时的电视节目。如果用户想看这个电视节目可能需要等待,但最长不会超过10分钟,他们会选择距他们最近的某个时间起点进行收看。在这种方式下,一个视频流可能为许多用户共享。

(2) TVOD (True Video On Demand):称为真实点播电视,它真正支持即点即放。当用户提出请求时,视频服务器将会立即传送用户所要的视频内容。若有另一个用户提出同样的需求,视频服务器就会立即为他再启动另一个传输同样内容的视频流。不过,一旦视频流开始播放,就要连续不断的播放下去,直到结束。这种方式下,每个视频流转为某个用户服务。

(3) IVOD (Interactive Video On Demand):称为交互式点播电视。它比前两种方式有很大程度上的改进。它不仅支持即点即放,而且还可以让用户对视频流进行交互式的控制。这时,用户就可像操作传统的录像机一样,实现节目的播放、暂停、倒回、快进和自动搜索等。

版权方授权希赛网发布,侵权必究

[上一节](#)

[本书简介](#)

[下一节](#)

第7章:数据库系统

作者:希赛教育软考学院 来源:希赛网 2014年05月20日

考点分析

第7章 数据库系统

数据库系统是软件设计师的一个考试重点,上午考试中大约有6分的试题是数据库技术方面的试题,下午有1道试题是数据库技术方面的试题,占15分。在这些试题中,主要考查数据库模型、数据的基本操作、数据库设计,以及事务处理。

7.1 考点分析

本节把历次考试中数据库系统方面的试题进行汇总,得出本章的考点,如表7-1和表7-2所示。

表7-1 数据库系统上午试题知识点分布