网络工程师学习笔记

maodou#show run
!

Written by maodou(毛豆) maojinjin(毛晋晋)
Description 水平有限,欢迎指正,可以转载,请保留作者信息.
2006-4-21
ip address 于湖南长沙空军航空学院
E-mail address maodou@mail.com(国际英文) maodou66@163.com(国内中文)
MSN maodou66@msn.com
Oicq number 12356857
Homepage http://maodou.10000te.com

!

网络工程师学习笔记

考试科目
1：计算机与网络知识
1.计算机系统知识

第 3 章 交换技术
主要内容：1、线路交换
2、分组交换
3、帧中继交换
4、信元交换
一、线路交换
1、线路交换进行通信：是指在两个站之间有一个实际的物理连接，这种连接是结点之间线路的连接序列。
2、线路通信三种状态：线路建立、数据传送、线路拆除
3、线路交换缺点：典型的用户/主机数据连接状态，在大部分的时间内线路是空闲的，因而用线路交换方法实现数据连接效率低下；为连接提供的数据速率是固定的，因而连接起来的两个设备必须用相同的数据率发送和接收数据，这就限制了网络上各种主机以及终端的互连通信。
二、分组交换技术
1、分组交换的优点：线路利用率提高；分组交换网可以进行数据率的转换；在线路交换网络中，若通信量较大可能造成呼叫堵塞的情况，即网络拒绝接收更多的连接要求直到网络负载减轻为止；优先权的使用。
2、分组交换和报文交换主要差别：在分组交换网络中，要限制所传输的数据单位的长度。报文交换系统却适应于更大的报文。
3、虚电路的技术特点：在数据传送以前建立站与站之间的一条路径。
4、数据报的优点：避免了呼叫建立状态，如果发送少量的报文，数据报是较快的；由于其较原始，因而较灵活；数据报传递特别可靠。
5、几点说明：
路线交换基本上是一种透明服务，一旦连接建立起来，提供给站点的是固定的数据率，无论是模拟或者是数字数据，都可以通过这个连接从源传输到目的。而分组交换中，必须把模拟数据转换成数字数据才能传输。
6、外部和内部的操作
外部虚电路，内部虚电路。当用户请求虚电路时，通过网络建立一条专用的路由，所有的分组都用这个路由。
外部虚电路，内部数据报。网络分别处理每个分组。于是从同一外部虚电路送来的分组可以用不同的路由。在目的结点，如有需要可以先缓冲分组，并把它们按顺序传送给目的站点。
外部数据报，内部数据报。从用户和网络角度看，每个分组都是被单独处理的。
外部数据报，内部虚电路。外部的用户没有用连接，它只是往网络发送分组。而网络为站之间建立传输分组用的逻辑连接，而且可以把连接另外维持一个扩展的时间以便满足预期的未来需求。

三、帧中继交换

1、X.25 特性：(1)用于建立和终止虚电路的呼叫控制分组与数据分组使用相同的通道和虚电路；(2)第三层实现多路复用虚电路；(3)在第二层和第三层都包含着流控和差错控制机制。

2、帧中继与 X.25 的差别：(1)呼叫控制信号与用户数据采用分开的逻辑连接，这样，中间结点就不必维护与呼叫控制有关的状态表或处理信息；(2)在第二层而不是在第三层实现逻辑连接的多路复用和交换，这样就省掉了整个一层的处理；(3)不采用一步一步的流控和差错控制。

3、在高速 H 通道上帧中继的四种应用：数据块交互应用；文件传输；低速率的复用；字符交互通信。

四、信元交换技术

1、ATM 信元

ATM 数据传送单位是一固定长度的分组，称为信元，它有一个信元头及一个信元信息域。信元长度为 53 个字节，其中信元头占 5 个字节，信息域占 48 个字节。

信元头主要功能是：信元的网络路由。

2、ATM 采用了异步时分多路复用技术 ATDM，ATDM 采用排队机制，属于不同源的各个信元在发送到介质上之前，都要被分隔并存入队列中，这样就需要速率的匹配和信元的定界。

3、应用独立：主要表现在时间独立和语义独立两方面。时间独立即应用时钟和网络时钟之间没有关联。语义独立即在信元结构和应用协议数据单元之间无关联，所有与应用有关的数据都在信元的信息域中。

3、ATM 信元标识

ATM 采用虚拟通道模式，通信通道用一个逻辑号标识。对于给定的多路复用器，该标识是本地的，并在任何交换部件处改变。

通道的标识基于两种标识符，即虚拟通路标识 VPI 和虚拟通道标识 VCI。一个虚拟通路 VP 包含有若干个虚拟通道 VC

4、ATM 网络结构

虚拟通道 VC：用于描述 ATM 信元单向传送的一个概念，信元都与一个惟一的标识值-虚拟通道标识符 VCI 相联系。

虚拟通路 VP：用于描述属于虚拟通路的 ATM 信元的单向传输的一个概念，虚拟通路都与一个标识值-虚拟通路标识符相联系。

虚拟通道和虚拟通路者用来描述 ATM 信元单向传输的路由。每个虚拟通路可以用复用方式容纳多达 65535 个虚拟通道，属于同一虚拟通道的信元群，拥用相同虚拟通道标识 VCI，它是信元头一部分。

第 4 章 网络体系结构及协议

主要内容：1、网络体系结构及协议的定义

2、开放系统互连参考模型 OSI

3、TCP/IP 协议集

一、网络体系结构及协议的定义

1、网络体系结构：是计算机之间相互通信的层次，以及各层中的协议和层次之间接口的集合。

2、网络协议：是计算机网络和分布系统中互相通信的对等实体间交换信息时所必须遵守

的规则的集合。

3、语法（syntax）:包括数据格式、编码及信号电平等。

4、语义（semantics）：包括用于协议和差错处理的控制信息。

5、定时（timing）：包括速度匹配和排序。

二、开放系统互连参考模型

1、国际标准化组织 ISO 在 1979 年建立了一个分委员会来专门研究一种用于开放系统的体系结构，提出了开放系统互连 OSI 模型，这是一个定义连接异种计算机的标准主体结构。

2、OSI 简介：OSI 采用了分层的结构化技术，共分七层，物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

3、OSI 参考模型的特性：是一种异构系统互连的分层结构；提供了控制互连系统交互规则的标准骨架；定义一种抽象结构，而并非具体实现的描述；不同系统中相同层的实体为同等层实体；同等层实体之间通信由该层的协议管理；相信层间的接口定义了原语操作和低层向上层提供的服务；所提供的公共服务是面向连接的或无连接的数据服务；直接的数据传送仅在最低层实现；每层完成所定义的功能，修改本层的功能并不影响其他层。

4、物理层：提供为建立、维护和拆除物理链路所需要的机械的、电气的、功能的和规程的特性；有关的物理链路上传输非结构的位流以及故障检测指示。5、数据链路层：在网络层实体间提供数据发送和接收的功能和过程；提供数据链路的流控。

6、网络层：控制分组传送系统的操作、路由选择、拥护控制、网络互连等功能，它的作用是将具体的物理传送对高层透明。

7、传输层：提供建立、维护和拆除传送连接的功能；选择网络层提供最合适的服务；在系统之间提供可靠的透明的数据传送，提供端到端的错误恢复和流量控制。

8、会话层：提供两进程之间建立、维护和结束会话连接的功能；提供交互会话的管理功能，如三种数据流方向的控制，即一路交互、两路交替和两路同时会话模式。

9、表示层：代表应用进程协商数据表示；完成数据转换、格式化和文本压缩。

10、应用层：提供 OSI 用户服务，例如事务处理程序、文件传送协议和网络管理等。

三、TCP/IP 的分层

1、TCP/IP 的分层模型

Internet 采用了 TCP/IP 协议，如同 OSI 参考模型，TCP/IP 也是一种分层模型。它是基于硬件层次上的四个概念性层次构成，即网络接口层、IP 层、传输层、应用层。

网络接口层：也称数据链路层，这是 TCP/IP 最底层。功能：负责接收 IP 数据报并发送至选定的网络。

IP 层：IP 层处理机器之间的通信。功能：它接收来自传输层的请求，将带有目的地址的分组发送出去。将分组封装到数据报中，填入数据报头，使用路由算法以决定是直接将数据报传送至目的主机还是传给路由器，然后把数据报送至相应的网络接口来传送。

传输层：是提供应用层之间的通信，即端到端的通信。功能：管理信息流，提供可靠的传输服务，以确保数据无差错的地按序到达。

2、TCP/IP 模型的分界线

协议地址分界线：以区分高层和低层的寻址，高层寻址使用 IP 地址，低层寻址使用物理地址。应用程序 IP 层之上的协议软件只使用 IP 地址，而网络接口层处理物理地址。

操作系统分界线：以区分系统与应用程序。在传输层和应用层之间。

3、复用与分解

发送报文时，发送方在报文中加和了报文类型、选用协议等附加信息。所有的报文以帧的形式在网络中复用传送，形成一个分组流。在接收方收到分组时，参考附加信息对接收到的分组进行分解。

四、IP 协议

1、Internet 体系结构

一个 TCP/IP 互联网提供了三组服务。最底层提供无连接的传送服务为其他层的服务提供了基础。第二层一个可靠的传送服务为应用层提供了一个高层平台。最高层是应用层服务。

2、IP 协议： 这种不可靠的、无连接的传送机制称为 internet 协议。

3、IP 协议三个定义：

（1）IP 定义了在 TCP/IP 互联网上数据传送的基本单元和数据格式。

（2）IP 软件完成路由选择功能，选择数据传送的路径。

（3）IP 包含了一组不可靠分组传送的规则，指明了分组处理、差错信息发生以及分组德育的规则。

4、IP 数据报：联网的基本传送单元是 IP 数据报，包括数据报头和数据区部分。

5、IP 数据报封装：物理网络将包括数据报报头的整个数据报作为数据封装在一个帧中。

6、MTU 网络最大传送单元：不同类型的物理网对一个物理帧可传送的数据量规定不同的上界。

7、IP 数据报的重组：一是在通过一个网络重组；二是到达目的主机后重组。后者较好，它允许对每个数据报段独立地进行路由选择，且不要求路由器对分段存储或重组。

8、生存时间：IP 数据报格式中设有一个生存时间字段，用来设置该数据报在联网中允许存在的时间，以秒为单位。如果其值为 0，就把它从互联网上删除，并向源站点发回一个出错消息。

9、IP 数据报选项：

IP 数据报选项字段主要是用于网络测试或调试。包括：记录路由选项、源路由选项、时间戳选项等。

路由和时间戳选项提供了一种监视或控制互联网路由器路由数据报的方法。

五、用户数据报协议 UDP

1、UDP 协议功能

为了在给定的主机上能识别多个目的地址，同时允许多个应用程序在同一台主机上工作并能独立地进行数据报的发送和接收，设计用户数据报协议 UDP。

使用 UDP 协议包括：TFTP、SNMP、NFS、DNS

UDP 使用底层的互联网协议来传送报文，同 IP 一样提供不可靠的无连接数据报传输服务。它不提供报文到达确认、排序、及流量控制等功能。

2、UDP 的报报文格式

每个 UDP 报文分 UDP 报头和 UDP 数据区两部分。报头由四个 16 位长（8 字节）字段组成，分别说明该报文的源端口、目的端口、报文长度以及校验和。

3、UDP 协议的分层与封装

在 TCP/IP 协议层次模型中，UDP 位于 IP 层之上。应用程序访问 UDP 层然后使用 IP 层传送数据报。IP 层的报头指明了源主机和目的主机地址，而 UDP 层的报头指明了主机上的源端口和目的端口。

4、UDP 的复用、分解与端口

UDP 软件应用程序之间的复用与分解都要通过端口机制来实现。每个应用程序在发送数据报之前必须与操作系统协商以获得协议端口和相应的端口号。

UDP 分解操作：从 IP 层接收了数据报之后，根据 UDP 的目的端口号进行分解操作。

UDP 端口号指定有两种方式：由管理机构指定的为著名端口和动态绑定的方式。

六、可靠的数据流传输 TCP

1、TCP/IP 的可靠传输服务五个特征：面向数据流、虚电路连接、有缓冲的传输、无结构

的数据流、全双工的连接。

2、TCP 采用了具有重传功能的肯定确认技术作为可靠数据流传输服务的基础。

3、为了提高数据流传输过程的效率，在上述基础上引入滑动窗口协议，它允许发送方在等待一个确认之前可以发送多个分组。滑动窗口协议规定只需重传未被确认的分组，且未被确认的分组数最多为窗口的大小。

4、TCP 功能

TCP 定义了两台计算机之间进行可靠的传输而交换的数据和确认信息的格式，以及计算机为了确保数据的正确到达而采取的措施。

5、TCP 连接使用是一个虚电路连接，连接使用一对端点来标识，端点定义为一对整数（host,port）其中 host 是主机的 IP 地址，port 是该主机上 TCP 端口号。

6、TCP 使用专门的滑动窗口协议机制来解决传输效率和流量控制这两个问题，TCP 采用的滑动窗口机制解决了端到端的流量控制，但并未解决整个网络的拥塞控制。

7、TCP 允许随时改变窗口小，通过通告值来说明接收方还能再接收多少数据，通告值增加，发送方扩大发送滑动窗口；通告值减小，发送方缩小发送窗口。

8、TCP 的报文格式

报文分为两部分：报头和数据，报头携带了所需要的标识和控制信息。

确认号字段指示本机希望接收下一个字节组的序号；

顺序号字段的值是该报文段流向上的数据流的位置，即发送序号；

确认号指的是与该报文段流向相反方向的数据流。

9、TCP 使用 6 位长的码位来指示报文段的应用目的和内容

URG 紧急指针字段可用；ACK 确认字段可用；PSH 请求急近操作；RST 连接复位；SYN 同步序号；FIN 发送方字节流结束。

10、TCP 的三次握手

为了建立一个 TCP 连接，两个系统需要同步其初始 TCP 序号 ISN。序号用于跟踪通信顺序并确保多个包传输时没有丢失。初始序号是 TCP 连接建立时的起始编号。

同步是通过交换携带有 ISN 和 1 位称为 SYN 的控制位的数据包来实现的。

握手可由一方发起也可以双方发起，建立就可以实现双向对等地数据流动，没有主从关系。

第 5 章局域网技术

主要内容：1、局域网定义和特性

2、各种流行的局域网技术

3、高速局域网技术

4、基于交换的局域网技术

5、无线局域网技术及城域网技术

一、局域网定义和特性

局域网（Local Area Network）即 LAN：将小区域内的各种通信设备互联在一起的通信网络。

1、局域网三个特性：（1）高数据速率在 0.1-100Mbps（2）短距离 0.1-25Km（3）低误码率 10-8-10-11。

2、决定局域网特性的三个技术：（1）用以传输数据的介质（2）用以连接各种设备的拓扑结构（3）用以共享资源的介质控制方法。

3、设计一个好的介质访问控制协议三个基本目标：（1）协议要简单（2）获得有效的通道利用率（3）对网上各站点用户的公平合理。

二、以太网 Ethernet IEEE802.3

以太网是一种总路线型局域网，采用载波监听多路访问/冲突检测 CSMA/CD 介质访问控制方法。

1、载波监听多路访问

CSMA 的控制方案：（1）一个站要发送，首先需要监听总线，以决定介质上是否存在其他站的发送信号。（2）如果介质是空闲的，则可以发送。（3）如果介质忙，则等待一段间隔后再重试。

坚持退避算法：

（1）非坚持 CSMA：假如介质是空闲的，则发送；假如介质是忙的，等待一段时间，重复第一步。利用随机的重传时间来减少冲突的概率，缺点：是即使有几个站有数据发送，介质仍然可能牌空闲状态，介质的利用率较低。

（2）1-坚持 CSMA：假如介质是空闲的，则发送；假如介质是忙的，继续监听，直到介质空闲，立即发送；假如冲突发生，则等待一段随机时间，重复第一步。缺点：假如有两个或两个以上的站点有数据要发送，冲突就不可避免的。

（3）P-坚持 CSMA：假如介质是空闲的，则以 P 的概率发送，而以（1-P）的概率延迟一个时间单位，时间单位等于最大的传播延迟时间；假如介质是忙的，继续监听，直到介质空闲，重复第一步；假如发送被延迟一个时间单位，则重复第一步。

2、载波监听多路访问/冲突检测

这种协议广泛运用在局域网内，每个帧发送期间，同时有检测冲突的能力，一旦检测到冲突，就立即停止发送，并向总线上发一串阻塞信号，通知总线上各站冲突已经发生，这样通道的容量不致因白白传送已经损坏的帧而浪费。

冲突检测的时间：对基带总线，等于任意两个站之间最大的传播延迟的两倍；对于宽带总线，冲突检测时间等于任意两个站之间最大传播延迟时间的四倍。

3、二进制退避算法：

（1）对每个帧，当第一次发生冲突时，设置参量为 L=2；

（2）退避间隔取 1-L 个时间片中的一个随机数，1 个时间片等于 2a；

（3）当帧重复发生一次冲突时，则将参量 L 加倍；

（4）设置一个最大重传次数，则不再重传，并报告出错。

二、标记环网 Toke Ring IEEE802.5

1、标记的工作过程：

标记环网又称权标网，这种介质访问使用一个标记沿着环循环，当各站都没有帧发送时，标记的形式为 01111111，称空标记。当一个站要发送帧时，需要等待空标记通过，然后将它改为忙标记 011111110。并紧跟着忙标记，把数据发送到环上。由于标记是忙状态，所以其他站不能发送帧，必须等待。发送的帧在环上循环一周后再回到发送站，将该帧从环上移去。同时将忙标记改为空标记，传至后面的站，使之获得发送帧的许可权。

2、环上长度用位计算，其公式为：存在环上的位数等于传播延迟（5μs/km）×发送介质长度×数据速率＋中继器延迟。对于 1km 长、1Mbps 速率、20 个站点，存在于环上的位数为 25 位。

3、站点接收帧的过程：当帧通过站时，该站将帧的目的地址和本站的地址相比较，如地址相符合，则将帧放入接收缓冲器，再输入站，同时将帧送回至环上；如地址不符合，则简单地将数据重新送入环。

4、优先级策略

标记环网上的各个站点可以成不同的优先级，采用分布式高度算法实现。控制帧的格式如下：P 优先级、T 空忙、M 监视位、预约位

三、光纤分布式数据接口 FDDI ISO9314

1、FDDI 和标记环介质访问控制标准接近，有以下几点好处：

（1）标记环协议在重负载条件下，运行效率很高，因此 FDDI 可得到同样的效率。

（2）使用相似的帧格式，全球不同速率的环网互连，在后面网络互加这一章将要讨论这个问题

（3）已经熟悉 IEEE802.5 的人很容易了解 FDDI

（4）已经积累了 IEEE802.5 的实践经验，特别是将它做集成电路片的经济，用于 FDDI 系统和元件的制造。

2、FDDI 技术

（1）数据编码：用有光脉冲表示为 1，没有光能量表示为 0。FDDI 采用一种全新的编码技术，称为 4B/5B。每次对四位数据进行编码，每四位数据编码成五位符号，用光的存在和没有来代表五位符号中每一位是 1 还是 0。这种编码使效率提高为 80%。为了得到信号同步，采用了二级编码的方法，先按 4B/5B 编码，然后再用一种称为倒相的不归零制编码 NRZI，其原理类似于差分编码。

（2）时钟偏移： FDDI 分布式时钟方案，每个站有独立的时钟和弹性缓冲器。进入站点缓冲器的数据时钟是按照输入信号的时钟确定的，但是，从缓冲器输出的信号时钟是根据站的时钟确定的，这种方案使环中中继器的数目不受时钟偏移因素的限制。

3、FDDI 帧格式：

由此可知：FDDI MAC 帧和 IEEE802.5 的帧十分相似，不同之处包括：FDDI 帧含有前文，对高数据率下时钟同步十分重要;允许在网内使用 16 位和 48 位地址,比 IEEE802.5 更加灵活;控制帧也有不同。

4、FDDI 协议

FDDI 和 IEEE802.5 的两个主要区别：

（1）FDDI 协议规定发送站发送完帧后，立即发送一幅新的标记帧，而 IEEE802.5 规定当发送出去的帧的前沿回送至发送站时，才发送新的标记帧。

（2）容量分配方案不同，两者都可采用单个标记形式，对环上各站点提供同等公平的访问权，也可优先分配给某些站点。IEEE802.5 使用优先级和预约方案。

5、为了同时满足两种通信类型的要求，FDDI 定义了同步和异步两种通信类型，定义一个目标标记循环时间 TTRT，每个站点都存在有同样的一个 TTRT 值。

四、局域网标准

IEEE802 委员会是由 IEEE 计算机学会于 1980 年 2 月成立的，其目的是为局域网内的数字设备提供一套连接的标准，后来又扩大到城域网。

1、服务访问点 SAP

在参考模型中，每个实体和另一个实体的同层实体按协议进行通信。而一个系统内，实体和上下层间通过接口进行通信。用服务访问点 SAP 来定义接口。

2、逻辑连接控制子层 LLC

IEEE802 规定两种类型的链路服务：无连接 LLC（类型 1），信息帧在 LLC 实体间，无需要在同等层实体间事先建立逻辑链路，对这种 LLC 帧既不确认，也无任何流量控制或差错恢复功能。

面向连接 LLC（类型 2），任何信息帧，交换前在一对 LLC 实体间必须建立逻辑链路。在数据传送方式中，信息帧依次序发送，并提供差错恢复和流量控制功能。

3、介质访问控制子层 MAC

IEEE802 规定的 MAC 有 CSMA/CD、标记总线、标记环等。

4、服务原语

（1）ISO 服务原语类型

REQUEST 原语用以使服务用户能从服务提供者那里请求一定的服务，如建立连接、发送数据、结束连接或状态报告。

INDICATION 原语用以使服务提供者能向服务用户提示某种状态。如连接请求、输入数据或连接结束。

RESPONSE 原语用以使服务用户能响应先前的 INDIECATION，如接受连接 INDICATION。

CONFIRMARION 原语用以使服务提供者能报告先前的 REQUEST 成功或失败。

（2）IEEE802 服务原语类型

和 ISO 服务原语类型相比 REQUEST 和 INDICATION 原语类型和 ISO 所用的具有相同意义。IEEE802 没有 REPONSE 原语类型，CONFIRMATION 原语类型定义为仅是服务提供者的确认。

五、逻辑链路控制协议

1、IEEE802.2 是描述 LAN 协议中逻辑链路 LLC 子层的功能、特性和协议，描述 LLC 子层对网络层、MAC 子层及 LLC 子层本身管理功能的界面服务规范。

2、LLC 子层界面服务规范 IEEE802.2 定义了三个界面服务规范：（1）网络层/LLC 子层界面服务规范；（2）LLC 子层/MAC 子层界面服务规范；（3）LLC 子层/LLC 子层管理功能的界面服务规范。

3、网络层/LLC 子层界面服务规范

提供两处服务方式

不确认无连接的服务：不确认无连接数据传输服务提供没有数据链路级连接的建立而网络层实体能交换链路服务数据单元 LSDU 手段。数据的传输方式可为点到点方式、多点式或广播式。这是一种数据报服务

面向连接的服务：提供了建立、使用、复位以及终止数据链路层连接的手段。这些连接是 LSAP 之间点到点式的连接，它还提供数据链路层的定序、流控和错误恢复，这是一处虚电路服务。

4、LLC 子层/MAC 子层界面服务规范

本规范说明了 LLC 子层对 MAC 子层的服务要求，以便本地 LLC 子层实体间对等层 LLC 子层实体交换 LLC 数据单元。

（1）服务原语是：MA-DATA.request 、MA-DATA.indication、MA-DATA.confirm

（2）LLC 协议数据单元结构 LLC PDU：

目的服务访问点地址字段 DSAP，一个字节，其中七位实际地址，一位为地址型标志，用来标识 DSAP 地址为单个地址或组地址。

源服务访问点地址字段 SSAP，一个字节，其中七位实际地址，一位为命令/响应标志位用来识别 LLC PDU 是命令或响应。

控制字段、信息字段。

5、LLC 协议的型和类

LLC 为服务访问点间的数据通信定义了两种操作：Ⅰ型操作，LLC 间交换 PDU 不需要建立数据链路连接，这些 PDU 不被确认，也没有流量控制和差错恢复。

Ⅱ型操作，两个 LLC 间交换带信息的 PDU 之间，必须先建立数据链路连接，正常的通信包括，从源 LLC 到目的 LLC 发送带有信息的 PDU，它由相反方向上的 PDU 所确认。

LLC 的类型：第 1 类型，LLC 只支持Ⅰ型操作；第 2 类型，LLC 既支持Ⅰ型操作，也支持Ⅱ型操作。

6、LLC 协议的元素

控制字段的三种格式：带编号的信息帧传输、带编号的监视帧传输、无编号控制传输、无编号信息传输。

带编号的信息帧传输和带编号的监视帧传输只能用于Ⅱ型操作。

无编号控制传输和无编号信息传输可用于Ⅰ型或Ⅱ型操作，但不能同时用。

信息帧用来发送数据，监视帧用来作回答响应和流控。

六、CSMA/CD 介质访问控制协议

1、MAC 服务规范三种原语

MA-DATA.request 、MA-DATA.indication、MA-DATA.confirm

2、介质访问控制的帧结构

CSMA/CD 的 MAC 帧由 8 个字段组成：前导码；帧起始定界符 SFD；帧的源和目的地址 DA、SA；表示信息字段长度的字段；逻辑连接控制帧 LLC；填充的字段 PAD；帧检验序列字段 FCS。

前导码：包含 7 个字节，每个字节为 10101010，它用于使 PLS 电路和收到的帧定时达到稳态同步。

帧起始定界符：字段是 10101011 序列，它紧跟在前导码后，表示一幅帧的开始。帧检验序列：发送和接收算法两者都使用循环冗余检验（CRC）来产生 FCS 字段的 CRC 值。

3、介质访问控制方法

IEEE802.3 标准提供了介质访问控制子层的功能说明，有两个主要的功能：数据封装（发送和接收），完成成帧（帧定界、帧同步）、编址（源和目的地址处理）、差错检测（物理介质传输差错的检测）；介质访问管理，完成介质分配避免冲突和解决争用处理冲突。

七、标记环介质访问控制协议

标记环局域网协议标准包括四个部分：逻辑链路控制 LLC、介质访问控制 MAC、物理层 PHY 和传输介质。

1、IEEE802.5 规定了后面三个部分的标准。LLC 和 MAC 等效于 OSI 的第二层（数据链路层），PHY 相当于 OSI 的第一层（物理层）。LLC 使用 MAC 子层的服务，提供网络层的服务，MAC 控制介质访问，PHY 负责和物理介质接口。

2、介质访问控制帧结构

标记环有两个基本格式：标记和帧。在 IEEE802.5 中帧的传输是从最高位开始一位一位发送，而 IEEE802.3 和 IEEE802.4 正好相反，帧的传输是从最低位开始一位一位发送的，这一点对于不同协议的局域网互连时要进行转换。

3、介质访问控制方法

（1）帧发送：对环中物理介质的访问系采用沿环传递一个标记的方法来控制。取得标记的站具有发送一帧或一系列帧的机会。

（2）标记发送：在完成帧发送后，该站就要查看本站地址是否在 SA 字段中返回，若未查看到，则该站就发送填充，否则就发送标记。标记发送后，该站仍留在发送状态，起到该站发送的所有的帧从环上移去为止。

（3）帧接收：若帧的类型比特表示为 MAC 帧，则控制比特由环上所有的站进行解释。如果帧的 DA 字段与站的单地址、相关组地址或广播地址匹配，则把 FC、DA、SA、INFO 以及 FS 字段拷贝入接收缓冲区中，并随后转送至适当子层。

（4）优先权操作：访问控制字段中的优先权比特 PPP 和预约比特 RRR 配合工作，使环中服务优先权与环上准备发送的 PDU 最高优先级匹配。

八、快速以太网

1、快速以太网的类型

快速以太网（Fast Ethernet）是一个新的 IEEE 局域网标准，于 1995 年由原来制定的以太网标准的 IEEE802.3 工作组完成。快速以太网正式名为 100Base-T。

共享介质快速以太网和传统以太网采用同样的介质访问控制协议 CSMA/CD 所有的介质访问控制算法不变，只是将有关的时间参量加速 10 倍。

快速以太网的三种标准：100Base-4、100Base-TX、100Base-FX

快速以太网的产品：

适配器：一边是总线结构，将数据传送至主机、中继器或 HUB；另一边接到所选的介质，可以是双绞线、光纤，或者是一个介质独立接口 MII，MII 是用来连接外部收发器用的，其功能类似于以太网的 AUI。

HUB：可分为共享机制的中继器和交换机制的交换器。

九、基于交换技术的网络

1、交换网结构

交换技术的两种主要应用形式是：折叠式主干网和高速服务器联接。

2、全双工以太网

全双工运行在交换器之间，以及交换器和服务器之间，是和交换器一起工作的链路特性，它使数据流在链路中同时两个方向流动，不是所有收发器都支持它的全双工功能。

3、在下列情况下全双工最有用：

（1）在服务器和交换器之间。这是目前全双工应用最普遍的配置。

（2）在两个交换器之间。

（3）在远离的两个交换器之间。

3、多媒体

多媒体的应用基于 MPEG、JPEG、H.261 等视频压缩算法。

缺点：是由网络缓存产生的延迟，一方面为了平滑抖动数据要插入足够的缓存，另一方面缓存又不能太大，以至引起无法接受的视频延迟。

对视频应用的低延迟需求有四种解决方案：（1）采用 10Mbps 交换器（2）采用 100Mbps 中继器（3）用 100Mbps 的交换器（4）采用流控技术

4、千兆位以太网

千兆位以太网也有铜线及光缆两种标准。

铜线标准 1000Base-CX，最大传输距离，25 英尺，并需用 150 欧姆的屏蔽双绞线 STP，

光缆标准 1000Base-SX，850nm 的短波长，300m 传输距离。

1000Base-LX，1300nm 的波长，550m 传输距离。

十、ATM 局域网

十一、无线局域网

1、IEEE802.11 体系结构

无线 LAN 最小构成模块是基本服务集 BSS，它由一些运行相同 MAC 协议和争用同一共享介质的站点组成。一个扩展服务集 ESS 由两个或更多的通过分布系统互连的 BSS 组成。

2、基于移动性，无线 LAN 定义了三种站点：

（1）不迁移，这种站点的位置是固定的或者只是在某一个 BSS 的通信站点的通信范围内移动。

（2）BSS 迁移，站点从某个 ESS 的 BSS 迁移到同一个 ESS 的另一个 BSS。如果进行数据传输，就需要具备寻址功能以便识别站点的新位置。

（3）ESS 迁移，站点从某个 ESS 的 BSS 迁移到另一个 ESS 的 BSS。服受到破坏。

3、物理介质规范

（1）红外线：数据率为 1Mbps 或 2Mbps，波长在 850nm 和 950nm 之间。

（2）直接序列扩展频谱：运行在 2.4GHzISM 频带。最多有 7 个通道，每个通道的数据率为 1Mbps 或 2Mbps。

（3）频率跳动扩展频谱：运行在 2.4GHzISM 频带，在研究之中。

4、介质访问控制

IEEE802.11 形成的一个 MAC 算法称为 DFWMAC 分布式基础无线 MAC，它提供分布式访问

控制机制，处于其上的是一个任选的中央访问控制协议。

（1）在 MAC 层的靠下面是的分布式协调功能子层 DCF，采用争用算法，为所有通信提供访问控制，一般异步通信采用 DCF。

（2）在 MAC 层的靠上面是点协调功能 PCF，采用中央 MAC 算法，提供无争用服务。

5、分布协议功能

DCF 子层采用简单的 CSMA 算法。DCF 没有冲突检测功能，为了保证算法的顺利和公平，采用了一系列的延迟，相当于一种优先权机制。首先考虑称为帧间空隙 IFS 的简单延迟。

十二、城域网

城域网是在 5Km-100Km 的地理覆盖范围内，以高的传输速率充分支持数据、声音和图像综合业务传输的一种通信结构网络。它以光纤为主要传输介质，其传输率为 100Mbps 或更高。IEEE802.6 分布式队列双总线 DQDB 为城域网的标准。

第 6 章广域网技术

主要内容：1、公共交换电话网 PSTN

2、综合业务数字网 ISDN

3、分组交换网 X.25

4、帧中继网 FR

5、异步转移模式网 ATM

6、数字数据网 DDN

7、移动通信及卫星通信网 GSM

8、线缆调制解调器 Cable Modem

9、数字用户线 XDSL

一、电话网

公用交换电话网 PSTN 是向公众提供电话通信服务的一种通信网。电话通信网主要提供电话通信服务，同时还可提供非话音的数据通信服务。

1、计算机交换分机 CBX

采用数字电话：可以建立综合声音/数据工作站

分布式结构：具有分布智能的多级或网关结构的多路形状的可靠性提高。

非阻塞结构：所有电话和设备都有专门的指定端口。

CBX 的结构：核心是某种数字开关网络。开关负责对数字信号流进行操作和交换，数字开关网络由某些空分和时分交换级组成。接到形状的是一级接口单元，通过接口单元访问外界或外界可访问接口单元。通常接口单元完成同步时分多路复用功能，以适应多个输入线。另一方面，为了达到全双工操作，单元要用两条线与开关相连。

二、点到点通信

1、点到点的通信主要适用于两种情况：（1）是成千上万组织有各种局域网，每个局域网含有多众多主机和一些联网设备以及连接至外部的路由器，通过点到点的租线和远地路由器相连；（2）是成千上万用户在家里使用调制解调器和拨号电话线连接到 internet，这是点到点连接的最主要应用。

2、串行 IP 协议（SLIP）

SLIP 是 1984 年制定的，协议文本描述为 RFC1055。

工作过程：当工作站发送 IP 分组时，在帧的末尾带一个专门的标志字节（0XC0），如果在 IP 分组中含有同样的标志字节，则加两个填充字节（0XDB、0XDC）于后，如果 IP 分组中含有 0XDB，则加同样的填充字节。

存在的问题：（1）这种协议无任何检错和纠错功能；（2）只支持 IP 分组；（3）每一方需要知道另一方面的 IP 地址，且在设置是不能动态赋给 IP 地址；（4）不提供任何的身份验证；

（5）未被接受为 internet 标准。

3、点对点协议（PPP）

PPP 由 internet IETF 成立了一个组来制定的数据链路，描述于 RFC1661。

主要功能：成帧的方法可清楚地区分帧的结束和下一帧起始，帧格式还处理差错检测；链路控制协议 LCP 用于启动线路、测试、任选功能的协商以及关闭连接；网络层任选功能的协商方法独立于使用的网络层协议，因此可适用于不同的网络控制协议 NCP。

工作过程：（1）PC 通过调制解调器呼叫 ISP 路由器，然后路由器一边的调制解调器响应电话呼叫，建立一个物理连接。（2）接着 PC 对路由器发送一系列的 LCP 分组，用这些分组以及其响应来选择所用的 PPP 参数。（3）当双方协商一致后，PC 发送一系列的 NCP 分组以配置网络层（NCP 的功能就是动态分配 IP 地址）PC 就成为一个 internet 主机，可以发送和接收 IP 分组。（4）当 PC 用户完成发送、接收功能后不需要再联网时 NCP 用来断开网络层连接，并且释放 IP 地址，然后 LCP 断开链路层连接。（5）最后 PC 通知调制解调器断开电话，释放物理层连接。

三、综合业务数字网 ISDN

综合业务数字网 ISDN 是由国际电报电话咨询委员会 CCITT 和各国标准化组织开发的一组标准，这些标准将决定用户设备到全局网络的联接，使之能方便地用数字形式处理声音、数据和图像通信。ISDN 提供了各种服务访问，提供开放的标准接口，提供端到端的数字连接，用户通过公共通道、端到端的信令实现灵活的智能控制。

1、ISDN 的系统结构

NT1：网络终端设备，不仅起到了接插板的作用，它还包括网络管理、测试、维护和性能监视等。是一个物理层设备。

NT2：是计算机的交换分机 CBX，NT1 和 NT2 连接，并对各种得以和、终端以及其他设备提供真正的接口。

CCITT 为 ISDN 定义了四个参考点：R、S、T、U。U 参考点连接 ISDN 交换系统和 NT1，目前采用两线的铜的双绞线；T 参考点是 NT1 上提供给用户的连接器；S 参考点是 ISDN 和 CBX 和 ISDN 终端的接口；R 参考点是连接终端适配器和非 ISDN 终端；R 参考点使用很多不同的接口。

2、ISDN 的功能：线路交换、分组交换、公共通道信令、网络操作和管理数据库以及信息处理和存储功能。

（1）线路交换支持实时通信和大量信息传输，速率为 64Kbps，ISDN 环境中，线路交换连接由公共通道信令技术控制。

（2）分组交换支持像交互数据应用那样的猝发通信特性，速率为 64Kbps。

（3）公共通信令用于建立、管理和释放线路交换连接，CCITT 公共通信令系统 CCSSNO.7 用来交换信令。

3、ISDN 定义交换设备和用户设备之间的两种数字位通道接口

基本速率接口 BRI：2B+D，两个传输声音和数据的 64 Kbps 的 B 通道和一个传输控制信号和数据 16 Kbps 分组交换数据通道 D 通道。144Kbps

一次群速率接口 PRI：23B+D 或者 30B+D，在北美日本，欧洲国家使用

ISDN 公用了公共通信信令技术，以实现用户网络访问和信息交换。允许使用公共通道信令通路来控制多个线路交换连接。

4、ISDN 协议参考模型

ISDN 参考模型与 ISO/OSI 参考区别在于多通道访问接口结构以及公共通道信令，它包括了多种通信模式和能力：在公共通道信令控制下的线路交换连接，在 B 通道和 D 通道上的分组交换通信，用户和网络设备之间的信令、用户之间的端到端的信令，在公共信令控制下

同时实现多种模式的通信。

用于线路交换的 ISDN 网络结构笔协议，它包括 B 通道和 D 通道。B 通道透明地传送用户信息，用户可用任何协议实现端到端通信；D 通道在用户和网络间交换控制信息，用于呼叫建立、拆除和访问网络设备。D 通道上用户与 ISDN 间的接口由三层组成：物理层、数据链路层 LAP-D、CCSSNO.7。

用于低速分组交换的 ISDN 网络结构和及协议。它使用 D 通道，本地用户接口只需要执行物理层功能，作用如同 x.25 的 DCE。

四、分组交换网

1、分组交换网工作原理

公共分组交换网 PSDN 已经成为广域网中的重要传输系统。分组交换是一种在距离相隔较远的工作站点之间进行大容量数据传输的有效方法，它结合线路交换和报文交换的优点，将信息分成较小的分组进行存储、转发，动态分配线路的带宽。

优点：出错少、线路利用率高。工作方式：数据报，虚电路。

主要特性：由于建立和拆除虚电路的呼叫控制分组和数据分组在同一通道和同一虚电路上传输，其结果是占用了通道频带；虚电路的复用发生在第三层；第二层和第三层都需要流控和差错控制机制。

2、公共数据网（CCITT X.25 网）

X.25 实际上包括相关的一组协议：X.3、X.28、X.29、X.75 协议等。

X.25 描述了将一个分组终端连接到一个分组网络上所需要做的工作。通过虚电路它能负责维护一个通过单一物理连接的多用户会话，每个用户会话被分配一个逻辑信道。提供了高优先级类型和正常优先级类型。

X.25 网络与计算机之间的接口一般是通过专用设备或网关、路由器来解决的。

X.3 描述了一个 X.25 PAD 的功能和控制参数；X.28 定义了一台终端与 X.25 PAD 之间的交互作用，为每个用户提供了一个常规的 X.25 网络连接；X.29 定义了一台主机和其相连的 PAD 之间的交互作用。

X.25 互连方案：(1)采用路由器和网关同时联接 x.25 和本地局域网，这种方案适合规模较大、多种协议共存的网络；(2)采用一台微机作为路由器，安装相应的 x.25 网卡和路由软件，使用于中小规模且协议比较小的网络；(3)使用 PAD 机，这种方案只适合 x.25 协议的环境，与远程其他协议的网络互连受到限制。

3、X.25 分层协议

X.25 分层：物理层、数据链路层、分组层，这三层对应于 OSI 模型的最底下三层。

（1）物理层：涉及站点与把这个站边到分组交换网的链路之间的新产品。其标准 X.21。

（2）链路层：所用的标准 LAP-B，是 HDLC 的一个子集。

（3）分组层：提供外部虚电路服务。

三层之间的关系：用户数据被送到 X.25 第三层，在第三层加上含有控制信息的报头，从而组成了一个分组。控制信息用于协议的操作。整个 X.25 分组然后送到 LAP-B 实体，LAP-B 在此分组的前后各加上控制信息组成一个 LAP-B 帧，在帧中加入控制信息也是为了协议的操作。

4、虚电路服务

X.25 的分组层提供虚电路服务，数据以分组形式通过外部虚电路传输。虚电路有两类型：呼叫虚电路，是通过呼叫建立和呼叫清除等过程动态地建立起来的虚电路；永久虚电路则是固定的虚电路。

虚电路实现的过程：

5、X.25 的分组格式

用户数据被分成多个块，每个块加上 24 位或 32 位的报头形成数据分组。

报头含有 12 位的虚电路号，其中 4 位号为组号，8 位为通道号。

P（S）、P（R）用于流控和差错控制。M 位和 D 位可用于流控和差错控制也可用于 X.25 完全分组序列。

五、帧中继网

帧中继网是由 X.25 分组交换技术演进而来的，由于光纤通信的误码率低，为了提高网络速率，活动了很多在 X.25 分组交换中的纠错功能，使帧中继的性能优于 X.25 分组交换的性能。

1、帧中继的主要特点：中速到高速的数据接口；标准速率为 DS1，即 T1 速率 1.544Mbps；可用于专用和公共网；仅传输数据；使用可变长度分组。

2、帧中继网与 X.25 网比较

载送呼叫控制信令的逻辑连接和用户数据是分开的。因此中间节点毋需为每个连接的呼叫控制保持状态表；逻辑连接的复用和交换发生在第二层，而不是在第三层，从而减少了处理的层次；结点到结点之间毋需流控和差错控制，由高层负责端到端的流控和差错控制。

3、帧中继的优点：精简了通信处理。协议对用户-网络接口以及网络内部处理的功能降低了，从而得到了低延迟和高吞吐率的性能。

4、帧中继在 H 信道上的应用：大信息量的交互数据应用；大的文件传送；低数据率的多路复用；字符交互通信。

5、帧中继的协议结构

协议有两个分开的操作平台：（1）控制平台（C），它涉及逻辑连接的建立和终止。（2）平台是用户平台（U），负责用户之间的数据传输。

用户与网络之间的是控制平台，而端到端之间则是用户平台协议。

控制平台：帧模式传输服务的控制平台类似于分组交换服务中用于公共通道信号的控制平台。其中，控制信号使用一个单独的逻辑通道。链路层用 LAP-D（Q.921）提供可靠的数据链路控制服务，在 D 通道的用户（TE）和网络（NT）之间进行流控和差错控制。数据链路服务用于交换 Q.933 控制信号报文。

用户平台：用户之间传输信息的用户平台协议是 LAP-F 由 Q.922（是 LAP-D Q.921 的增强版本）定义。

6、LAP-D 的核心功能

（1）帧的定界，组合和透明性；（2）帧的多路复用/多路分解；（3）对帆进行检查以保证在零位手稿前以及零位剔除后，帧的长度是字节的整数倍；（4）对帧进行检查以保证其长度符合要求；（5）检测传输差错；（6）冲突控制功能（LAP-F 新增功能）。

7、帧中继的呼叫控制

呼叫控制方案选择：

（1）交换访问（Switched Access）在用户连接到交换网络，而本地交换不提供帧处理功能，在这种情况下，必须提供从用户的终端设备到网络帧处理器的交换访问。

（2）集成访问（Intergraded Access）用户接到帧中继网络或者交换网络，其中的本地交换提供帧处理功能，因为用户能对帧处理器进行直接逻辑访问。

帧中继和 X.25 一样支持在一个链路上利用多个连接，称为数据链路连接，每个连接都有一个惟一的数据链路连接标识 DLCI。其数据传输涉及的步骤如下：（1）在两个端点之间建立逻辑连接，并指定惟一的数据链路标识 DLCI 的值；（2）交换数据帧；（3）释放逻辑连接。

呼叫控制逻辑连接的 DLCI=0，其帧的信息域中包含有呼叫控制报文，至少需要四种报文类型：建立 （setup）、连接（connect）、释放（release）、和释放完成（release complete）。

8、用户数据传输

LAP-F 帧格式类似于 LAP-D 和 LAP-B，但有一个明显的差别，即没有控制域。即意味着：（1）只有一种帧的类型，即用户数据帧，没有控制帧。（2）不可能用 inband 信号。逻辑连接只能用于传输用户数据。（3）不可能进行流控和差错控制，因为没有顺序号。

六、ATM 网

1、ATM 协议参考模型

用户面：提供用户信息的传输。控制面：负责呼叫控制和连接控制功能。管理面：负责网络维护和完成运行功能。面管理：执行与整个系统有关的管理功能。层管理：处理的运行和维护功能。

物理层：主要是传输信息；ATM 层：主要完成交换、路由及多路复用；ATM 适配层 AAL：主要负责与较高层信息的匹配。

（1）、物理层：由两个子层组成，物理介质子层和传输汇聚子层。

物理介质子层支持纯粹与介质有关的位功能。传输汇聚子层把 ATM 信元流转换成在物理介质上传输的位，如把帧匹配成在传输系统中所用的格式（SDH、PDH、基于信元的格式）、信元定界等功能。

（2）、ATM 层：基本功能是负责生成信元，它不管载体的内容，且与服务无关。主要功能有多路复用、多路复用分解、信元 VPI、VCI 的转换，信元头的产生和去除，流控。

（3）、ATM 适配层：由两个子层组成，分段和重组子层（SAR），把高一层的信息单位分段成 ATM 信元，或者把 ATM 信元重组成高一层的信息单位；汇聚子层（CS）与服务有关，可以完成的功能有信报标识和时钟恢复等。

信元类型

（1）空信元（物理层）：为了使信元流的速率与传输系统可用 的有效负载容量相匹配而在物理层插入或除去的信元。

（2）有效信元：没有头差错的信元或已经由头差错控制进程修正过的信元。

（3）无效信元（物理层）：有头差错且尚未由头差错控制进程修正的信元。

（4）指定的信元（ATM 层）：使用 ATM 层服务为应用提供服务的信元。

（5）非指定的信元（ATM 层）：尚未指定的信元

2、ATM 层

信元结构：字节是按递增顺序发送，从第一个字节开始，字节中的位是按递减顺序发送，从第 8 位开始。

GFC 总流控；PT 有效载荷类型,；CLP 信元丢失优先权；HEC 信元头差错控制。

ATM 层原语

ATM-DATA-REQUEST：AAL 请求把与此原主相关的 ATM-SDU 传送给它的对等实体。

ATM-DATA-INDICATION：指示 AAL 与原语相关的 ATM-SDU 可用。

3、ATM 物理层

传输汇聚子层（1）信元头保护机制，所生成的多项式 X8+X2+X+1（2）信元定界机制，有搜索、预同步和同步三个状态。（3）混杂，这是一种附加机制，用来对付恶意用户和假冒，采用 X43+1 的自同步混杂器随机处理，信元头并没有被混杂。（4）信元去耦，信元的数据率应低于可用的传输容量。（5）与传输系统的匹配。

物理介质子层：提供位传输能力，传输功能与所用的介质有关，这些功能包括线路编码、再生、均衡、电光转换。

物理层原语

PH-DATA-REQUEST：ATM 层请求把与原主有关的 SDU 传送给它的对等实体。

PH-DATA-INDICATION：指示与原主有关的 SDU 可用。

4、ATM 适配层

AAL 服务分类：A 类线路仿真 AAL1 类型，B 类 VBR 视频 AAL2 类型，C 类文件传送 AAL5 类型，D 类无连接信报 ALL3/4 类型。

AAL 的子层包括：汇聚子层 CS 和分段和重组子层 SAR。

CS 负责来自用户面的信息单元作分段准备，以使这些分组再重组成原始状态。主要功能是在 AAL－SAP 提供 AAL 服务。

SAR 将来自汇聚子层的信元分段成 48 字节的载体，或把来自 ATM 层的信元信息域内容组装成高层信息单位。

七、数据数据网 DDN

1、数字数据网 DDN 是一种利用数字信道提供半永久连接专用电路，传输以数据信号为主的数字传输网络。

2、我国 DDN 提供 2.4Kbps－2.408Mbps 的中高速率的点到点和点到多点的专用电路，用户到用户传输差错率优于 10－6

3、DDN 组成：由本地传输系统、复用及交叉连接系统、局间传输及同步系统、网络管理系统等四部分组成。

4、按组建、运营、管理维护的责任和地理区域来划分网络地域等级，可分为三级：本地网、一级干线网、二级干线网。按层次功能也可分三级：核心层、接入层、用户接入层。

八、移动通信

1、移动通信网组成：移动通信交换 MTX、基地站 BS、移动台 MS 和局间和局站的中继线组成。移动台和基地站、移动台和转动台之间采用无线传输方式。基地站与移动通信交换局，移动通信交换局与有线网 PSTN 之间一般采用有线方式进行信息传输。

2、全球移动通信系统 GSM 是一个完整的数字移动通信标准体系。它是 1982 年欧洲邮电管理委员会 CEPT 开发的第二代数字蜂窝移动系统。

3、GSM 组成：网络子系统 NSS、基站子系统 BSS 和移动台 MS 三部分组成。移动台主要功能除了通过无线接入进入通信网络，完成各种控制和处理以提供主叫或被叫通信，还提供与使用者之间的人机接口或与其他终端设备向连接适配装置等。通过用户身份模块 SIM 卡向通信网络提供了用户注册和管理所需要的信息。

基站子系统包含了 GSM 无线通信部分的所有地面基础设施。分为三个部分：基站控制器 BSC、基站收发信机 BTS 以及操作维护中心 OMC－R

网络子系统由移动交换机 MSC、归属位置寄存器 HLR、访问搁置寄存器 VLR、鉴权中心 AUC、设备识别寄存器 EIR、操作维护中心 OMC－S 和德厚流光息业务中心 SC 组成。

MSC 是对位于它覆盖区域中的 MSC 进行控制和交换话务的功能实体，也是 GSM 网络与其他通信网之间的接口实体，负责整个 MSC 区内的呼叫控制、移动性管理和无线资源管理。

4、无线软件应用协议 WAP

WAP 是以国际互联网上所采用的 HTTP/HTML 协议为基础，针对无线移动通讯的特性建立的通信协议，是对小型显示界面、低功率、小内存、CPU 运算能力低的通讯工具，以及低带宽、延迟大、和较不可靠的无线移动通讯网络进行修改而成的协议。

WAP 采用客户机服务器结构，提供了一个灵活而强大的编程模型。WAP 网关起着协议翻译的作用，是联系移动网与 internet 的桥梁。

WAP 的分层：无线应用环境 WAE 应用层协议、无线会话协议 WSP 会话层协议、无线事务处理协议 WTP 事务处理层协议、无线传输安全协议 WTLS 安全层协议、无线数据报 WDP 传输层协议、无线载体、其他应用和服务

5、个人通信业务/个人通信网

个人通信特征：

九、卫星通信系统

1、按空间轨道位置可分为：静止轨道 GEO 系统、非对地静止轨道 MEO；按照业务提供的范围可分为：全球卫星移动通信和区域卫星移动通信系统。LEO 高度一般为 500Km－1500Km 左右，MEO 高度通常指 5000Km－15000Km 左右，GEO 为 35768Km 高度赤道上空的轨道。

2、卫星通信系统组成：空间分系统、通信地球站、跟踪遥测及指令分系统、监控管理分系统。

3、卫星通信网络的结构主要有两种：星形和网格形。

4、国际电信联盟 ITU 有关空间通信的世界无线电行政会议 WARC 规定了空间使用的频率分配原则。甚高频波段 UHF400/200MHz；L 波段 1.6/1.5GHz 主要用于移动卫星通信、海事卫星业务；C 波段 6.0/4.0GHz，主要用于固定卫星业务和专用卫星业务、VSAT 网络等；X 波段 8.0/7.0GHz，主要用于固定卫星业务；Ku 波段 14.0/11.0GHz，主要用于 VSAT 网络、卫星电视广播、移动卫星通信等；Ka 波段 30.0/20.0GHz，主要用于 VSAT 网络、卫星电视广播。

十、Cable Modem 线缆调制解调器

Cable Modem 通过使用与传送有线电视一样的同轴电缆实现了双向和高速的数据传输。

1、工作方式：

与电话调制解调器类似，Cable Modem 对于数据信号进行调制和解调。但是，Cable Modem 包括了许多当今高速互联网业务而设计的功能。数据从网络到用户的传输称为"下流"，数据从用户到网络的传输称为"上流"。从用户的角度看，Cable Modem 是一个 64/256 正交调幅 QAM 射频 RF 接收器，它能够在一个 6MHz 电缆信道中以 30 到 40Mbit/s 的速率传送数据。在一个局域网内一个 Cable Modem 可以被 16 个用户共享。

2、Cable Modem 和 OSI 模型

（1）物理层：分为下传流和上传流

下传数据流的信道是基于北美数字视频规范的包括以下特性：

64 和 256 正交调幅 QAM；在电缆路线中与其他信号共同占用 6MHz 的频宽；可变长度的交叉支持，同时包括延时敏感和延时非敏感的数据业务；连续的串行比特流，没有默认的帧，提供物理层和介质访问控制层 MAC 的完全分离

上传数据流信道是一个共享的信道，包括以下特性：

QPSK 和 16QAM 格式；数据速率从 320Kbit/s 到 10Mbit/s；在 CMTS 控制下的灵活且可编程的 Cable Modem；时分多种复用访问；支持固定长度的帧和可变长度的协议数据单元 PDU。

数据链路层：MCNS MAC（MPEG 帧）、IEEE802.2

十一、数字用户线

数字用户线 DSL 是一项调制解调器技术，它利用现有的双绞电话线传输高带宽数据来为用户提供服务。

术语 XDSL 涵盖了许多类似但相互竞争的 DSL 形式，包括非对称的 DSL（ADSL），单线 DSL（SDSL）和高数据速率 DSL（HDSL）、自适应速率 DSL（RADSL）以及甚高速 DSL（VDSL）。

1、 非对称数字用户线 ADSL

它提供了下行带宽（从 NSP 的交换局到客户地点）比上行带宽（从客户地点到交换局）更宽。ADSL 能以高于 6Mbps/s 的速率向用户传输数据，并且能够以高于 640Kbit/s 的速率在两个方面上同时传输数据。

2、ADSL 业务结构

组成：由用户终端设备 CPE 和位于 ADSL 接入点 POP 的支持设备组成。网络接入提供商 NAP 负责管理第二层的网络核心部分，而网络服务提供商 NSP 负责管理第三层的网络核心部分。

对向 subtending：可以把若干 DSL 接入复用器 DSLAMs 连接到一起以提高 ATM 管道的利

用率。DSL 接入复用器 DSLAMs 在本地相互连接或通过交换局 CO 连接到本地接入集中点 LAC，LAC 能提供 ATM 业务疏导、PPP 隧道以及访问本地内容或缓存内容的第三层终结。

3、ADSL 技术

ADSL 依靠先进的数字信号处理技术和创造性的算法，把大量的信息压缩到双绞电话线进行传输。

第 7 章网络互连技术

主要内容：1、局域网互连

2、网络互连原理

3、无连接网络互连、各种路由选择算法和协议

4、核心路由器体系结构体系

一、局域网互连

1、网络互连的目的：是将多个网络互相连接，以实现在更大范围内的信息交换资源共享和协同工作。

2、局域网互连方式：从距离上分有本地局域网互连和远程局域网互连即 LAN-LAN 和 LAN-WAN-LAN；从互连所采用的介质区分，有同轴细缆或粗缆(coaxial cable)、各类非屏蔽双绞线 UTP(Unshielded Twisted pair)和屏蔽双绞线 STP(shielded Twisted pair)、单模或多模光纤等(optical fiber)连接方式。

3、局域网互连划分：

物理层(中继器 repeater)：使用中继器在不同电缆段之间复制位信号，工作在 OSI 物理层，互连同类型网段，只起到放大信号的作用，驱动长距离通信。又称集线器(hub)，可分为普通型，可叠加组合型和高档智能型。

网桥(bridge)：使用网桥在局域网之间存储、转发帧，工作在 OSI 数据链路层，更准确地说应该位于 MAC 层，它互连兼容地址的局域网，利用同 MAC 和 MAC 地址，以及存储、转发功能进行局域网间的信息交换。从应用上分本地网桥和远程网桥、主干网桥；从帧转发功能分配分透明网桥和源地址路径选择网桥。透明网桥 TB 的基本功能有学习及过滤、帧转发和分枝树算法功能。

(1)网桥作信息帧转发时要利用地址转发表，按表中学习到的 MAC 地址和网桥对应关系，将包准确转发到该网桥。但如网桥未学习到 MAC 地址时，便将帧发向除接收口之外的所有接口，这在网桥刚启动工作时会造成　　大量的广播帧，称为广播风暴(broadcast storm)。

(2)扩展树协议是为了克服由于网桥不具网络层功能，在常任冗余路径的网桥中出现信息回路造成网桥瘫痪的问题。IEE802.1 定义了分枝树协议 STP，将整个网络路由定义为无回路的树形结构。

(3)源地址路径选择网桥 SRB 主要用于标记环 IEEE802.5 标记环局域网。互连不同型局域网时使用封装网桥(encapsulation bridging)和转换桥接方式(translation bridging)和源地址路径选择透明网桥 SRT。

路由器(router)：使用路由器在不同网络间存储、转发分组，工作在 OSI 网络层，它需要处理网络层的数据分组或网络地址，决定数据分组的转发，它要决定网桥中信息通信的完整路由。

网关(gateway)：使用协议转换器提供高层接口，工作在应用层。

二、网络互连原理

1、网络互连的要求：在网络之间提供一条链路，至少需要一条物理和链路控制的链路；在不同网络的进程间提供路径选择和传递数据；提供各用户使用网络的记录和保持状态信息；在提供上述服务时不需要修改原有各网络的网络结构。

2、网络互连的功能分类：基本功能，指的是网络互连必须的功能，即使对那些类型相同的网络互连也应该具备的功能，它包括不同网络之间传送寻址和路径选择等。扩展功能，指的是当各种互连的网络提供不同的服务级别时所需要的功能，包括协议转换、分组的分段组合和重定序及差错检测。3、面向连接运行模式：连到同一子网上的两个 DTE 之间可建立一条逻辑的网络连接。4、无连接运行模式：对应于分组交换网的数据报机制，而面向连接运行对应于虚电路机制。

三、无连接网络互连

1、IP 提供无连接或数据报服务优点：无连接互连网络设备灵活性较好，对子网要求低；无连接网络能提供强健的服务；无连接网络服务对于无连接传输层协议最为适用。

2、无连接网络互连设计主要问题：路由、数据报生命周期，分段和重组，纠错和流控。

重组：一种重组的方法是在目的站进行重组，其缺点是分成小段的数据通过网络胆识的效率。另一种重组方法是由中间的路由器进行重组，则也会下列问题：路由器需要大容量缓冲器，还可能发生缓冲器不够用的情况；一个数据报的所有分段必须使用同一路由，限制了动态路由的使用。

IP 数据报报头中，包含下列内容：数据单元标识(ID)，数据长度，偏移(offset)，还有标识(more flag)。路由器中 IP 分段的功能：offset=0 是整个数据的开始，more-flag=0 是整个数据报的结束。

（1）建立两个新的数据报，它们的头部就是原先数据报的头报

（2）以 64 位为边界，把原先的数据报分成长度差不多的两部分，把它们分别放入新的数据报中。第一部分必须是 64 位的倍数。

（3）把第一个新数据报的长度设置为所插入的数据，把 more-flag 设置成 1，offset 不变。

（4）把第二个新数据报的长度设置为所插入的数据，把 more-flag 设置成 0，offset 设置成第一部分数据长度除以 8。

生命周期：一种是对来到的第一段设置一个生命周期，如果在生命周期内没有完成重级工作，那么就撤销已经到达的分段；第二种是利用数据报的生命周期，它包含在每一段的头部中，若重组工作没有在数据报生命周期内完成，则撤销接收到的分段。

四、IP 数据报的路由选择

1、直接传送和间接传送

直接传送将一个数据报从一台机器经过单个物理网络直接传送至目的站点，这是所有 internet 通信的基础。只有当两台机器连在同一底层物理传输系统时，才能采用直接传送方式。否则只能用间接传送方式，发送方将数据发送给一个路由器再传送。

2、IP 路由选择表

路由表存储各个目的站点以及如何到达目的站点的信息。为了尽可能使用最少的信息进行路由选择，采用信息隐蔽原则。

路由表的选择表的大小仅取决于互联网中网络的数量，与连到网上的主机的数量无关。IP 路由选择软件仅需要维护有关目的网络地址的信息，而与主机地址的信息无关。

保持路由表尽可能小的技术是把多个表项统一到一个默认的情况。

3、ICMP 差错与控制报文协议

（1）为了使互联网中的路由器报告差错或提供有关意外的情况信息，在 TCP/IP 中设计了一个特殊用的报文机制，称 internet 控制报文协议 ICMP，它是 IP 的一部分。

（2）ICMP 机制：ICMP 报文放在一个 IP 数据报的数据部分中通过互联网。允许路由器向其他路由器或主机发送差错或控制报文。ICMP 是一个差错报告机制，它为发生差错的路由器提供了向初始源站点报告差错的方法。

（3）ICMP 报文格式：由三个字段组成，即一个 8 位整数的报文类型字段用来标识报文、一个 8 位代码字段提供有关报文类型的进一步信息、以及一个 16 位校验和字段。

（4）ICMP 报文类型：回送请求/应答报文(回送请求/应答、时间戳请求/应答、地址请求/应答)，差错报告(包括主机不可达报告、超时报告、参数出错报告)，控制报文(源抑制报文、重定向报文)。

五、路由选择算法

1、距离矢量路由选择 V-D，

2、链路状态路由选择或称最短路径优先算法(SPF)，要求每个参与的路由器都要具有完全的拓扑结构，只需要完成两项任务：负责检测所有相邻路由器状态；周期地向其他路由器传递链路状态信息。其优点：每个路由器用相同的原始状态数据独立地计算路由，并不依赖于中间的机器。

六、内部网关协议

在一个自治系统内的两个路由器彼此互为内部路由器，使用内部网关协议(IGP)，自治系统之间的使用外部网关协议(EGP)来通信。

1、路由选择信息协议(RIP)采用 V-D 算法，距离矢量路由选择算法，分成主动和被动两类，只有路由器工作在主动模式，主机必须使用被动模式。工作在主动模式的路由器进行监听，并根据收到的通知更新其路由。以主动方式运行 RIP 的路由器每间隔 30 秒广播一次报文。

RIP 对点到点连接和广播型网络两者都提供支持。RIP 分组是通过 UDP 和 IP 传输的。RIP 进程使用 UDP 的 520 端口来进行发送和接收。

RIP 报文格式：报头 32 位，命令字为 1 表示请求部分的或全部的路由选择信息。命令字为 2 表示响应，包含发送方路由选择表内的网络地址和距离值一对信息。

2、IGRP，运行频率比较低，每 90 秒更新；路由更新的每一项都包含一个四种度量制式，即延迟、带宽、可靠性、负载；采用保守式预防环路的保护措施、选择多路径路由以及处理默认路由器的手段等。

3、开放最短路径优先协议 OSPF

优点：计算迅速，无环路的收敛性；支持精确的度量值，也能支持多重度量制式；支持通往一个目的站点的多重路径；能区分不同的外部路由。是基于链路状态路由选择算法 SPF。

OSPF 报文报头格式：24 个 8 位组报头，共有五种类型的报文类型，类型 1）hello；2）拓扑结构的数据库描述；3）链路状态请求；4）链路状态更新；5）链路状态确认。

Hello 报文的两种功能：检测链路状态是否可用；在广播型与非广播型网络上选择指定网络路由器及后备。

七、外部网关协议

1、两个交换路由选择信息的路由器若分别属于两个自治系统，则称为外部邻站。外部邻站使用的向其他自治系统通知可达的信息的协议称为外部网关协议(EGP)

2、EGP 有三种功能：它支持邻站猎取机制，允许一个路由器请求另一个路由器同意交换可达信息；路由器持续地测试其邻站是否有响应；EGP 邻站周期地传送路由更新报文来交换网络可达的信息。

3、EGP 定义了 9 种报文类型，它允许两种测试邻站是否存活的方式：一种是主动方式，路由器周期地发送 hello 报文和轮询报文，并等待邻站响应。另一种被动方式，路由器依靠邻站向其发送 hello 报文和轮询报文，并利用可达报文的状态字段信息来判断邻站是否知道其存活。

第 8 章网络操作系统

主要内容：1、网络操作系统的功能

2、流行的网络操作系统

一、网络操作系统的功能

1、网络操作系统 NOS，是使网络上各计算机能方便而有效地共享网络资源，为网络用户提供所需要的各种服务的软件和有关规程的集合。

2、局域网 NOS 有两个基本要求：（1）允许在局域网上的资源被共享；（2）要使现有的 PC 操作系统仍能继续运行，而不需要作任何改变。NOS 有两个组成，主要是控制服务器的操作、管理存储在服务器上的文件。第二个组成，运行在客户系统的软件，使客户能访问网络及网上资源。

3、在 NetWare 中：第一部分是 PC 和网络接口卡联系的机制，采用 IPX/SPX 互连网分组交换/顺序分组交换接口协议来进行通信；第二部分称为解释器或重定向器(redirector)。

二、NetWare 系列

1、NetWare 有两部分组成：NetWare 的外层(shell)和 NetWare 核心组成。

2、NetWare 的外层(shell)在 NetWare4 中称为 DOS Requester。它有两个相关的功能：将应用和桌面操作系统连接，决定将来自应用的命令传送到本地操作系统；和网络接口卡 NIC 通信，使命令和数据包装成能在诸如以太网、标记环网等标准网络上接收和发送。

3、NetWare 首次将容错引入 NOS，称为系统容错(SFT system fault tolerant)

4、NetWare 结构中 NetWare 支持传输层协议自主性的两个重要组成，为开放数据链路层接口 ODI 和 Streams 模块。ODI 为多种传输层协议提供了一种标准的接口，其功能是使多种传输层协议可以共享同一个网络卡而不发生冲突。Streams 模块在高层提供了一个接口，一方面为其底层那些需要向 NetWare 传送数据请求的协议提供一个通用接口，另一方面还要向上为 NetWare 本身提供一个接口。

5、NetWare 工作站利用 shell 和 IPX/SPX 通信协议与文件服务器通信。

NETX．COM 通过向 IPX 发送命令，将 DOS 的文件请求发送到文件服务器在，或从文件服务器上传回重定向。

NET．COM 程序将工作站的请求传送给 DOS 和 NetWare。

IPX．COM 向文件服务器发送网络信息，它是工作站与服务器通信的规程。

三、Windows NT

1、Windows NT 服务器被优化成一个文件、打印机和应用程序服务器在，同时又能处理从小型的工作组到企业网络范围内的各种事务。

2、Windows NT Server 优点：服务器性能，在完全版本中支持达 4 个 CPU，OEM 已经实现了对称多处理环境中支持达 32 个 CPU；256 个 RAS 入站接入；磁盘容错支持，RAID 级的数据保护；IIS 服务；管理向导；苹果机客户的支持；其他网络服务(DHCP、DNS、WINS)；Windows NT 目录服务。

3、Microsoft 网络包括：Windows NT、Windows95、Windows for Workgroup、LAN manager

4、Windows NT 网络结构：包括 I/O 管理器组件、NDIS 兼容网卡驱动程序、NDIS4.0，传输协议、传输驱动程序接口 TDI、文件系统驱动程序。

第 9 章 网络管理

主要内容：1、局域网管理技术

2、网络管理功能和协议

3、网络管理系统

4、网络日常管理和维护

一、局域网管理技术

网络管理是对计算机网络的配置、运行状态和计费等进行的管理。它提供了监控、协调和测试各种网络资源以及网络运行善的手段，还可提供安全管理和计费等功能。

1、网络管理包括三个方面：

(1)了解网络：识别网络对象的硬件情况、差别局域网的拓扑结构、确定网络的互连、确定用户负载和定位。

(2)网络运行：配置网络，选择网络协议是配置网络的重要组成部分；配置网络服务器；网络安全控制。

(3)网络维护：主要包括故障检测与排除，发现故障、追踪故障、排除故障、记录故障的解决方法；网络检查；网络升级，主要包括用户许可证的升级，服务器操作系统升级，服务器的硬件升级。

2、局域网管理工具

NetWare 管理工具：SYSCON 工具

Windows NT 管理工具：服务管理器，性能监视器

二、网络管理功能

1、网络管理的五大功能

配置管理：配置管理的自动获取，在网络设备中自动配置信息中，根据获取手段大致可以分成三类，第一类网络管理协议标准的 MIB 中定义的配置信息；第二类不在网络管理协议标准中有定义，但对设备运行比较重要的配置信息；第三类就是用于管理的一些辅助信息；自动备份及相关技术；配置一致性检查；用户操作记录功能。

性能管理：过滤、归并网络事件，有效地发现、定位网络故障，给出排错建议与排错工具，形成整套的故障发现、告警与处理机制。

故障管理：采集、分析网络对象的性能数据、监测网络对象的性能，对网络线路质量进行分析。

安全管理：结合使用用户认证、访问控制、数据传输、存储的保密与完整性机制，以保障网络管理系统本身的安全。安全管理分三个部分，首先是网络管理本身的安全，其是被管理网络对象的安全。计费管理：

二、网络管理协议

1、IAB 最初制定关于 internet 管理的发展策略，其实采用 SGMP 作为暂时的管理解决方案。后来演变为 SNMP，简单网络管理协议。

2、SNMP 简单网络管理协议在 OSI 的第三层网络层提供的管理服务

优点：与 SNMP 相关的管理信息结构(SMI)和管理信息库(MIB)非常简单，从而能够迅速、简便地实现；　　SNMP 是建立在 SGMP 基础上，而对于 SGMP 从们积累了大量的操作经验。

SNMP 是按照简单和易于实现的原则设计的。

3、CMIS/CMIP 公共管理信息服务和公共管理信息协议：是在 OSI 应用层上提供的网络协议簇，CMIS/CMIP 提供支持一个完整的网络管理方案所需要的功能。

CMIS 提供了应用程序使用的 CMIP 接口，同时还包括两个 ISO 应用协议：联系控制服务元素 ACSE 和远程操作服务元素 ROSE，其中 ACSE 在应用程序之间建立和关闭联系，而 ROSE 则处理应用之间的请求/响应交互。

4、CMOT 公共管理信息服务与协议是在 TCP/IP 协议上实现的 CMIS 服务，这是一个过渡性的解决方案。CMOT 没有直接使用参考模型中表示层实现，而是要求在表示层中使用另外一个协议，轻量表示协议(LPP)，该协议提供了目前最普通的两种传输层协议 TCP 与 UDP 的接口。

5、LMMP 局域网个人管理协议，在 IEEE802 逻辑链路控制 LLC 上的公共管理信息服务与协议 CMOL，它不依赖于任何特定的网络层协议进行网络传输。

三、简单网络管理协议 SNMP

1、SNMP 概述：

设计时围绕四个概念和目标进行设计：保持管理代理的软件成本尽可能低；最大限度地保持远程管理的功能，以便充分利用因特网资源；体系结构必须有扩充的余地；保持 SNMP 独立性，不依赖于具体的计算机、网关和网络传输协议。

提供了四类管理操作：get 操作用来提取特定的网络管理信息；get-next 操作通过遍历活动来提供强大的管理信息提取能力；set 操作用来对管理信息进行控制；trap 用来报告重要的事件。

2、SNMP 管理控制框架与实现

SNMP 定义了管理进程和管理代理之间的关系，这个关系称为共同体。位于网络管理工作站和各网络元素上利用 SNMP 相互通信对网络进行管理的软件统称为 SNMP 应用实体。

SNMP 的应用实体对 internet 管理信息库 MIB 中的管理对象进行操作。SNMP 的报文总是源自每个应用实体，报文中包括访应用实体所在的共同的名字。这种报文称为"有身份标志的报文"，共同体名字是在管理进程和管理代理之间交换管理信息报文时使用。

管理信息报文包括：共同体名，数据。

SNMP 的实现方式:SNMP 在其 MIB 中采用了树状命名方法对每个管理对象实例命名。SNMP 中各种管理信息大多以表格形式存在，一个表格对应一个对象类，每个元素对应于该类的一个对象实例。

3、SNMP 协议是一个异步的请求/响应协议，是一个非面向连接的协议，是一个对称的协议，没有主从关系。SNMP 的设计是基于无连接的用户数据报协议 UDP。四种基本协议的交互过程，都是请求管理进程给管理代理，响应则都是由管理代理发给管理进程的。只有 Trap 是无响应的，有管理代理单向发给管理进程。

SNMP 协议实体之间的协议数据单元 PDU 只有两种不同的结构和模式，一个 PDU 格式在大部分操作中使用，而另一个则在 Trap 操作中作为 trap 的协议数据单元。

4、Trap 操作，是一种捕捉事件并报告的操作，实际上几乎所有网络管理系统和管理协议都具有这种机制。

四、网络管理系统

1、HP-Open View

不能处理因为某一网络对象故障而误导致的其他对象的故障,不具备理解所有网络对象在网络中相互关系的能力。也不能把服务的故障与设备的故障区分开来。性能的轮与状态的轮询是截然分开的，这样导致一个网络对象响应性能轮询失败但不触发一个报警。

2、IBM-Net View

不能对故障事件进行归并,它不能找出相关故障卡片的内在关系,因此对一个失效设备，即使是一个重要的路由器，将导致大量的故障卡片和一系列类似的告警。不具备在掌握整个网络结构情况下管理分散对象的能力。性能轮询与状态轮询也是彻底分开的，这将导致故障响应的延迟。

3、SUN-SunNet Manager

是第一个重要的基于 UNIX 的网络管理系统。

4、Cabletron SPECTRUM

是一个可扩展的、智能的网络管理系统，它使用了面向对象的方法和客户服务器体系结构。SPECTRUM 构筑在一个人工智能的引擎之上，IMT(Inductive Modeling Technology)。它是所有四种网络管理软件中惟一具备处理网络对象相关性能力的系统。

SPECTRUM 服务器提供了两种类型的轮询：自动轮询和手动轮询。

SPECTRUM 提供了多种形式的告警手段，包括弹出窗口，发出报警声响等。

SPECTRUM 能自动的发现拓扑结构，但相对比较慢。

五、网络日常管理和维护

1、VLAN 的管理

2、WAN 接入的管理

3、网络故障诊断和排除

物理故障：

逻辑故障：

路由器故障：

主机故障：

4、网络管理工具

连通性测试程序 Ping ：

路由跟踪程序 Traceroute：在 Windows 中是 tracert

MIB 变量浏览器：

第 10 章　网络安全与信息安全

主要内容：1、密码学、鉴别

2、访问控制、计算机病毒

3、网络安全技术

4、安全服务与安全机制

5、信息系统安全体系结构框架

6、信息系统安全评估准则

一、密码学

1、密码学是以研究数据保密为目的，对存储或者传输的信息采取秘密的交换以防止第三者对信息的窃取的技术。

2、对称密钥密码系统(私钥密码系统)：在传统密码体制中加密和解密采用的是同一密钥。常见的算法有：DES、IDEA

3、加密模式分类：

（1）序列密码：通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流逐位加密得到密文。

（2）分组密码：在相信复杂函数可以通过简单函数迭代若干圈得到的原则，利用简单圈函数及对合等运算，充分利用非线性运算。

4、非对称密钥密码系统(公钥密码系统)：现代密码体制中加密和解密采用不同的密钥。

实现的过程：每个通信双方有两个密钥，K 和 K′，在进行保密通信时通常将加密密钥 K 公开(称为公钥)，而保留解密密钥 K′（称为私钥），常见的算法有：RSA

二、鉴别

鉴别是指可靠地验证某个通信参与方的身份是否与他所声称的身份一致的过程，一般通过某种复杂的身份认证协议来实现。

1、口令技术

身份认证标记：PIN 保护记忆卡和挑战响应卡

分类：共享密钥认证、公钥认证和零知识认证

（1）共享密钥认证的思想是从通过口令认证用户发展来了。

（2）公开密钥算法的出现为

2、会话密钥：是指在一次会话过程中使用的密钥，一般都是由机器随机生成的，会话密钥在实际使用时往往是在一定时间内都有效，并不真正限制在一次会话过程中。

签名：利用私钥对明文信息进行的变换称为签名

封装：利用公钥对明文信息进行的变换称为封装

3、Kerberos 鉴别：是一种使用对称密钥加密算法来实现通过可信第三方密钥分发中心的

身份认证系统。客户方需要向服务器方递交自己的凭据来证明自己的身份，该凭据是由 KDC 专门为客户和服务器方在某一阶段内通信而生成的。凭据中包括客户和服务器方的身份信息和在下一阶段双方使用的临时加密密钥，还有证明客户方拥有会话密钥的身份认证者信息。身份认证信息的作用是防止攻击者在将来将同样的凭据再次使用。时间标记是检测重放攻击。

4、数字签名：

加密过程为 C=EB(DA(m)) 用户 A 先用自己的保密算法(解密算法 DA)对数据进行加密 DA(m)，再用 B 的公开算法(加密算法 EB)进行一次加密 EB(DA(m))。

解密的过程为 m= EA (DB (C)) 用户 B 先用自己的保密算法(解密算 DB)对密文 C 进行解密 DB (C)，再用 A 的公开算法(加密算法 EA)进行一次解密 EA (DB (C))。只有 A 才能产生密文 C，B 是无法依靠或修改的，所以 A 是不得抵赖的 DA(m)被称为签名。

三、访问控制

访问控制是指确定可给予哪些主体访问的权力、确定以及实施访问权限的过程。被访问的数据统称为客体。

1、访问矩阵是表示安全政策的最常用的访问控制安全模型。访问者对访问对象的权限就存放在矩阵中对应的交叉点上。

2、访问控制表(ACL)每个访问者存储有访问权力表，该表包括了他能够访问的特定对象和操作权限。引用监视器根据验证访问表提供的权力表和访问者的身份来决定是否授予访问者相应的操作权限。

3、粗粒度访问控制：能够控制到主机对象的访问控制

细粒度访问控制：能够控制到文件甚至记录的访问控制

4、防火墙作用：防止不希望、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政策。

防火墙的分类：IP 过滤、线过滤和应用层代理

路由器过滤方式防火墙、双穴信关方式防火墙、主机过滤式防火墙、子网过滤方式防火墙

5、过滤路由器的优点：结构简单，使用硬件来降低成本；对上层协议和应用透明，无需要修改已经有的应用。缺点：在认证和控制方面粒度太粗，无法做到用户级别的身份认证，只有针对主机 IP 地址，存在着假冒 IP 攻击的隐患；访问控制也只有控制到 IP 地址端口一级，不能细化到文件等具体对象；从系统管理角度来看人工负担很重。

6、代理服务器的优点：是其用户级身份认证、日志记录和帐号管理。缺点：要想提供全面的安全保证，就要对每一项服务都建立对应的应用层网关，这就极大限制了新应用的采纳。

7、VPN：虚拟专用网，是将物理分布在不同地点的网络通过公共骨干网，尤其是 internet 联接而成的逻辑上的虚拟子网。

8、VPN 的模式：直接模式 VPN 使用 IP 和编址来建立对 VPN 上传输数据的直接控制。对数据加密，采用基于用户身份的鉴别，而不是基于 IP 地址。隧道模式 VPN 是使用 IP 帧作为隧道的发送分组。

9、IPSEC 是由 IETF 制订的用于 VPN 的协议。由三个部分组成：封装安全负载 ESP 主要用来处理对 IP 数据包的加密并对鉴别提供某种程序的支持。，鉴别报头(AP)只涉及到鉴别不涉及到加密，internet 密钥交换 IKE 主要是对密钥交换进行管理。

四、计算机病毒

1、计算机病毒分类：操作系统型、外壳型、入侵型、源码型

2、计算机病毒破坏过程：最初病毒程序寄生在介质上的某个程序中，处于静止状态，一旦程序被引导或调用，它就被激活，变成有传染能力的动态病毒，当传染条件满足时，病毒

就侵入内存，随着作业进程的发展，它逐步向其他作业模块扩散，并传染给其他软件。在破坏条件满足时，它就由表现模块或破坏模块把病毒以特定的方针表现出来。

五、网络安全技术

1、链路层负责建立点到点的通信，网络层负责寻径、传输层负责建立端到端的通信信道。

2、物理层可以在通信线路上采用某些技术使得搭线偷听变得不可能或者容易被检测出。数据链路层，可以采用通信保密机进行加密和解密。

3、IP 层安全性

在 IP 加密传输信道技术方面，IETF 已经指定了一个 IP 安全性工作小组 IPSEC 来制订 IP 安全协议 IPSP 和对应的 internet 密钥管理协议 IKMP 的标准。

（1）IPSEC 采用了两种机制：认证头部 AH，提前谁和数据完整性；安全内容封装 ESP，实现通信保密。1995 年 8 月 internet 工程领导小组 IESG 批准了有关 IPSP 的 RFC 作为 internet 标准系列的推荐标准。同时还规定了用安全散列算法 SHA 来代替 MD5 和用三元 DES 代替 DES。

4、传输层安全性

（1）传输层网关在两个通信节点之间代为传递 TCP 连接并进行控制，这个层次一般称作传输层安全。最常见的传输层安全技术有 SSL、SOCKS 和安全 RPC 等。

（2）在 internet 编程中，通常使用广义的进程信 IPC 机制来同不同层次的安全协议打交道。比较流行的两个 IPC 编程界面是 BSD Sockets 和传输层界面 TLI。

（3）安全套接层协议 SSL

在可靠的传输服务 TCP/IP 基础上建立，SSL 版本 3，SSLv3 于 1995 年 12 月制定。SSL 采用公钥方式进行身份认证，但是大量数据传输仍然使用对称密钥方式。通过双方协商 SSL 可以支持多种身份认证、加密和检验算法。

SSL 协商协议：用来交换版本号、加密算法、身份认证并交换密钥 SSLv3 提供对 Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一种实现在 Frotezza chip 上的密钥交换机制的支持。

SSL 记录层协议：它涉及应用程序提供的信息的分段、压缩数据认证和加密 SSLv3 提供对数据认证用的 MD5 和 SHA 以及数据加密用的 R4 主 DES 等支持，用来对数据进行认证和加密的密钥可以有通过 SSL 的握手协议来协商。

SSL 协商层的工作过程：当客户方与服务方进行通信之前，客户方发出问候；服务方收到问候后，发回一个问候。问候交换完毕后，就确定了双方采用的 SSL 协议的版本号、会话标志、加密算法集和压缩算法。

SSL 记录层的工作过程：接收上层的数据，将它们分段；然后用协商层约定的压缩方法进行压缩，压缩后的记录用约定的流加密或块加密方式进行加密，再由传输层发送出去。

5、应用层安全性

6、WWW 应用安全技术

（1）解决 WWW 应用安全的方案需要结合通用的 internet 安全技术和专门针对 WWW 的技术。前者主要是指防火墙技术，后者包括根据 WWW 技术的特点改进 HTTP 协议或者利用代理服务器、插入件、中间件等技术来实现的安全技术。

（2）HTTP 目前三个版本：HTTP0.9、HTTP1.0、HTTP1.1。HTTP0.9 是最早的版本，它只定义了最基本的简单请求和简单回答；HTTP1.0 较完善，也是目前使用广泛的一个版本；HTTP1.1 增加了大量的报头域，并对 HTTP1.0 中没有严格定义的部分作了进一步的说明。

（3）HTTP1.1 提供了一个基于口令基本认证方法，目前所有的 WEB 服务器都可以通过"基本身份认证"支持访问控制。在身份认证上，针对基本认证方法以明文传输口令这一最大弱点，补充了摘要认证方法，不再传递口令明文，而是将口令经过散列函数变换后传递它的摘

要。

（4）针对 HTTP 协议的改进还有安全 HTTP 协议 SHTTP。最新版本的 SHTTP1.3 它建立在 HTTP1.1 基础上，提供了数据加密、身份认证、数据完整、防止否认等能力。

（5）DEC-Web

WAND 服务器是支持 DCE 的专用 Web 服务器，它可以和三种客户进行通信：第一是设置本地安全代理 SLP 的普通浏览器。第二种是支持 SSL 浏览器，这种浏览器向一个安全网关以 SSL 协议发送请求，SDG 再将请求转换成安全 RPC 调用发给 WAND，收到结果后，将其转换成 SSL 回答，发回到浏览器。第三种是完全没有任何安全机制的普通浏览器，WANS 也接受它直接的 HTTP 请求，但此时通信得不到任何保护。

六、安全服务与安全与机制

1、ISO7498-2 从体系结构的观点描述了 5 种可选的安全服务、8 项特定的安全机制以及 5 种普遍性的安全机制。

2、5 种可选的安全服务：鉴别、访问控制、数据保密、数据完整性和防止否认。

3、8 种安全机制：加密机制、数据完整性机制、访问控制机制、数据完整性机制、认证机制、通信业务填充机制、路由控制机制、公证机制，它们可以在 OSI 参考模型的适当层次上实施。

4、5 种普遍性的安全机制：可信功能、安全标号、事件检测、安全审计跟踪、安全恢复。

5、信息系统安全评估准则

（1）可信计算机系统评估准则 TCSEC：是由美国国家计算机安全中心于 1983 年制订的，又称桔皮书。

（2）信息技术安全评估准则 ITSEC：由欧洲四国于 1989 年联合提出的，俗称白皮书。

（3）通用安全评估准则 CC：由美国国家标准技术研究所 NIST 和国家安全局 NSA、欧洲四国以及加拿大等 6 国 7 方联合提出的。

（4）计算机信息系统安全保护等级划分准则：我国国家质量技术监督局于 1999 年发布的国家标准。

6、可信计算机系统评估准则

TCSEC 共分为 4 类 7 级：D，C1，C2，B1，B2，B3，A1

D 级，安全保护欠缺级，并不是没有安全保护功能，只是太弱。

C1 级，自主安全保护级，

C2 级，受控存取保护级，

B1 级，结构化保护级

B3 级，安全域级

A1，验证设计级。

七、评估增长的安全操作代价

为了确定网络的安全策略及解决方案：首先，应该评估风险，即确定侵入破坏的机会和危害的潜在代价；其次，应该评估增长的安全操作代价。

安全操作代价主要有以下几点：

（1）用户的方便程度

（2）管理的复杂性

（3）对现有系统的影响

（4）对不同平台的支持

第 11 章 Internet

主要内容：1、internet 体系结构

2、internet 连接的方法

3、internet 地址

4、internet 域名系统

5、internet 地址是的扩展

一、Internet 体系结构

1、自治系统：原始的 Internet 核心体系是在 Internet 权有一个主干网的那个时期开发的。但是这种体系结构存在以下一些问题：

这种体系不能适应互联网扩展到任意数量的网点；

许多网点由多个局域网组成，且用多个多路由器互连，由于一个核心路由器在每个网点上与一个网络相连，核心路由器就只知道那个网点中的一个网络的情况；

一个大型的互联网是独立的组织管理的网络的互连集合，路由选择体系结构必须为每个组织提供独立的控制路由选择和访问网络的方法，因此必须用一个单一的协议机制来构造一个由许多网点构成的互联网，同时，各个网点又是一个自治系统。

二、Internet 连接的方法

1、将计算机连接到一个局域网，这个局域网的服务器是 Internet 的一个主机。

条件：必须连接到一个与 Internet 连接的网络，需要网络适配卡和 ODI 或 NDIS 驱动程序，还需要在本地计算机上运行 TCP/IP，如果是 Windows 系统还需要 Winsock 支持。

2、利用串行接口协议(SLIP)或点到点协议(PPP)，通过电话拨号方式进入一个 Internet 的主机

条件：需要一个调制解调器 Modem、TCP/IP 软件和 SLIP 或 PPP 软件，如果是 Windows 系统还需要 Winsock 支持。

3、通过电话拨号进入一个提供 Internet 服务的联机服务系统。

条件：需要一个调制解调器 Modem、标准的通信软件和一个联机服务帐号。

4、用户选择连接方法的考虑因素：联网的目标和需求；用户内部配置的网络基础设施；用户支付 Internet 联网费用的能力；对 Internet 安全服务的需求。

三、Internet 地址

在 TCP/IP 协议中，规定分配给每台主机一个 32 位数作为该主机 IP 地址。每个 IP 地址由两个部分组成，即网络标识 netid 和主机标识 hostid。

IP 地址的层次结构具有两个重要特性：第一，每台主机分配了一个惟一的地址；第二，网络标识号的分配必须全球统一，但主机标识号可由本地分配，不需要全球一致。

1、A 类：1.0.0.1 至 126.255.255.254 可能的网络数有 126 个，主机部分有 1677216 台(224-2)

2、B 类：128.0.0.1 至 191.255.255.254 可能的网络数有 16384 个，主机有 65536 台

3、C 类：192.0.0.1 至 223.255.255.254 可能的网络数有 2097152 个，主机有 256 台

4、D 类：用于广播传送至多个目的地址用 224-239

5、E 类：用于保留地址 240-255

RFC1918 将 10.0.0.至 10.255.255.255、127.16.0.0 至 172.31.255.255、192.168.0.0 至 192.168.255.255 的地址作为预留地址，用作内部地址，不能直接连接到公共因特网上。

四、Internet 地址映射

将一台计算机的 IP 地址映射到物理地址的过程称地址解析。

常用的地址解析算法有以下三种：

1、查表法：将地址映射关系放在内存中的一些表里，当解析地址时，通过查表得到解析的结果。用于广域网。

2、相近形式计算法：通过简单的布尔和算术运算得出映射地址。用于可配置网络。

3、消息交换法：计算机通过网络交换信息得到映射地址。用于静态编址。

TCP/IP 协议组包含一个地址解析协议(ARP)。ARP 协议定义了两类基本消息，一类消息是请求消息，另一类是应答消息。

五、Internet 地址空间的扩展

1、IPV6 仍然支持无连接传送；允许发送方选择数据报大小；要求发送方指明数据报在到达目的站前的最大跳数。更大的地址空间；灵活的报头格式；增强的选项；支持资源分配；支持协议扩展。

2、IPV6 的数据报格式：IPV6 数据有一个固定的基本报头 40 字节其后可以允许多个扩展报头，也可以没有扩展报头，扩展报头后是数据。

IPV4 的数据报格式：包括数据报报头和数据区的部分。报头：版本号、IHL、服务级别、数据单元长度、标识、标记、分段偏移、生命期、用户协议、报头检查和、源地址、目的地址、任选项+填充、数据。

3、该基本报头包含版本号、数据流标记、PAYLOAD 长度、下一个报头、跳数极限、源地址、目的地址。

4、IPV4 与 IPV6 比较：取消了报头长度字段，数据报长度字段被 PAYLOAD 长度字段代替；源地址和目的地址字段大小增加为每个字段占 16 个八位组，128 位；分段信息从基本报头的固定字段移动扩展报头；生存时间字段改为跳数极限字段；服务类型字段改为数据流标号字段；协议字段改为指明下一个报头类型字段。

5、IPV6 有三个基本地址类型，单播地址(unicast)即目的地址指明一台计算机或路由器，数据报选择一条最短的路径到达目的站；群集地址(cluster)即目的站是共享一个网络地址的计算机的集合，数据报选择一条最短路径到达该组，然后传递给该组最近的一个成员；组播地址(multicast)即目的站是一组计算机，它们可以在不同地方，数据报通过硬件组播或广播传递给该组的每一成员。

6、对任何地址若开始 80 位是全零，接着 16 位是全 1 或全零，则它的低 32 位就是一个 IPV4 地址。

第 12 章 企业网与 Intranet

主要内容：1、企业网络计算的组成和管理

2、企业网络开放系统集成技术

3、intranet 定义和要素

4、intranet 应用和建立

一、企业网络计算的背景和挑战

企业网是连接企业内部各部门并和企业外界相连，为企业的通信、办公自动化、经营管理、生产销售以及自动控制服务的重要信息基础设施。Intranet 是基于 TCP/IP 协议，使用环球网 WWW 工具，采用防止外界侵入的安全措施，为企业内部服务，并有连接 Intranet 功能的企业内部网络。

1、驱动企业网络计算的因素：用户需求，这是基本动力；先进和实用的信息技术；迅速变化中的市场。

2、可采用两种模型：一种是可伸缩的模型，即企业网络计算的同样的软件可运行在企业内部的不同平台上；另一种是集成的模型，即企业内部不同平台上的软件的集成。

二、企业网络计算的组成和特性

1、企业网络计算的组成：客户机/服务器计算；分布式数据库；数据仓库；网络和通信；网络和系统的管理；各种网络应用。

2、企业网络计算的特性：支持客户机/服务器计算械；支持管理海量数据的能力和设施；

分布数据管理的设施；国际化和本地化；功能强的通信设施；系统的灵活性；分布资源管理；开发工具和开发手段的提供。

三、开放系统

开放系统：是对一个不断发展的、厂家中立的、用于对整个系统进行有效配置、操作和替换的接口、服务、协议和格式的规范描述的实现，它的应用和组成部件可以用不同厂家的其他相同实现替代。

1、开放系统的两个特点：开放系统所采用的规范是厂家中立的，或者是与厂家无关的；开放系统允许不同厂家的产品替换，这种替换包括整个系统其组成部件。

2、专用系统：它所采用的规范是专用，而不是厂家中立的；专用系统不允许由不同厂家的产品替换；它的组成部件允许具有许可证的厂家产品替换。

3、驱动开放系统发展的因素：功能、可用性、复杂性、价格。

四、企业网络开放系统集成技术

1、FRAMWORK 是应用程序的开发和运行环境，它实际上是蹭件和操作系统的组合。比较有名的产品有 CICS、Windows、UNIX。

2、COSE 专门制定了自己的开放系统环境规范，主要技术包括用于窗口管理的 Motif、标准 API 接口和用于数据库管理的 SQL。

3、信息系统与网络计算主要实现网络范围数据管理、通信和网络管理，主要技术有：在数据管理方面有用于数据库间通信的 RDA，即远程数据访问；通信服务 DCE 分布式计算环境，RPC 远程过程调用，OSI 开放系统互连；管理服务，DME 分布管理环境，SNMP 简单网络管理协议。

五、开放系统环境应用可移植框架

六、Intranet 的定义和要素

1、Intranet 是基于 Internet TCP/IP 协议，使用的环球网 WWW 工具、采用防止外界侵入的安全措施、为企业内部服务，并有连接 Internet 的功能的企业内部网络。

2、Intranet 的组成：网络、电子邮件、内部环球网、邮件地址清单、新闻组 Newsgroups、闲谈 Chat、FTP、Telnet、Gopher。

第 13 章 TCP/IP 联网

主要内容：1、TCP/IP 实现的基本原理

2、Windows NT 平台的联网

3、UNIX 平台的联网及 LINUX 网络的联网

一、TCP/IP 实现基本原理

1、TCP/IP 的实现方式：

TSR 常驻内存程序是一种安装在 Windows 之前在 DOS 上运行的程序。缺点，不能动态分配内存，TSR 需要动态链接库 DLL 帮助，才能让 Windows 程序访问网络。目前只有在 DOS 环境下才使用 TSR 方式

DLL 动态链接库是一个 16 位的 Windows 程序函数库，只有当用到其中的过程时才会被调用。缺点，它们不能直接与网卡通信，它们依赖于 Windows 的调度程序。

VxD 虚拟设备是在 Windows 32 位保护方式下实现的，用于实现一些关键的部分，如视频、鼠标及通信端口驱动程序。它是通过硬件中断方式响应网络中的通信，可以彻底地访问 Windwos 和 DOS 程序。

2、网络配置基本参数：PC 中网络适配卡基本参数，I/O 端口地址、内存地址及中断号 IRQ。与 Microsoft 相关的网络信息，主机标识、工作组名、WINS 服务器地址、DHCP 服务器地址；与 TCP/IP 网络信息有关，IP 地址、子网掩码、主机名、域名、域名服务器、默认网关 IP

地址。

二、Windows NT 平台的 TCP/IP 联网

三、UNIX 平台的 TCP/IP 联网

1、建立 UNIX 联网的几个步骤：设计物理和逻辑的网络结构；分配 IP 地址；安装网络硬件；为每个主机配置启动时候的网络接口；设立服务程序或者静态路由。

2、IP 地址的获取和分配：可能通过/etc/hosts 文件、DNS 或者其他域名系统来实现。

3、网卡的配置：ifconfig 命令可以设置网卡 IP 地址、子网掩码、广播地址、网卡的使能状态及其他选项参数。Ifconfig interface [family] address up option ，其中 interface 是指定的网卡名，可以用 netstat-i 来检查当前系统网卡的芯片类型。Loopback 网卡通常叫 lo0 它是一个假想的硬件，用来作本机内部网络包的路由，

4、路由配置：route 配置静态路由，route [-f] op [type] destination gateway hop-count ，op 参数如果是 add 就是增加一个路由表项，如果 delete 就是删除一个路由表项。

5、routed 标准路由 daemon，只支持 RIP，它使用 hop 作为距离计数单位。Routed 有两种运行方式：服务器模式和安静模式。两种模式都要监听广播包，但只有服务器模式才能发布自己的路由信息，通常只有多网卡的机器才设置成服务器模式，如果未说明就是安静模式。

6、gated 一个更好的路由 daemon，gated 配置文件在/etc/gated.conf 的语法中加入 BGP 后有了很大改动，gated 能细粒度地控制广播路由、广播地址、信任策略、距离向量等。

四、Linux 网络的安装与配置

1、手工进行网络硬件配置：

系统启动时会自动检测网卡，有两个缺点：一个是不通正确的检查所有的网卡，特别是一些比较廉价的网卡，二是核心程序不会自动检测一个以上的网卡，这点是为了使用户可以控制将山上设置到指定的端口上。如果使用两个以上的网卡，自动检测网卡就会失败。

手动进行配置，一种方法是在核心程序的源代码的/drivers/net/space.c 文件中修改或添加信息，然后重新编译内核。另一种方法在系统启动过程中将这些信息提供给内核程序。在 LILO 系统时可以通过 lilo.conf 文件中的 append 参数来传递给内核。

2、手工 TCP/IP 网络配置

设置主机名：hostname name，为接口进行 IP 配置：ifconfig interface ip-address

route add -net 202.112.58.0 -net 的含义，因为 route 既可以处理到网络的路由，又可以处理到单个主机的路由。通过 net 来告诉它此地址是代表的一个网络，用 host 来告诉它此地址是代表一个主机。如果为了方便，还可以在/etc/networks 中定义网络名字，route 后面直接使用网络名字就可以了。

route add default gw 2-2.112.58.254 网络名字 default 是 0.0.0.0 的简写，指示默认的路径，并不需要将这个名字加入到/etc/networks 文件。

3、编辑 hosts 与 networks 文件

如果不打算使用 DNS 或者 NIS 进行地址解析时，就必须将所有的主机名字都放入 hosts 文件中。伴随 hosts 文件的还有一个/etc/networks 文件，它在网络的名字和网络号之间建立映射。

4、编译内核

命令如下：cd/usr/src/linux make config

新的 Linux 核心版本中，对核心的配置除了上述 make config 命令外，还增加了字符状态下以菜单形式对核心进行配置的命令 make colormenu 以及在 X 窗口系统中运行的图形配置界面命令 make xconfig

五、高级 TCP/IP 应用配置

1、网络配置文件：在 Linux 中是通过/etc/rc.d/rc.inet1 和/etc/rc.d/rc.inet2 两个文件实现的，/etc/rc.d/rc.inet1 主要是通过 ifconfig 和 route 命令进行基本的 TCP/IP 接口配置，主要由两部分组成，第一部分是对回送接口的配置，第二部分是对以太网接口的配置。/etc/rc.d/rc.inet2 主要是用来启动一些网络监控的进程，inetd portmapper 等。

2、名字服务和解析器配置

运行 named：大多数 UNIX 机器上提供域名服务的程序叫 named 它是一个服务器程序，用来向客户或其他名字服务器提供域名服务。它从配置文件/etc/named.boot 中获取信息，以及各种包含域名到地址映射的数据文件，后者称为"区文件"zone file。Named 包含的主文 named.hosts。

第 14 章 Internet 与 Intranet 信息服务

主要内容：1、环球信息网的服务和管理

2、动态 Web 文件与 CGI 技术

3、活动 Web 文件与 Java 技术

4、FTP 服务配置和管理及广域信息服务 WAIS

WWW 服务器把信息组织成分布式的超文本，这些信息节点是文本、子目录或信息指针。WWW 浏览器程序为用户提供基于超文本传输协议 HTTP 的用户界面。WWW 服务器数据文件由超文本标记语言 HTML 描述。HTML 利用通用资源访问地址 URL 表示超媒体链接，并在文本内指向其他网络资源

一、环球信息网

1、环球信息网的定义：环球信息网(WWW)是基于客户机/服务器方式的信息发现技术和超文本技术的结合。

2、超文本文档包含着一些借用标题、章节本身等构造文本的命令，从而允许浏览程序格式化为一种文本类型，以获得最佳的屏幕显示效果。

3、Web 任务：是使用一个起始 URL 来获取一个 Web 服务器上的 Web 文档，解释这个 HTML，并将文档内容以用户环境所许可的效果最大限度地显示出来。

4、浏览器分类：线模式和图形界面。

lynx 是线模式浏览器，使用箭头键来浏览内在 HTML 连接，支持书签和表格功能。特点是：在交互状态，可以将文章发布到新闻组；在非交互状态，可以将 HTML 过滤为纯文本。

midasWWW 是基于 X-windows 系统浏览程序，支持更多的嵌入图形。

Mosaic 是可以支持嵌入的 gif 和 xbm 图形，其他的视频影像。

Netscape 页面采取边传送文档边显示的方式，增强了交互效果。

Micosoft Explorer

5、Web 服务器：在目前主要 3 种基于 UNIX 的 web 服务器公用软件。

NCSA Web 是 C 语言编写的，程序小，速度快，可以单独作为服务进程运行，也可以设置在 inetd 中运行。

CERN httpd 是早期 C 语言编写的 Web 服务器，主要特点为提供 proxy 代理和缓存功能。

Plexus httpd 是 perl 语言编写的，可扩展性好，易于使用和更新，但行动时开销较大。

二、环球信息网服务的建立

1、编译 Web 服务程序：获取源程序包；编辑修改相应的 Makefile；设置选择项，修改 src/config.h 头文件；在每个目录中运行 make 编译命令。必要时修改 src/makefile，cgi-src/makefile，support/makefile 三个配置文件，编译三项内容：httpd 服务程序，support 支持程序，cgi-bin 接口程序。

2、配置 Web 系统服务：包括在三个配置文件，Web 系统配置文件 httpd.conf；Web 资源文档配置文件 srm.conf;Web 服务访问控制配置文件 access.conf,还包括如何扩充文档 MIME

类型。

3、http 配置文件使用的一些约定：不分大小写；以#开始的为注释行；一个指令定义一行；忽略多余的安全可靠，只认为是一个空格。

4、系统配置文件 httpd.conf

配置时首先需要选择 httpd 的运行方式(单独运行或是在 inetd 下运行)，是否进行服务访问控制。然后以 httpd.conf.dist 为模板，修改各个变量。

5、文档配置文件 srm.conf

指定了 Web 服务的文档和接口程序等所在的路径。

6、服务访问控制配置文件 access.conf

定义了 Web 用户的访问权限。默认的定义是用户可以浏览 Web 服务器所能提供的所有文档。

7、访问控制策略：目前有两种方式来控制对文档目录的访问。全程访问控制配置文件，单个目录访问控制文件。

8、扩展文档 MIME 类型：mime.types 文件中定义了 httpd 不能直接处理的文件类型。可以通过 srm.conf 设置变量 AddEncoding/Addtype/Default Type 来定义新的类型。

三、WWW 服务管理

1、扩充 WWW 服务功能

CGI 接口程序能够通过 WWW 服务执行外部程序。外部程序接收用户的输入:传送给 WAIS，SQL 等服务器；将查询结果以 HTML 文档或 URL 的形式返回给 WWW 服务；CGI 接口可用多种编程语言编写，也可以自己编写

2、WWW 服务与 CGI 的交互技术

WWW 服务与 CGI 交互过程分为两部分：接口程序接收用户输入；从接口程序输出信息到 WWW 服务。

接口程序通过三个方式接收用户输入：环境变量，WWW 服务在将浏览器的请求传送给接口程序时，为接口程序设置的环境变量。标准输入，在查询参数较多，尤其在接收用户 FORM 表格输入方式设置为 POS。命令参数，HTML 的 < ISINDEX > 标号来输入查询关键字，浏览器遇到标号时显示。

CGI 接口程序输出：CGI 接口程序的执行结果以标准输出的形式传递给 WWW 服务。输出中包含一行描述数据类型的头信息、一个分隔行，接着是实际文档数据。

三、FTP 服务的配置和管理

1、FTP 传送服务主要用于存放大量的网络公用软件、常用工具和技术文档，以及一些著名的 FTP 镜像。传递的数据类型：ASCII，Postscript、SGML、可执行代码、图像、声音、视频动画。

2、FTP 服务通过 FTP 服务器与 FTP 客户程序之间的信息交换。数据上载将数据从 FTP 客户程序传输到 FTP 服务器。数据下载 FTP 客户程序从 FTP 服务获取数据。

3、FTP 服务器可提供两种访问形式

内部用户 FTP：在主机上有帐号的用户，用户在输入正确的帐号和口令字后，可以访问整个文件系统中有读权限的文档，并可以任意数据到有写权限的目录。

匿名 FTP：匿名 FTP 是 internet 的公共信息服务，访问范围限于匿名 FTP 区域(FTP 服务器定义的子文件系统)。用户只需要以 Anonymous/ftp 登录，输入自己的电子邮件作为口令字即可访问并下载所提供的信息资源。

4、FTP 包含两个部分：服务器，响应客户请求，传送文档；文件系统，服务器文档扫描调用的区域。FTP 服务器命名通常是 ftpd 或 in.ftpd。

5、FTP 的运行方式：通常 ftpd 是在系统超级服务 inetd 进程下运行。使用 TCP 的 21 号

端口。基本传输模式：流方式、块方式、压缩方式三种

6、FTP 配置，在 Inetd 的配置文件中(/etc/inetd.conf)中添加相应的一行设置为 ftp stream tcp nowait root /etc/ftpd 。每次更新配置后，和 kill -HUP INETD 进程号，重新启动 INETD。

7、在 Inetd 下配置好 FTP 后，需要在主机/etc/passwd 中设置用户 FTP，因为 ftpd 在允许用户匿名访问 ftp 之前，首先检查 ftp 用户是否存在，如果不存在，ftpd 拒绝匿名用户访问。

四、建立 FTP 服务器

1、FTP 系统服务及其目录配置

.company/：存放公司本身的信息

.pub/：公用软件目录

.in-coming/：匿名 FTP 用户上载文件目录

.usr/，bin/，etc/：FTP 系统占用的目录

(1)设置 FTP server 的目录：

(2)修改 password 和 group 文件内容及访问权限

(3)在 FTP server 中设置目录

2、建立镜像系统

文件服务器镜像系统(mirror sites)完成对远程匿名 FTP 服务器资源的本地镜像。在镜像描述文件中指定远程 FTP 服务器地址、登录名及口令、需要镜像的远程 FTP 服务器的目录或文件、本地 FTP 服务器上的文件存放路径和权限控制码，系统就能够根据镜像描述文件使用 FTP 协议自动登录到远程 FTP 服务器，进入相应的目录，取得该目录下的文件列表，与本地目录下的文件列表进行比较。目录流行的镜像软件是 mirror-2.3，是用 perl 语言编写的程序，按照 FTP 协议，在运行它的主机与远程主机之间，按目录和文件结构进行数据传输。

3、REAMME 文件用于描述各个文件及子目录。包括以下内容：系统管理员电子邮件地址，便于用户求助；本服务的基本信息；版权的基本信息；热点透视；声明信息。

4、统计日志 WU-FTPD 系统定义了访问日志文件的格式，FTP 访问日志统计工具有 xferstats、iisstat 等

5、访问控制

WU-FTP 访问控制配置文件是 ftpaccess、ftphosts、ftpusers、ftpgroups 等。可以根据用户访问控制、CPU 负载控制、用户组别控制、向用户自动显示状态信息，记录系统使用情况，文件访问快捷方式，控制文件载。

用户访问控制：可以通过 fptaccess 定义多种类别来控制用户的访问。类别定义由用户类型和主机地址来组合。用户类型有三种：anonymous，匿名 FTP，只有访问 FTP 系统目录；guest，用户使用帐号和口令访问文件系统的一部分；real，系统本身的用户，可以访问整个文件系统。

6、向用户发送提示信息：WU-FTP 有四种方式可向进入系统的用户提示信息，他们是：banner，在用户登录时，将一个提示文件显示给用户；message 可以控制在适当的时候提示用户，一般在用户登录或用户转移到某一目录时提示；readme 可以提示用户 README 文件已经更新。Shutdwon 关闭 FTP 服务有两种方式：在 ftpaccess 中使用 shutdown 命令；使用 ftpshut 工具

7、一些管理工具

Ftpshutd 在系统将要关闭时，根本上新的用户访问；并关闭服务。

ftpwho 显示当前每个类别的用户当前有多少人在访问以及最多可访问数、其他一些用户使用情况。

ftpcount 显示每个类别的用户当前访问 ftp 服务的数目，以及最多访问数.

Fftpmail 是电子邮件与 ftp 的接口。

五、动态 Web 文档与 CGI 技术

1、Web 文档的三种基本形式

静态文档：是一个存储于 Web 服务器的文件，静态文档由作者在写作时决定文档内容，它的内容不会变化。是一种排版语言，主要优点，是简单、可靠、性能好；主要缺点，是灵活性差，当信息变化时，必须重新设计文档。

动态文档：它在浏览器访问 Web 服务器时创建，没有预先定义的格式。内容总是变化的，每次访问都要创建新文档。可以用来显示天气预报、股市行情等时效性很强的信息。主要缺点创建费用较高、访问的时间较长、且浏览器取得一个复制的文档后不会再改变。

活动文档：它不完全由服务器产生，一个活动文档包括一个计算和显示的程序。只要用户程序保持运行，该文档可以不断地变化。活动文档本身不包含运行所需要的软件，大部分支持软件在浏览器上。主要缺点，是创建和运行这类文档费用高，安全性差。

2、动态文档的实现

处理动态文档的服务器有三个特性：服务器必须扩展，对来自浏览器的每次请求，能执行一个创建文档的应用程序，并将产生的活动文档返回给浏览器；必须为每个动态文档写一个应用程序；服务器使用设置信息来区分动态文档和静态文档。

3、通用网关接口 CGI

构建动态 Web 文档广泛使用的技术是通用网关接口(common gateway interface)CGI。CGI 标准说明了服务器如何和应用程序交互作用，以实现一个动态文档，这种应用程序称为 CGI 程序。

CGI 是服务器和 HTML 文件之间的接口程序，负责处理 HTML 文件与运行在服务器中的非 HTML 程序之间的数据交换。

CGI 可以是一个编译的程序，或者是一个批处理文件，或者任何可执行的二进制文件。CGI 存放在 Web 服务器的 cgi-bin 子目录下，必须要求系统管理员开放对 cgi-bin 目录的访问权。CGI 实现交互查询有两种方法：一种是基于文件的查询；另一种是使用 FROM。

六、活动 Web 文档和 Java 技术

七、广域信息服务

1、广域信息服务 WAIS(Wide Area Information Search)是一种网络信息查询系统，它可以和关键字对服务器数据库进行全文索引，获取索引所得的信息。

2、WAIS 运行模式，采用客户机和服务器方式。运行方式，standalone 和 inetd 方式。包括三部分内容，客户方软件、服务器软件和索引程序。

3、WAIS 数据主要有 8 个文件构成，其中 xx.src 用于客户端服务器说明，xx.dct，xx.inv 用于查询。

4、在 UNIX 机器上，有 waisserch 和 xwais。在 PC 要上有 winwais。这些客户程序和服务器之间采用 Z39.50 标准协议，在不同平台上，只要遵循这些协议就能和 waisserver 进行通信。

5、FreeWais 系统组成：其软件由索引建立器、服务器和客户访问程序三部分组成。其工作过程：

（1）索引建立器从数据库中读取数据并建立索引，它为文档中出现的单词建立一个列表，并在一个表中记录单词的出现位置。

（2）服务器则根据用户指定的查询条件，使用已经有的索引进行检索。服务器首先分解出一个用户自然语言的查询条件，把每个单词作为关键词，找出包含这些单词的文档，并给出一个分数来提醒用户每篇文档的切题程序。分数越高表示切题程序越高。

（3）客户程序通过 Z39.50 标准协议来形成检索规则，显示服务器找到的命中文档，还允许用户查看某一文档的内容。文档的类型包括 ASCII 文本、二进制信息、声音文件、Post Script 文件、HTML 文件、JPEG、GIF 文件。

第 15 章 网络应用

主要内容：1、网络化经济的新模式

2、internet 服务平台

3、计算机支持的协同工作

4、电子商务

5、远程教育以及远程医疗

一、21 世纪网络发展趋向

1、摩尔定律：是 Intel 公司创始人莫尔于 20 世纪 70 年代提出的，其表达式 D(T)=D(T0)2(T-T0)/1.5。每 18 个月集成电路器件数翻一番。

2、曼卡夫定律：是以太网发明者曼卡夫于 20 世纪 90 年代初提出的，其表达式为网络价值=N(N-1)/2 。N 为用户数。任何通信网络的价值是以网络内用户数的平方来增长，即 N 个用户可能的连接数。由此可以导出网络频宽的按拉入网络的 PC 能力的平方增长。

二、网络化经济的新模式

1、Internet 协议和 WWW 技术已经 Internet 的两个重要标准

2、IP 服务平台的要求：网络安全、服务扩展、平台的扩展、网络管理、互操作性、高效的实施、各种设施的接入、国际化和本地化、可商业化应用、移动服务、开放性和易于使用。

3、采用网络中间件实现 IP 服务平台是行之有效的方法。中间件位于网络层之上应用层之下，为应用提供公共基础，以共享结构、框架以及公共功能。

4、中间件可分三类：通信中间件，由协议和体系结构组成，支持基本面向对象的分布系统和分布计算。安全中间件，包括认证、访问控制、数据保密和完整性以及加密等功能。集成中间件，集成计算平台和企业范围的各种应用。

三、计算机支持的协同工作

1、CSCW(computer supported cooperative work) 是研究地域分散的一个群体如何借助计算机及其网络技术支持，共同协调与协作来完成一项任务的技术领域。

2、CSCW 包括协同工作体系结构、群体协作方式和模型研究、支持群众工作的相关技术研究、应用系统的开发等部分。

3、CSCW 的系统体系结构：

CSCW 可分为四层结构模型：第一层为开放系统互连环境，提供开放的通信网络支持环境，保证协同工作过程中有效的信息交流。第二层为协同工作支撑平台，解决协同工作所需要的主要机制和工具。第三层协同工作应用接口，提供协同应用的编程接口 API、人中接口 HCI、人际接口 IPI。第四层各种 CSCW 应用系统，针对各种协同工作应用领域，提供所需要的协作支持工具和剪裁和集成，协同应用系统的开发。

4、群件：是指给人们提供一个访问某共享环境的界面，以支持他们去完成某个总体的目标或任务的计算机应用系统。

四、电子商务

1、电子商务 EC：是一种现代商业经营方法，可满足企业、商贸、消费者的需求，以达到降低成本、改进产品和服务质量、提高服务传递速度的目的。电子商务通过计算机网络实现信息、产品、服务的交换。

2、电子商务的特征：2P+3C

以计算机网络为基础；贸易伙伴以协调和协作方式；围绕贸易或商务这个主题；对商务内容

和信息计算机化处理；利润。

3、电子商务的框架：社会法规政策与隐私和电子文本、多媒体和网络协议的技术标准是两个十分重要的支柱。

4、电子商务的类型：

5、电子商务的流程：

6、电子商务的组成原理：电子商务是贸易链上的各个参与方，在计算机信息网络环境下，通过 CA 认证和信息安全保证的基础上，对贸易流程洽谈、销售、支付、贸易执行、客户服务全方位处理的过程。

五、远程教育

1、远程教育：是指与传统的以课堂为主体的、都是与学生面对面的教学相别的另一种教学模式，它有函授教学、广播电视教学、网络远程教学。

2、远程教育特点：访问方式的时空无限性；教育信息的共享性；教学方式的双向交互性；自学模式的多样性

3、网络远程教学的形式：远程访问；远程体验；远程辅导；远程共享；虚拟出版；虚拟教室；计算机支持的协作学习。

4、远程教学系统包括两个部分：课件开发系统和教学运行系统。

六、远程医疗

1、远程医疗系统的工作模式或服务可以分为异步非实时和同步实时两类。前者通过电子邮件信函进行医疗咨询或会诊，后者通过视频会议系统进行远程实时会诊乃至手术指导等医疗活动。

网络工程师最容易忽视的七大问题！

1．配置交换机

将交换机端口配置为 100M 全双工，服务器安装一块 Intel100M

EISA 网卡，在大流量负荷数据传输时，速度变得极慢，最后发现这款网卡不支持全双工。将交换机端口改为半双工以后，故障消失。这说明交换机的端口与网卡的速率和双工方式必须一致。目前有许多自适应的网卡和交换机，由于品牌的不一致，往往不能正确实现全双工方式，只有手工强制设定才能解决。

2．双绞线的线序

将服务器与交换机的距离由 5 米改为 60 米，结果无论如何也连接不通，为什么呢?以太网一般使用两对双绞线，排列在 1、2、3、6 的位置，如果使用的不是两对线，而是将原配对使用的线分开使用，就会形成缠绕，从而产生较大的串扰(NEXT)，影响网络性能。上述故障的原因是由于 3、6 未使用配对线，在距离变长的情况下连接不通。将 RJ45 头重新按线序做过以后，一切恢复正常。

3．网络与硬盘

基于文件访问和打印的网络的瓶颈是服务器硬盘的速度，所以配置好服务器硬盘对于网络的性能起着决定性的作用。以下提供几点意见供你参考：

- 选用 SCSI 接口和高转速硬盘。
- 硬盘阵列卡能较大幅度地提升硬盘的读写性能和安全性，建议选用。
- 不要使低速 SCSI 设备(如 CD)与硬盘共用同一 SCSI 通道。

4．网段与流量

某台服务器，有两台文件读写极为频繁的工作站，当服务器只安装一块网卡，形成单独网段时，这个网段上的所有设备反应都很慢，当服务器安装了两块网卡，形成两个网段以后，将这两台文件读写极为频繁的工作站分别接在不同的网段上，网络中所有设备的反应速度都

有了显著增加。这是因为增加的网段分担了原来较为集中的数据流量，从而提高了网络的反应速度。

5．桥接与路由

安装一套微波联网设备，上网调试时服务器上总是提示当前网段号应是对方的网段号。将服务器的网段号与对方改为一致后，服务器的报警消失了。啊!原来这是一套具有桥接性质的设备。后来与另外一个地点安装微波联网设备，换用了其他一家厂商的产品，再连接，将两边的网段号改为一致，可当装上设备以后，服务器又出现了报警：当前路由错误。修改了一边的网段以后，报警消失了。很明显这是一套具有路由性质的设备。桥的特征是在同一网段上，而路由必须在不同网段上。

6．广播干扰

上述通过桥接设备联网的两端，分别有一套通过广播发送信息的应用软件。当它们同时运行时，两边的服务器均会发出报警：收到不完全的包。将一套应用软件转移到另外一个网段上以后，此报警消失。这是因为网络的广播在同一网段上是没有限制的。两个广播就产生了相互干扰从而产生报警。而将一个应用软件移到另外一个网段以后，就相当于把这个网段的广播与另外网段上的广播设置了路由，从而限制了广播的干扰，这也是路由器最重要的作用。

7．WAN 与接地

无意将路由器的电源插头插在了市电的插座上，结果 64KDDN 就是无法联通。电信局来人检查线路都很正常，最后检查路由器电源的接地电压，发现不对，换回到 UPS 的插座上，一切恢复正常。路由器的电源插头接地端坏掉，从而造成数据包经常丢失，做 PING 连接时，时好时坏。更换电源线后一切正常。WAN 的连接因为涉及到远程线路，所以对于接地要求较为严格，才能保证较强的抗干扰性，达到规定的连接速率，不然会出现奇怪的故障。