第一章 网络概述

1.1 ARPANET 为分组交换网之父，并将分组交换网的出现作为现代电信时代的开始。

1.2 分组交换网特点：

通常我们将发送的整块数据称为一个报文。在发送报文之前，先将较长的报文划分成为一个个更小的等长数据段。在每一个数据段的前面，加上首部后，就构成了一个分组。分组又称为“包”。分组中的首部包含了诸如目的地址和源地址等重要控制信息，而分组交换网只有从分组的首部才能获知应将此分组发往何处。

1.3 Internet 成为世界上最大的计算机网络。

1.4 N-ISDN 窄带综合业务数字网（传输速度不高）

B-ISDN 宽带综合业务数字网（传输速度高）

1.5 计算机网络定义(资源共享的角度)：

把分布在不同地理位置的计算机，通过通信系统连接起来，达到资源共享的计算机系统。

1.6 计算机网络的基本特征主要表现在：

1）计算机网络建立的目的是实现计算机资源共享

2）计算机是分布在不同地理位置的多台独立的“自治计算机”

3）连网计算机必须遵循全网统一的网络协议

1.7 计算机网络：把地理上分散的多台自治计算机互连的集合。（计算机互连必须遵循约定的通信协议）

1.8 互联网：一些相互连接的计算机网络的集合。

1.9 internet 和 Internet 区别：

internet 是普通名词，泛指一般的互联网

Internet 是专有名词，是使用 TCP/IP 协议组、前身是美国的阿帕网（ARPANET）的世界范围的互联网。

1.10 中国四大公用数据通信网：

公用分组交换数据网（ChinaPAC）、公用数字数据网（ChinaDDN）

公用帧中继网（ChinaFRN）、公用计算机互联网（ChinaNet）。

1.11 按覆盖的地理范围进行分类，计算机网络可以分为：广域网 WAN、城域网 MAN、局域网 LAN、个域网 PAN。

1.12 各网络特点：

1）广域网：几十公里到几千公里，网络覆盖范围广；传输速度低；通信设备属国家所有；对入网计算机不作限制

2）城域网：介于广域网与局域网之间的一种高速网络。其设计的目标是要满足几十公里范围内的企业、机关、公司的多个局域网互连的需求。

3）局域网：十米到一公里，覆盖范围小；传输速率高；设备为单位或个人所有；入网计算机大多为 PC。

1.13 按网络的拓扑结构分类，网络可分为：**星型、树型、总线型、环型、网状型**。

1.14 按网络控制方式分类，网络可分为：**集中式**计算机网络和**分布式**计算机网络。

1.15 集中式和分布式网络简要说明：

1）集中式网络：这种网络的处理和控制功能都高度集中在一个或少数几个结点上，所有的信息流都必须经过这些结点之一。

优点:实现简单，其网络操作系统很容易从传统的分时操作系统经适当地扩充和改造而成。

缺点:实时性差、可靠性低、缺乏较好的可扩充性和灵活性。

2）分布式网络：网络中的任一结点都至少和另外两个结点相连接，信息从一个结点到达另一结点时，可能有多条路径。同时，网络中的各个结点均以平等地位相互协调工作和交换信息，并可共同完成一个大型任务。

优点:信息处理的分布性、可靠性高、可扩充性及灵活性好。

1.16 计算机网络的组成：根据网络的定义，一个典型的计算机网络主要是由**计算机系统、数据通信系统、网络软件及协议**三大部分组成。计算机系统是网络的基本模块，为网络内其他计算机资源提供共享资源；数据通信系统是连接网络基本模块的桥梁，提供各种连接技术和信息交换技术；网络软件是网络的组织者和管理者，在网络协议的支持下，为网络用户提供各种服务。

1.17 计算机网络各模块说明：

1）计算机系统：主要完成数据信息的收集、存储、处理和输出任务，并提供各种网络资源。计算机系统根据在网络中的用途可分为服务器和工作站。

2）数据通信系统：主要由网络适配器（网卡）、传输介质和网络互联设备等组成。

3）网络软件：网络软件是实现网络功能所不可缺少的软环境。包括：网络协议和协议软件；网络通信软件；网络操作系统；网络管理及网络应用软件。

1.18 局域网组成：网络工作站；网络适配器；集线器（交换机）；传输介质；网络服务器。

1.19 广域网组成：

WAN 最基本的功能是数据通信和资源共享。从逻辑上 WAN 分成两大部分：1）**资源子网**：主要负责全网的信息处理，为网络用户提供网络服务和资源共享功能；2）**通信子网**：主要负责全网的数据通信，为网络用户提供数据传输、转接、加工和变换等通信处理工作。

1.20 通信子网：由通信控制处理机、通信线路和其他设备组成，完成网络数据传输、转发等通信处理任务。

1.21 通信控制处理机：

1）在网络拓扑结构中被称为网络结点；

2）作为与资源子网的主机、终端的连接的接口，将主机和终端连入网内；

3）作为通信子网中的分组存储转发结点，完成分组的接收、校验、存储、转发等功能；

1.22 资源子网的组成：主机、终端、终端控制器、外设、软件资源、信息资源。

1.23 计算机网络的功能：

以资源共享为目标的计算机网络，具有下列几方面功能：

A、数据通信：可以传输各种类型的信息,包括数据信息和图形、图像、声音、视频流等多媒体信息

B、资源共享：数据迁移、计算迁移

C、分布式处理：进程迁移的启动、进程迁移的内容、进程如何迁移

D、集中管理：对地理位置分散的组织和部门,可通过计算机网络来实现集中管理,如数据库情报检索系统、交通运输部门的定票系统、军事指挥系统等

E、均衡负荷：将作业分散到网络中的其它计算机中，共同完成

1.24 比特（bit）：计算机中数据量的单位，也是信息论中使用的信息量的单位，一个比特就是二进制数字中的一个 1 或 0。

1.25 速率即数据率(data rate)或比特率(bit rate)：计算机网络中最重要的一个性能指标。指连接在计算机网络上的主机在数字信道上传送数据的速率。单位：b/s　　kb/s　　Mb/s　　Gb/s

1.26 带宽与宽带：

1）带宽：指网络带宽，表示在单位时间内从网络的某节点到另一个节点所能传送的“最高数据率” ，单位是“比特每秒”，或 b/s (bit/s)（注意：kb/s=10^3 b/s）。

2）宽带线路：可通过较高数据率的线路。

1.27 宽带线路和窄带线路上比特的**传播速率是一样的**。

1.28 吞吐量：表示在单位时间内通过某个网络（或信道、接口）的数据量。

1.29 时延：指一个报文或分组从一个网络的一端传送到另一个端所需要的时间。它包括了**发送时延，传播时延，处理时延，排队时延**。即：**总时延 = 发送时延 + 传播时延 + 处理时延 + 排队时延**

1） **发送时延**:发送数据时，数据块从结点进入到传输媒体所需要的时间

2） **传播时延**:电磁波在信道中需要传播一定的距离而花费的时间。

3） **处理时延**:交换结点为存储转发而进行一些必要的处理所花费的时间。

4） **排队时延**:结点缓存队列中分组排队所经历的时延。

1.30 时延注意点

1）**对于高速网络链路，我们提高的仅仅是数据的发送速率（减小发送时延）而不是比特在链路上的传播速率**

2）提高链路带宽减小了数据的发送时延。

1.31 时延带宽积：又称为以比特为单位的链路长度，它表示这样的链路可容纳多少个比特。

时延带宽积 = 传播时延 × 带宽

1.32 利用率

1） 信道利用率：指出某信道有百分之几的时间是被利用的（有数据通过）。完全空闲的信道利用率为 0

2） 网络利用率：全网络的信道利用率的加权平均值。

信道利用率并非越高越好。

1.33 当某信道的利用率增大时，该信道引起的时延也就迅速增加。

$$D = \frac{D_0}{1-U}$$

D_0表示网络空闲时的时延，D 表示当前的时延，U 是网络利用率

信道或网络利用率过高会产后非常大的时延

1.34 电路交换

传统电话网使用电路交换。

1） 通话前先拨号建立连接。

2）通话过程中，通信双方一直占用所建立的连接。

3）通话结束后，挂机释放连接。

1.35 分组交换

在发送端把要发送的报文分隔为较短的数据块，每个块增加带有控制信息的首部构成分组，依次把每个分组发送到接收端，接收端剥去首部，抽出数据部分，还原成报文。

1.36 存储转发：报文交换、分组交换。

第二章 网络体系结构

2.1 计算机网络的体系结构：计算机网络的各层及其协议的集合。

计算机网络体系结构={系统、实体、层次、协议}

对计算机网络及其部件所完成功能的比较精确的定义。仅仅定义了网络及其部件通过协议应完成的功能；不定义协议的实现细节和各层协议之间的接口关系。

2.2 网络协议：为进行网络中的数据交换而建立的规则、标准或约定。

网络协议三要素：

(1)**语法：语法就是数据的结构或格式，也就是指数据呈现的顺序。**

(2)**语义：语义是每一部分位的意思。**

(3)**规则：有 2 个特点：数据在何时应当发送出去以及数据应当发送得多快。**

2.3 层次结构：从上至下，文件传送模块、通信服务模块、网络接入模块。

2.4 开放系统互连参考模型（OSI/RM）：

1）开放：只要遵循 OSI 标准，一个系统就可以和世界上任何地方的、也遵循这同一标准的其他任何系统进行通信。

2）系统：指按一定关系或规则工作在一起的一组物体或一组部件

3）实系统：表示在现实世界中能够进行信息处理或信息传递的自治整体，它可以是一台计算机或者多台计算机以及和这些计算机相关的软件、外部设备、终端、操作员、信息传递手段的集合。

2.5 OSI / RM 开放系统互连参考模型（Open System Interconnection/reference model）分层原则：

① 结构的层次不能太多，以免造成系统结构的繁杂；结构的层次也不能太少会使每层协议过于复杂

② 当必须区分不同类型功能群时，应设置一个层次

③ 每一层只与它相邻的上、下层发生关系，且层与层边界的选取应使通过边界的信息量尽可能少

④ 每层功能应非常明确

2.6 OSI 分层：

1）应用层：提供应用进程与通信进程之间的接口

2）表示层：在两个应用层之间的传输过程中负责数据的表示语法，关心的是语法和语义

3）会话层：负责建立（或清除）在两个通信的表示层之间的通信通道，包括交互管理、同步，异常报告。

4）传输层：提供端到端的通路，应用到应用的通路，为会话层提供与下面网络无关的可靠消息传送机制

5）网络层：提供主机到主机的通路，其间可能存在多条通路

6）链路层：提供点到点的可靠传输，通常需把数据分成帧，并且保证帧的正确发送和接收，共享网络中需解决信道共享问题。

7）物理层：与传输媒体的接口，完成传输媒体上的信号与二进制数据间的转换

对等层之间的通信为虚拟通信，实际的通信在相邻层之间通过层间接口进行。

2.7 协议和服务：

协议：计算机网络同等层次中，通信双方进行信息交换时必须遵守的规则。

服务：层间交换信息时必须遵守的规则。

2.8 服务访问点（SAP）：在同一系统中相邻两层的实体进行交换信息的地方。

任何层间服务是在接口的 SAP 上进行的

每个 SAP 有唯一的识别地址

每个层间接口可以有多个 SAP

2.9 信息传送单元：

1）协议数据单元（PDU）：协议数据单元就是在不同站点的各层对等实体之间，为实现该层协议所交换的信息单元。PDU 含 2 个部分：本层的用户数据和本层的协议控制信息。

2）接口数据单元（IDU）：在同一系统中的相邻实体的依次交互中，经过层间接口的信息单元。

3）服务数据单元（SDU）：实体为了完成服务用户所请求的功能所需要的数据单元。

2.10 通信服务可以分为两大类：

1）面向连接服务：面向连接服务是在数据交换之前，必须建立连接。数据交换结束后,则终止这个连接。

面向连接服务的优点：

A.在连接时,给出双方地址，连接成功后，给出一个连接符,在传输过程中使用连接符。

B.报文按顺序发送,质量好,不会丢失。

缺点：协议复杂，通信效率不高。

2）无连接服务:在无连接服务的情况下，两个实体之间的通信不需要先建立好一个连接。

灵活方便，但无连接服务不能防止报文的丢失，每个报文都需要提供全地址，开销大 。

无连接服务有以下三种类型：

a 数据报：它的特点不需要接收端做任何响应，因此是一种不可靠的服务。

b 证实交付：它又称为可靠的数据报。

c 请求回答：这种类型的数据报是收端用户每收到一个报文，就向发端用户发送一个应答报文。

2.11 无连接服务的特点：

- 每个分组都携带完整的目的结点地址，各分组在系统中是独立传送的；
- 数据传输过程不需要经过连接建立、连接维护与释放连接的三个过程；
- 数据分组传输过程中，目的结点接收的数据分组可能出现乱序、重复与丢失的现象；
- 可靠性不好，但是协议相对简单，通信效率较高。

2.12 TCP/IP 体系结构：

1 链路层：有时也称作数据链路层或网络接口层。

2 网络层：有时也称作互联网层，处理分组在网络中的活动。

3 运输层：主要为两台主机上的应用程序提供端到端的通信。

4 应用层：负责处理特定的应用程序细节 。

2.13 TCP/IP 协议的特点：

- 开放的协议标准;
- 独立于特定的计算机硬件与操作系统；
- 独立于特定的网络硬件，可以运行在局域网、广域网，更适用于互连网中；
- 统一的网络地址分配方案，使得整个 TCP/IP 设备在网中都具有惟一的地址；
- 标准化的高层协议，可以提供多种可靠的用户服务。

2.14 OSI 参考模型与 TCP/IP 参考模型的比较：

1）OSI 评价：

- 层次数量与内容选择不是很好，会话层很少用到，表示层几乎是空的，数据链路层与网络层有很多的子层插入；
- 寻址、流控与差错控制在每一层里都重复出现，降低系统效率；
- 数据安全性、加密与网络管理在参考模型的设计初期被忽略了；
- 参考模型的设计更多是被通信的思想所支配，不适合于计算机与软件的工作方式；
- 严格按照层次模型编程的软件效率很低。

2）TCP/IP 评价：

- 在服务、接口与协议的区别上不很清楚，一个好的软件工程应该将功能与实现方法区分开，参考模型不适合于其他非 TCP/IP 协议族；
- TCP/IP 参考模型的网络接口层本身并不是实际的一层；
- 物理层与数据链路层的划分是必要和合理的，而 TCP/IP 参考模型却没有做到这点。

2.15 标准创建委员会：在建立网络标准以确保通信和网络设备有统一的标准方面，许多美国和国际组织发挥了重要的作用。这些组织包括：

国际标准化组织（ I S O ）

国际通信联盟（ I T U ）[电信标准部（ITU-T）]

美国国家标准化局（ANSI）

电气电子工程师协会（ I E E E ）

电子工业联合会（ E I A ）

万维网联盟（W3C）

开放移动联盟（OMA）

第三章 物理层

3.1 物理层的主要任务:在两个网络设备之间提供透明的比特流传输。

3.2 OSI 的物理层定义：物理层提供机械的、电气的、功能的和规程的特性，目的是启动、维护和关闭数据链路实体之间进行比特传输的物理连接。

3.3 物理层的四个重要特性:

- 机械特性：指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等等
- 电气特性：指明在接口电缆的各条线上出现的电压的范围。
- 功能特性：指明某条线上出现的某一电平的电压表示何种意义，定义各条物理线路的功能。
- 规程特性：指明对于不同功能的各种可能事件的出现顺序。定义各条物理线路的工作规程和时序关系。

3.4 RS-232C 接口标准:提供了一个利用公用电话网络作为传输媒体，并通过调制解调器将远程设备连接起来的技术规定。规定使用一个 25 芯的标准连接器。不足：传输性能低、距离短、速率低

3.5 双绞线：由按规则螺旋结构排列的两根、四根或八根绝缘导线组成，一对线可以作为一条通信线路，各线对螺旋排列的目的是为了使之间的电磁干扰最小。分为屏蔽双绞线（STP）、非屏蔽双绞线（UTP）。按传输特性可以分为 1 类~5 类，局域网最常使用是 5 类非屏蔽的双绞线：该类电缆增加了绕线密度，外套一种高质量的绝缘材料，传输频率为 100MHz，用于语音传输和最高传输速率为 100Mbit/s 的数据传输。

1）连通性：双绞线既可用于点到点连接，也可用于多点连接。

2）地理范围：用做远程中继线时，最大距离可达 15 公里；与集线器的距离最大为 100 米，至少 0.6 米。

3）抗干扰性：双绞线的抗干扰性取决于一束线中相邻线对的扭曲长度及适当的屏蔽。

4）价格：双绞线的价格低于其它传输介质，并且安装、维护方便。

3.6 同轴电缆，由内导体、外屏蔽层、绝缘层、外部保护层组成。结构上由空芯的圆柱形外导体中包裹一根内导线构成。根据带宽不同，可以分为：宽带同轴电缆 75Ω、基带同轴电缆 50Ω。

1）连通性：可用于点-点及多点的链路结构。

2）地理范围：基带同轴电缆传输的最远距离只有几公里，宽带同轴电缆传输距离可达数十公里。

3）抗干扰性：低频段差，高频段好。

4）价格：安装同轴电缆局域网络的费用略微高于双绞线、低于光缆线的局域网络费用。但是，同轴电缆较之双绞线容量大、速率高；在大流量、重负载的场合下都很适用。其性能价格比仍为较优的。

3.7 光纤电缆，由两层折射率不同的材料所构成，是一种通过光线的细小而柔韧的传输介质。内层为具有较高折射率的玻璃或塑料单根纤维线，外层是折射率较低的材料。

1）分类：

多模光纤：存在许多条不同角度入射的光线在一条光纤中传输。

单模光纤：光纤的直径减小到只有一个光的波长，光线便会一直向前传播。

2）传输特性：光纤电缆是利用全反射的原理来传输被调制好的光信号。

3）链接方法：光纤电缆主要运用于点--点的链路。

4）距离范围：从目前的技术水平来看，光纤电缆可以在几十公里距离内不使用中继器就能进行有关信息的传输。因而，光纤较适合于在几个建筑物之间通过点-点链路实现局域网。

5）抗噪声性：光纤电缆不受电磁波的干扰或噪声的影响。

6）价格：光纤电缆局域网络比双绞线及同轴电缆局域网的费用要高得多。

3.8 非导向传输媒体：无线传输、短波通信、微波。

无线传输频段广

短波通信主要靠电离层的反射，通信质量较差

微波在空间主要是直线传播

3.9 微波信道：微波波段较高，频段范围广，信道容量大，传输质量高。相邻站之间必须直视，不能有障碍物，传播质量收天气影响较大；隐蔽性和保密性较差；需要大量中继站。

3.10 卫星信道：将微波中继站放在人造卫星上，是一种特殊的微波中继系统。通信距离远，且通信费用与通信距离无关，有较大的传播时延。

第四章 数据链路层

4.1 链路：就是一条无源的点到点的物理线路段，中间没有任何其他的交换结点。

4.2 数据链路：把实现规程的硬件软件加到链路上就构成了数据链路。

4.3 **数据链路层最重要的作用：通过一些数据链路层协议，在不太可靠的物理链路上实现可靠的数据传输**

PS：链路层只是保证了接受到的比特无差错，但不能保证比特的顺序、数量无差错（不能叫可靠传输），所以在传输层中使用 TCP 协议保证可靠传输。

4.4 为什么要设计数据链路层

- ◆ 在原始物理传输线路上传输数据信号是有差错的
- ◆ 设计数据链路层的主要目的：将有差错的物理线路改进成无差错的数据链路

  方法： 差错控制、流量控制

- 作用：改善数据传输质量，向网络层提供高质量的服务

4.5 传输差错：通过通信信道后接收的数据与发送数据不一致的现象。

4.6 差错控制：检查是否出现差错以及如何纠正差错。

4.7 通信信道的噪声分为两类：热噪声和冲击噪声。

4.8 误码率：$P_e = N_e/N$（N 为传输的二进制比特总数，N_e为被传错的比特数）

4.9 纠错码与检错码

- 纠错码：每个传输的分组带上足够的冗余信息，接收端能发现并自动纠正传输差错
- 检错码：分组仅包含足以使接收端发现差错的冗余信息，接收端能发现出错，但不能确定哪一比特是错的，并且自己不能纠正传输差错

4.10 常用的检错码：奇偶校验码、循环冗余编码 CRC

4.11 数据链路层的功能

- 链路管理
- 区分数据信息和控制信息
- 帧同步
- 可靠传输（流量控制， 差错控制）
- 透明传输
- 寻址

4.12 利用 CRC 进行检错的过程可简单描述为：

在发送端根据要传送的 m 位二进制码序列，以一定的规则产生一个校验用的 k 位监督码(CRC 码)，附在原始信息后边，构成一个新的二进制码序列数共 m+k 位，然后发送出去。在接收端，根据信息码和 CRC 码之间所遵循的规则进行检验，以确定传送中是否出错。这个规则在差错控制理论中称为“生成多项式”

4.13 停止等待协议

是一种不需要数据链路层协议、具有最简单流量控制的数据链路层协议（无差错的理想信道）

在发送结点：

(1) 从主机取一个数据帧；

(2) 将数据帧送到数据链路层的发送缓冲区；

(3) 将发送缓冲区中的数据帧发送出去；

(4) 等待；

(5) 若收到由接收结点发过来的信息 (此信息的格式与内容可由双方事先商定好)，则从主机取一个新的数据帧，然后转到(2)

在接收结点：

(1) 等待；

(2) 若收到由发送结点发过来的数据帧，则将其放入数据链路层的接收缓冲区；

(3) 将接收缓冲区中的数据帧上交主机；

(4) 向发送结点发一信息，表示数据帧已经上交给主机；

(5) 转到 (1)

4.14 实用的停止等待协议

在发送结点：

(1) 从主机取一个数据帧。

(2) V(S) ＝ 0 发送状态变量初始化

(3) N(S) ＝ V(S) 将发送状态变量的数值入发送序号将数据帧送交发送缓冲区

(4) 将发送缓冲区中的数据帧发送出去

(5) 设置超时定时器。 选择适当的超时重发时间 Tout

(6) 等待。 等待以下 3 个事件中最先出现的一个

(7) 若收到确认帧 ACK，则：从主机取一个新的数据帧；V(S) = 1－V(S) 更新发送状态变量，变为下一个序号转到(3) 。

(8) 若收到否认帧 NAK，则转到(4)。 重发数据帧

(9) 如果超时定时器时间到，则转到(4)。 重发数据帧

在接收结点：

(1) V(R) = 0 接收状态变量初始化

(2) 等待。

(3) 当收到一个数据帧，就检查有无产生传输差错(如用 CRC)若检查结果正确无误，则执行后续算法

否则转到(8)

(4) 若 N(S) = V(R)，则执行后续算法，收到发送序号正确的数据帧否则丢弃此数据帧. 然后转到(7)

(5) 将收到的数据帧中的数据部分送交主机

(6) V(R) = 1－V(R)。更新接收状态变量，准备接收下一个数据帧

(7) 发送确认帧 ACK，并转到(2)

(8) 发送否认帧 NAK，并转到(2)

4.15 停止等待协议 ARQ 的优缺点

优点：比较简单

缺点：通信信道的利用率不高，也就是说，信道还远远没有被数据比特填满

4.16 连续 ARQ 协议的工作原理

- 在发送完一个数据帧后，不是停下来等待确认帧，而是可以连续再发送若干个数据帧
- 如果这时收到了接收端发来的确认帧，那么还可以接着发送数据帧
- 由于减少了等待时间，整个通信的吞吐量就提高了

注意点：

结点 A 在每发送完一个数据帧时都要设置该帧的超时计时器。如果在所设置的超时时间内收到确认帧，就立即将超时计时器清零。但若在所设置的超时时间到了而未收到确认帧，就要重传相应的数据帧（仍需重新设置超时计时器）在等不到 2 号帧的确认而重传 2 号数据帧时，虽然结点 A 已经发完了 5 号帧，但仍必须向回走，将 2 号帧及其以后的各帧全部进行重传。该连续 ARQ 又称为 Go-Back-N ARQ，意思是当出现差错必须重传时，要向回走 N 个帧，然后再开始重传。

4.17 选择重传 ARQ 协议：

当接收方发现某帧出错后，其后继续送来的正确的帧虽然不能立即递交给接收方的高层，但接收方仍可收下来，存放在一个缓冲区中，同时要求发送方重新传送出错的那一帧。一旦收到重新传来的帧后，就可以原已存于缓冲区中的其余帧一并按正确的顺序递交高层。显然，选择重发减少了浪费，但要求接收方有足够大的缓冲区空间。

4.18 滑动窗口机制

- 发送端和接收端分别设定发送窗口和接收窗口
- 发送窗口用来对发送端进行流量控制
- 发送窗口的大小 W_T 代表在还没有收到对方确认信息的情况下发送端最多可以发送多少个数据帧

4.19 滑动窗口的重要特性

- 只有在接收窗口向前滑动时（与此同时也发送了确认），发送窗口才有可能向前滑动
- 收发两端的窗口按照以上规律不断地向前滑动，因此这种协议又称为滑动窗口协议
- 当发送窗口和接收窗口的大小都等于 1 时，就是停止等待协议
- 当用 n 个比特进行编号时，若接收窗口的大小为 1，则只有在发送窗口的大小 Wt<=2n -1 时，连续 ARQ 协议才能正确运行。这就是说，当采用 3 比特编码时，发送窗口的最大值是 7 而不是 8。

4.20 若传输信道的传输质量很差，因而误码率较大时，连续 ARQ 协议不一定优于停止等待协议

4.21 **PPP 协议：现在全世界使用得最多的数据链路层协议是点对点协议 PPP (Point-to-Point Protocol)**

- 链路控制协议 LCP：一种扩展链路控制协议，用于建立、配置、测试和管理数据链路连接
- 认证协议
- 网络控制协议 NCP：协商链路传输的数据包格式与类型，建立、配置不同的网络层协议功能：

（1）PPP 具有动态分配 IP 地址的能力；

（2）PPP 支持多种网络协议，比如 TCP/IP、NetBEUI、NWLINK 等；

（3）PPP 具有错误检测以及纠错能力，支持数据压缩；

（4）PPP 具有身份验证功能。

4.22 PPP 协议透明传输问题：目的是防止这些表面上的 ASCII 码控制符(在这里实际上已不是控制符了)被错误地解释为控制符。

4.23 PPP 协议之所以不使用序号和确认机制是出于以下的考虑：

- 在数据链路层出现差错的概率不大时，使用比较简单的 PPP 协议较为合理
- 在因特网环境下，PPP 的信息字段放入的数据是 IP 数据报。数据链路层的可靠传输并不能够保证网络层的传输也是可靠的
- 帧检验序列 FCS 字段可保证无差错接受

第五章 局域网

5.1 广域网：由于分布范围广，涉及的用户多，因此不能采用局域网的拓扑结构，而是**一般采用两级结构，通信子网和资源子网**。从计算机各组成部件的功能来看，主要功能为**网络通信**和**资源共享**。

5.2 把计算机网络中实现网络通信功能的设备及其软件的集合称为网络的通信子网，负责数据通信。

而把实现共享资源功能的设备及其软件的集合称资源子网，负责资源的存储、处理等。

5.3 从广域网角度看，通信子网由一些专用的通信处理机（节点交换机）机器运行的软件、集中器等设备和连接这些节点的通信链路组成；资源子网由上网的所有主机及其外部设备组成。

5.4 从局域网角度看，通信子网的设计一般有两种方式：**点到点通道、广播通道**。主要包括中继器、集线器、网桥、路由器网关等硬件设备。

资源子网主要由网络的服务器、工作站、共享的打印机和其他设备及相关软件所组成。资源子网的主体为网络资源设备。

5.5 局域网最主要的特点：网络为一个单位所拥有，且地理范围和站点数目均有限。

5.6 局域网具有如下的一些主要优点：

- 能方便地共享昂贵的外部设备、主机以及软件、数据。从一个站点可访问全网。
- 便于系统的扩展和逐渐地演变，各设备的位置可灵活调整和改变。
- 提高了系统的可靠性、可用性。

5.7 局域网的拓扑：**星形网（中心节点）、总线网（匹配电阻）、环形网（干线耦合器）、树形网（匹配电阻）**。

5.8 LAN 的结构主要由三种类型：**以太网、令牌环、令牌总线**。

5.9 IEEE802 参考模型

由于**局域网**只是一个计算机通信网，且局域网不存在路由选择问题，故**不需要网络层**，只有最低的两个层

次。然而局域网的种类繁多，其媒体接入控制的方法也各不相同，不像广域网那样简单。为了使局域网中的数据链路层不致过于复杂，就应当将局域网的数据链路层划分为两个子层：**MAC 和 LLC** 即：媒体接入控制或媒体访问控制 MAC 子层和逻辑链路控制 LLC 子层，而网络的服务访问点 SAP 则在 LLC 层与高层的交界面上

5.10 与接入各种传输媒体有关的问题都放在 MAC 子层，负责在物理层的基础上进行无差错的通信。MAC 子层的主要功能是：

1、将上层交下来的数据封装成帧进行发送(接收时进行相反的过程，将帧拆卸)

2、实现和维护 MAC 协议

3、比特差错检测

4、寻址

5.11 数据链路层中与媒体接入无关的部分都集中在逻辑链路控制 LLC 子层。LLC 子层的主要功能是：

1、建立和释放数据链路层的逻辑连接

2、提供与高层的接口

3、差错控制

4、给帧加上序号

5.12 在网络中的进程通信时，需要有以下两种地址：

1) **MAC 地址**，即主机在网络中的站地址或物理地址，这由 负责传送。

2) **SAP 地址**，即进程在某一主机中的地址，也就是 LLC 子层上面的服务访问点 SAP，这由 LLC 帧负责传送。

5.13 在局域网中，媒体接入控制 MAC 子层的地址较为复杂“名字指出我们所要寻找的那个资源，地址指出那个资源在何处,路由告诉我们如何到达该处。”802 标准为局域网上的每一个站规定了一种 48 比特的全局地址。当一个站接入到另一个局域网时，其全局地址并不改变。这就表明，802 标准所说的“地址”严格地讲应当是每一个站的“名字”或标识符

5.14 **MAC 地址具有唯一性**，取决于你所使用的网络设备。

5.15 MAC 子层基本工作过程

1）发送数据：

- ✓ 计算校验码
- ✓ 组装成数据帧
- ✓ 竞争总线
- ✓ 发送数据帧

2）接收数据：

- ✓ 接收数据帧到缓冲区
- ✓ 数据帧检错

- ✓ 是否为本机接收
- ✓ 递交网络层

5.16 **最初的以太网是将许多计算机都连接到一根总线上**。当初认为这样的连接方法既简单又可靠，因为总线上没有有源器件

5.17 以太网的广播方式发送

总线上的每一个工作的计算机都能检测到 B 发送的数据信号

由于只有计算机 D 的地址与数据帧首部写入的地址一致，因此只有 D 才接收这个数据帧

其他所有计算机（A,C 和 E）都检测到不是发送给它们的数据帧，因此就丢弃这个数据帧而不能够收下来

具有广播特性的总线上实现了一对一的通信

5.18 以太网采取了两种重要的措施：

1.采用较为灵活的**无连接**的工作方式，即不必先建立连接就可以直接发送数据。

2.以太网对发送的数据帧**不进行编号**，也**不要求对方发回确认**。

（理由是局域网信道的质量很好，因信道质量产生差错的概率是很小的）

5.19 以太网提供的服务

- ◆ 以太网提供的服务是**不可靠的交付**，即尽最大努力的交付
- ◆ 当目的站收到有差错的数据帧时就丢弃此帧，其他什么也不做。差错的纠正由高层来决定
- ◆ 如果高层发现丢失了一些数据而进行重传，但以太网并不知道这是一个重传的帧，而是当作一个新的数据帧来发送

5.20 在以太网中采用竞争策略获得信道。

以太网的工作原理可以概括为：先听后发、边听边发、冲突停止、延迟重发

监听方式：**不监听、发前监听、发时监听**

5.21 载波监听多路访问/冲突检测协议（CSMA/CD）

一种 CSMA 的改进方案是使发送站点传输过程中仍继续监听媒体，以检测是否存在冲突。如果发生冲突，信道上可以检测到超过发送站点本身发送的载波信号的幅度，由此判断出冲突的存在。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，用以通知总线上其它各有关站点。这样，通道容量就不致因白白传送已受损的帧而浪费，可以提高总线的利用率。

5.22 CSMA/CD 重要特性

- ◆ 使用 CSMA/CD 协议的以太网不能进行全双工通信而只能进行双向交替通信（**半双工通信**）。
- ◆ 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。
- ◆ 这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率。

5.23 CSMA/CD 的代价是用于检测冲突所花费的时间。最坏情况下，对 CSMA/CD 来说，检测出冲突的时间等于任意两个站之间最大传播时延的两倍

5.24 争用期

最先发送数据帧的站，在发送数据帧后至多经过时间 2τ（两倍的端到端往返时延）就可知道发送的数据帧是否遭受了碰撞。

以太网的端到端往返时延 2τ 称为争用期，或碰撞窗口。

经过争用期这段时间还没有检测到碰撞，才能肯定这次发送不会发生碰撞

长度

- 以太网取 51.2 μs 为争用期的长度。
- 对于 10 Mb/s 以太网，在争用期内可发送 $10*10^6*51.2*10^{-6}$=512 bit，即 64 字节。
- 以太网在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。
- 如果发生冲突，就一定是在发送的前 64 字节之内。
- 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节。
- 以太网规定了最短有效帧长为 64 字节，凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧

5.25 重发策略

一个站在发现冲突后，应立即停止本次发送，重新安排发送。有多种重发策略。目前常用策略有以下 3 种

(1)随机策略：工作站在发现冲突后，推迟一随机时间，再进行重发。

(2)二进制指数退避算法 BEB：重发的延迟时间是均匀地分布在 0~T_{BEB}之间，这里 $T_{BEB} = 2^{i-1}(2\tau)$

(3)截断式二进制指数退避算法：

该算法是对前一算法的改进，它仍然采用二进制指数退避策略，但当重发时延增加到一定大小时便停止后退，以后的多次重发延迟时间 T_{BEB}均采用这个时间。

5.26 常用的以太网 MAC 帧格式有两种标准

DIX Ethernet V2 标和 IEEE 的 802.3 标准，最常用的 MAC 帧是以太网 V2 的格式

5.27 当数据字段的长度小于 46 字节时，应在数据字段的后面加入整数字节的填充字段，以保证以太网的 MAC 帧长不小于 64 字节。

5.28 为了达到比特同步，在传输媒体上实际传送的要比 MAC 帧还多 8 个字节

5.29 无效的 MAC 帧

- 数据字段的长度与长度字段的值不一致；
- 帧的长度不是整数个字节；
- 用收到的帧检验序列 FCS 查出有差错；
- 数据字段的长度不在 46 - 1500 字节之间。

◆ 有效的 MAC 帧长度为 64 -1518 字节之间。

对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

5.30 令牌组成：SD，令牌帧的起始符；AC，访问控制字节；ED，令牌帧的结束符。

5.31 帧的发送

当一个站要发送数据时，要先将数据形成信息帧并存放在发送缓冲区中，然后命令环接口去截获令牌。环接口不断地检测环路中流动的比持流，当发现有令牌帧时，将令牌截获下来，接着便可将发送缓冲区中已准备好的帧送入环路。令牌环网允许一个站连接发送多个帧，只要不超过规定的占用令牌的最大时间。发送站把信息发送完后并不立即释放令牌，还需等待其所发出的帧返回本站后，方可释放令牌。

5.32 帧的接收和转发

帧在环路中传送时，每经过一个环接口，便由该接口检查该帧中的目标地址。若是本站地址，接口便将该帧复制下来。由于一个帧可发送给多个目标站，因此在复制该帧的同时，还需特它转发给下一站。若帧中的目标地址不是本站站址，则只需将该帧向下一站转发而不复制。帧在环路中如此逐个环接口地转发，直至返回到发出该帧的源站为止。

5.33 帧的撤销和重发

当环路中传送的帧返回源站后，由源站再对该帧进行检查。如果发现该帧已被目标站接收，便将它从环路中撤消，若此时又无数据帧要发送，便可将令牌传送给下一站。但若发现目标站因忙而末将该帧复制下来时，源站还应再次发送该帧。对于重发帧，目标站在识别后必须予以接收。显然，目标站在将该帧复制后，必须在该帧中置以标志。

5.34 令牌总线网：将局域网物理总线的站点构成一个逻辑环，每一个站点都在一个有序的序列中被指定一个逻辑位置，序列中最后一个站点的后面又跟着第一个站点。每个站点都知道在它之前的前趋站和在它之后的的后继站标识。

5.35 令牌总线工作原理

在正常运行时，当站点做完该做的工作或者时间终了时，它将令牌传递给逻辑序列中的下一个站点。

1、从逻辑上看，令牌是按地址的递减顺序传送至下一个站点的。

2、从物理上看，带有目的的令牌帧广播到总线上所有的站点的，当目的站点识别出符号它的地址，即把该令牌帧接收。

5.36 令牌

为了控制网络上各站对总线的访问，在网络中设置了一个令牌，任何工作站都仅在它持有令牌时才有权向总线上发送信息，而其余未获得令牌的站，只能监听总线或从总线上收信息。由于在总线网中只设置一个令牌. 在任何时到也只有一个工作站访问信道，因而不会发生访问冲突。实际上，令牌本身是一种特殊的帧。其中：PRE 为前导码，SD 和 ED 分别是起始和结束定界符，TS 和 NS 是本地址和下一站地址，令牌帧的控制码是

00001000。

5.37 令牌传递方式

网上各工作站在发送信息之前，必须先获得令牌，信息发送完后应立即交出令牌并将之传递给另一个站。在令牌总线中令牌的传递在逻辑上是顺序的，且以地址从大到小的递减方式传递，即令牌放从高地址站传递给较低地址的站，当令牌到达最低地址的站后，又返回去传送给最高地址的站。这样，所有传递令牌的站将构成一个逻辑环。

实现方法

为能正确地传递令牌，应使环内的每个站除知道本站地址(TS)外，还需知道其上一站的地址(PS)和下一站的地址(NS)。占有令牌的站在将令牌传递给下一站时，应以广播发送方式将令牌发送到总线上。这样，总线上所有工作站都能收到该令牌，再将本站地址与帧中的 NS 比较，若不相同,表明本站不是令牌发送帧的下一站，于是放弃收到的令牌；若相同，便将令牌收下

5.38 交换机的任务：

1.地址表学习：建立交换表。交换机的端口都具有编号，假设从某个端口 p 来的数据帧，则该数据帧中的源地址和 p 关联

2.帧的转发和过滤：进行数据交换

5.39 交换式集线器的交换方式：

1、存储转发交换 ：采用这种方式时，集线器就像一个分组结点交换机。它从一个输入端口收下一个帧，暂存后即根据其目的地址转发到适当的输出端口。

2、直通交换：这种方式利用了目的地址处于 MAC 帧的最前面这一特点，直通交换不必将整个数据帧先缓存后再进行处理，而是在接收数据帧的同时就立即按数据帧的目的地址决定该帧的转发端口，这就使得转发速度大大提高。对于多媒体应用，直通式交换是一种很好的方法。直通交换的一个缺点是它不检查 CRC 就直接将帧转发出去，因此有可能也将一些无效帧转发给其他的站

5.40 高速以太网

1.100 比特以太网：100Mb/s，全双工，争用期为 5.12μs，一个网段最大电缆长度 100m

2.吉比特以太网：1Gb/s，全双工或半双工（CSNA/CD 协议）

3.10 吉比特以太网：光纤传输，全双工，无争用，不使用 CSMA/CD 协议

5.41 使用高速以太网进行宽带接入

以太网接入的重要特点是它可提供双向的宽带通信，并且可根据用户对带宽的需求灵活地进行带宽升级。

采用以太网接入可实现端到端的以太网传输，中间不需要再进行帧格式的转换。这就提高了数据的传输效率和降低了传输的成本

5.42 交换机和集线器的区别

1、从 OSI 体系结构来看， **集线器属于 OSI 的物理层设备**，而**交换机属于 OSI 的数据链路层设备**。

2、 **集线器是一种广播模式**，集线器的某个端口工作时，其他所有端口都能够收听到信息，容易产生广播风暴。当**交换机**工作的时候，只有发出请求的端口和目的端口之间**相互响应**而不影响其他端口， 因此交换机就能够隔离冲突域和有效的抑制广播风暴的产生。

3、从带宽来看，**集线器不管有多少个端口，所有端口都是共享一条带宽**，在同一时刻只能有一个端口传送数据，其他端口只能等待，同时集线器只能工作在**半双工模式**下；而**交换机每个端口都有一条独占的带宽，**当二个端口工作时并不影响其他端口的工作，同时交换机不但可以工作在**半双工模式下而且可以工作在全双工模式**下。

5.43 交换式局域网技术特点：低交换延迟；支持不同的传输速率和工作模式；支持虚拟局域网服务。

5.44 虚拟局域网 VLAN ：由一些局域网网段构成的与物理位置无关的逻辑组。

5.45 用集线器扩展局域网（物理层）

- 优点：使原来属于不同碰撞域的局域网上的计算机能够进行跨碰撞域的通信、扩大了局域网覆盖的地理范围。
- 缺点：碰撞域增大了，但总的吞吐量并未提高；如果不同的碰撞域使用不同的数据率，那么就不能用集线器将它们互连起来。

5.46 使用网桥/交换机拓展局域网（数据链路层）。

网桥工作在数据链路层，它根据 MAC 帧的目的地址对收到的帧进行转发。具有过滤帧的功能。当网桥收到一个帧时，并不是向所有的端口转发此帧，而是先检查此帧的目的 MAC 地址，然后再确定将该帧转发到哪一个端口

5.47 网桥功能

地址映射表学习：采用逆向学习。

数据帧转发：根据数据帧中的目标 MAC 地址，查询地址映射表，从指定的端口转发数据帧，如果没有找到目的端口，则采用广播方式转发；如果源端口和目的端口所接网络类型不同，则需要进行数据帧转换。

环路避免

5.48 网桥好处：过滤通信量、扩大了物理范围、提高了可靠性、可互连不同物理层和不同 MAC 子层和不同速率（如 10 Mb/s 和 100 Mb/s 以太网）的局域网。

5.49 网桥缺点

- 存储转发增加了时延。
- 在 MAC 子层并没有流量控制功能。
- 具有不同 MAC 子层的网段桥接在一起时时延更大。

- 网桥只适合于用户数不太多(不超过几百个)和通信量不太大的局域网，否则有时还会因传播过多的广播信息而产生网络拥塞。这就是所谓的广播风暴。

5.50 网桥和集线器对比

- **集线器在转发帧时，不对传输媒体进行检测**。
- **网桥在转发帧之前必须执行 CSMA/CD 算法**。
  - 若在发送过程中出现碰撞，就必须停止发送和进行退避。
  - 在这一点上网桥的接口很像一个网卡，但网桥却没有网卡。
- 由于网桥没有网卡，因此**网桥并不改变它转发的帧的源地址**。

5.51 用以太网交换机拓展局域网

5.52 交换机的三个主要功能：**地址学习；帧的转发/过滤；回路防止**（有几个交换机时）。

5.53 广播风暴问题：产生转发的帧在网络中不断兜圈子

5.54 生成树算法

每隔几秒钟每一个网桥要广播其标识号(由生产网桥的厂家设定的一个惟一的序号)和它所知道的其他所有在网上的网桥。

支撑树算法选择一个网桥作为支撑树的根(例如，选择一个最小序号的网桥)，然后以最短路径为依据，找到树上的每一个结点。

当互连局域网的数目非常大时,支撑树的算法很花费时间。这时可将大的互连网划分为多个较小的互连网，然后得出多个支撑树

5.55 网络拓扑与对应的生成树

每个网桥广播其序号

序号最小的作为根

从根按最短路径构造生成树

第六章 网络层

★网络层概述

1.概念：网络层是 OSI 参考模型中的第三层，主要任务是为传输层提供服务，跨越不同的网络将传输层的数据送达到目的地。

2.网络层主要功能

- **路由控制**：利用网络的拓扑结构等网络状态，选择分组传送路径
- **拥塞控制**：控制和预防网络中出现过多的分组
- **异种网络的互连**：解决不同网络在寻址、分组大小、协议等方面的差异

3.提供服务：**面向连接服务（虚电路服务）**、**无连接服务（数据包服务）**，依靠网络层数据传输方式不同实现。传输方式：数据报、虚电路。

4.数据报传输过程

- 网络随时接受主机发送的分组（即数据报），为每个分组独立的选择路由
- 网络尽最大努力将分组交付给目的主机，但对源主机没有任何承诺
- 网络不保证所传输的分组不丢失，也不保障按主机发送分组的先后顺序以及在时限内必须将分组交付给主机
- 当网络发生拥塞时，网络中的结点可根据情况将一些分组丢弃
- 数据报提供的服务是不可靠的，“尽最大努力交付”的服务，即没有质量保证的服务

5.虚电路传输过程

在虚电路建立后，网络向用户提供的服务就好像在两个主机之间建立一对穿过网络的数字管道。所有发送的分组都按顺序进入管道，然后按照先进先出的原则沿着此管道传送到目的站主机。到达目的站的分组顺序就与发送时的顺序一致，因此网络提供虚电路服务对通信的服务质量有较好的保证

6.虚电路转发表在建立虚电路时确定，分组在传输时只需携带虚电路号，其只具有本地意义，根据虚电路建立顺序由各主机、各结点自主排序，入出口号不一定相同。

虚电路服务与数据报服务的对比

对比的方面	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不需要
终点地址	仅在连接建立阶段使用，每个分组使用短的虚电路号	每个分组都有终点的完整地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
当结点出故障时	所有通过出故障的结点的虚电路均不能工作	出故障的结点可能会丢失分组，一些路由可能会发生变化
分组的顺序	总是按发送顺序到达终点	到达终点时不一定按发送顺序
端到端的差错处理和流量控制	可以由网络负责，也可以由用户主机负责	由用户主机负责

★IP 地址

1.网际 IP 是 TCP/IP 体系中最重要的两个协议之一，与 IP 协议配套使用的还有四个协议：

- 地址解析协议 ARP (Address Resolution Protocol)
- 逆地址解析协议 RARP (Reverse Address Resolution Protocol)
- 网际控制报文协议 ICMP (Internet Control Message Protocol)
- 网际组管理协议 IGMP (Internet Group Management Protocol)

2.网际层的 IP 协议及配套协议

- 应用层　　HTTP　FTP　SMTP
- 运输层　　TCP　UDP
- 网络层　　ICNP　IGMP　RARP　ARP

3.IP 地址：就是给每个连接在因特网上的主机或路由器分配一个在全世界范围是唯一的 32 位标识符。

现在由因特网名字与编号分配公司 ICANN 进行分配。

4.IP 地址的编址方式：分类的 IP 地址、子网的划分、构成超网（无分类编址）。

IP 地址：由网络号（net-id）、主机号（host-id）组成。网络号标志主机或路由器所连接到的网络，主机号标志该主机或路由器。

各类网络地址范围

A 类：8+24　　网络号字段 1 字节　主机号字节 3 字节

B 类：16+16　　网络号字段 2 字节　主机号字节 2 字节

C 类：24+8　　网络号字段 3 字节　主机号字节 1 字节

D 类：多播地址

E 类：保留为今后使用

5.点分十进制计法：机器中存放的 IP 地址是 32 位二进制代码，每 8 位插入一个空格能提高可读性，每 8 位的二进制数转换为十进制数，方便记忆。

6.IP 地址的重要特点：

- IP 地址是分级的地质结构

  IP 地址管理机构只分配网络号，剩下的主机号由得到该网络号的单位自行分配

  路由器仅根据目的主机所连接的网络号转发分组，较少路由表项目数及占用的存储空间

- 实际上 IP 地址是标志一个主机或路由器和一条链路的接口
- 用转发器或网桥连接起来的若干局域网仍为一个网络，这些局域网具有相同的网络号
- 所有分配到网络号的网络，范围无论大小都是平等的
- 路由器总是具有两个或以上的 IP 地址，每一个接口都有一个不同网络号的 IP 地址

7.特殊作用的 IP 地址

- 私有地址

  多用于企业内部，不与外部连接，当接入 Internet 时要使用地址翻译 NAT 将其翻译成公用合法地址

  10.0.0.0 到 10.255.255.255

  172.16.0.0 至 172.31.255.255

  192.168.0.0 至 192.168.255.255

- 环回地址

  127 网段的所有地址都称为环回地址，主要用来测试网络协议是否工作正常的作用。

- 网络号为 0 的 IP 地址

  当某个主机向同一网段上的其他主机发送报文时就可以使用这样的地址，分组也不会被路由器转发

- 直接广播地址——主机号为全 1

  一个网络中的最后一个地址为直接广播地址，也就是 host-id 全为 1 的地址。主机使用这种地址把一个 IP 数据报发送到本地网段的所有设备上，路由器会转发这种数据报到特定网络上的所有主机。（这个地址在 IP 数据报中只能作为目的地址）

- 受限广播地址 255.255.255.255

  广播通信是一对所有的通信方式。若一个 IP 地址的 2 进制数全为 1，也就是 255.255.255.255，则这个地址用于定义整个互联网。

- 多播地址

  多播地址用在一对多的通信中，是从单个源地址把分组发送到一组目的设备，属于分类编址中的 D 类地址。（只能用作目的地址，不能用作分组中的源地址）

★IP 分组交付

1.分组交付可以分为直接交付和间接交付两类

直接交付：分组的源主机和目的主机在同一网络，或转发是在最后一个路由器与目的主机之间时。

间接交付：目的主机与源主机不在同一个网络上，或者路由器没有和目标主机连接在同一个网络上。

2.IP 地址解析协议 ARP（基于 IP 地址解析 MAC 地址）

不管网络层是用的是什么协议，在实际的网路链路上传送数据帧时，最终还必须使用硬件地址。

每一个主机都设有一个 ARP 高速缓存，里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表

当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。如有，就可查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址。

3.ARP 的作用

为了减少网络上的通信量，主机 A 在发送 ARP 请求分组时，就将 A 的 IP 地址到硬件地址的映射写入 ARP 请求分组；当主机 B 收到 A 的阿人品请求分组时，将 A 的地址映射写入 B 的高速缓存中

ARP 只能实现同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射

如果所要找的主机和源主机不同 LAN，则通过 ARP 找到某个本 LAN 上的路由器的硬件地址，把分组发送到这个路由器，让其把分组转发到下一个网络

4.反向地址解析协议 RARP

使只知道自己硬件地址的主机能够知道其 IP 地址，这种主机往往是无盘工作站

5.判断源地址和目标主机是否在同一个网络内

- 在同一个网络内
  - （1） 源主机网络层在 ARP 缓存中查找目标 IP 的 MAC 地址，如查找不到，则通过 ARP 模块查找
  - （2） 源主机构建数据帧，设置目的主机的 MAC 地址并发送
- 不在同一个网络内
  - （1） 源主机网络层查找网关的 IP 地址
  - （2） 在 ARP 缓存中查找目标 IP 的 MAC 地址，如查找不到，则通过 ARP 模块查找
  - （3） 源主机构建数据帧，设置目的主机的 MAC 地址并发送

★路由

1.路由选择：通信子网中的网络节点在收到一个分组后，根据分组中的目标地址以及当前子网的环境， 确定该分组转发的合适的路径。通常包括两个方面：路由表的构造、通过查找路由表决定 IP 分组的转发路径。

2.路由选择策略

静态路由选择策略：即非自适应路由选择，简单，开销较小，但不能及时适应网络状态的变化

分类：洪泛路由选择、固定路由选择、随机路由选择

动态路由选择策略：即自适应路由选择，能较好地适应网络状态的变化，但实现起来较为复杂，开销大

节点的路由选择能够依靠网络的当前状态信息决定

分类：集中路由选择、分布路由选择、混合路由选择

步骤：

测量并感知网络状态，主要包括拓扑结构、流量及延迟；

向有关进程或节点报告测量结果；

根据测量结果更新路由表；

根据新路由表重选合适路由转发数据分组

3.路由表：包含目标 IP 地址、网络掩码、网关、接口、跃点数。

目标 IP 地址：目标主机、子网地址、网络地址或默认路由

网络掩码：与目标位置结合使用以决定使用路由的时间

网关：数据包需要发送到的下一个路由器的 IP 地址

接口：表明用于接通下一个路由器的 LAN 或请求拨号接口

跃点数：表明使用本路由到达目标位置的相对成本。常用指标为跃点，或到达目标位置所通过的路由器数目。如果有多个相同目标位置的路由，跃数最低的路由为最佳路由。

4.决定路径的步骤

- 将 IP 封包的目的 IP 地址与路由记录的网络掩码做位 AND 运算。
- 将上述结果与路由记录的目的 IP 地址比较，若两者相同，才代表 IP 封包适用该路由记录。若找不到任何适用的记录，则使用默认路由，亦即将封包转送给默认的路由器来处理。
- 若某个目标地址，有多个路径都可以转发，则取掩码长的，即 1 最多的，这是因为 Netmask 字段的 1 愈多，代表目的网络的规模愈小，因此路径较为精确。
- 如果出现 3 也不能识别，则以 Metric 值最小的记录。Metric 值代表路径的成本，因此路由器会优先使用成本较低的路径。

★子网划分

1.子网划分：在 IP 地址中又增加了一个“子网号字段”，使两级的 IP 地址变成为三级的 IP 地址。

2.基本思路：

纯属一个单位内部的事情，单位对外仍表现为没有划分子网的网络。

从主机号借用若干比特作为子网号 subnet-id，而主机号相应减少若干比特

凡事从其他网络发送给本代为某个主机的 IP 数据报，仍然是根据目标网络号先找到连接在本单位的路由器，此路由器收到 IP 数据报后，按目的网络号和子网号找到目的子网，最后将 IP 数据报直接交付给目的主机

3.IP 地址 AND 子网掩码 =网络地址

4.子网划分后子网与主机的数量

如果网络位向主机位借了 n 位，那么可以划分子网的个数就是 2 的 n 次方。

如果 m 是网络位向主机位借位后所剩的主机位数，那么每个子网的主机个数就是 2 的 m 次方-2。(-2 是指减掉网络地址和广播地址）

★无分类域间路由选择 CIDR

1.CIDR 最主要的特点

CIDR 消除了传统的 A 类、B 类和 C 类地址以及划分子网的概念，因而可以更加有效地分配 IPv4 的地址空间。

IP 地址从三级编址（使用子网掩码）又回到了两级编址。

2.无分类的两级编址：CIDR 将网络前缀都相同的连续的 IP 地址组成 CIDR 地址快

IP 地址=网络前缀 + 主机号

CIDR 还使用“斜线记法” (slash notation)，它又称为 CIDR 记法，即在 IP 地址后面加上一个斜线“ /”，然后写上网络前缀所占的比特数（这个数值对应于三级编址中子网掩码中比特 1 的个数） 191.128.10.0/24

3.最长前缀匹配

用 CIDR 时，路由表中的每个项目由“网络前缀”和“下一跳地址”组成。在查找路由表时可能会得到不止一个匹配结果。应当从匹配结果中选择具有最长网络前缀的路由：最长前缀匹配。网络前缀越长，其地址块就越小，因而路由就越具体。最长前缀匹配又称为最长匹配或最佳匹配。

4.超网（子网汇聚）就是主机位向网络位借位，把一些小网络组合成一个大网络。换言之，就是减少网络位，增加主机位。子网汇聚相当于子网划分的逆运算，实际应用中是为了减轻路由表的负载而引进地址汇聚的概念

★IP 协议

1.IP 数据报格式：**一个 IP 数据报由首部和数据部分两部分组成。首部的前一部分是固定长度，共 20 字节，**是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，

其长度是可变的

2. IP 首部的可变部分就是一个选项字段，用来支持排错、测量以及安全等措施，内容很丰富。选项字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。增加首部的可变部分是为了增加 IP 数据报的功能，但这同时也使得 IP 数据报的首部长度成为可变的。这就增加了每一个路由器处理数据报的开销。实际上这些选项很少被使用

★因特网的路由选择协议

1.因特网采用分层次的路由选择协议。

2.自治系统 AS：在单一的技术管理下的一组路由器，而这些路由器使用一种 AS 内部的路由选择协议和共同的度量以确定分组在该 AS 内的路由,同时还使用一种 AS 之间的路由选择协议以确定分组在 AS 之间的路由。

3.因特网两大类路由选择协议

内部网关协议 IGP (Interior Gateway Protocol)，即在一个自治系统内部使用的路由选择协议。目前这类路由选择协议使用得最多，如 RIP 和 OSPF 协议。

外部网关协议 EGP (External Gateway Protocol)，若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。这样的协议就是外部网关协议 EGP。在外部网关协议中目前使用最多的是 BGP-4。

4. 自治系统之间的路由选择也叫做域间路由选择，在自治系统内部的路由选择叫做域内路由选择

5.内部网关协议 RIP 工作原理

路由信息协议 RIP 是内部网关协议 IGP 中最先得到广泛使用的协议，是一种分布式的基于距离向量的路由选择协议。RIP 协议要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离记录。

6.距离：从一路由器到直接连接的网络的距离定义为 1。从一个路由器到非直接连接的网络的距离定义为所经过的路由器数加 1。RIP 协议中的“距离”也称为“ 跳数” (hopcount)，因为每经过一个路由器，跳数就加 1。这里的“距离”实际上指的是“最短距离”。RIP 允许一条路径最多只能包含 15 个路由器。“距离”的最大值为 16 时即相当于不可达。可见 RIP 只适用于小型互联网。RIP 不能在两个网络之间同时使用多条路由。RIP 选择一个具有最少路由器的路由（即最短路由），哪怕还存在另一条高速(低时延)但路由器较多的路由 RIP 认为一个好的路由就是它通过的路由器的数目少，即“距离短

7.RIP 协议的三个要点

仅和相邻路由器交换信息。

交换的信息是当前本路由器所知道的**全部信息**，即自己的路由表。

按**固定的时间间隔交换路由信息**，例如，每隔 30 秒。

8.如何根据 RIP 更新路由表

收到相邻路由器（其地址为 X）的一个 RIP 报文：

(1) 先修改此 RIP 报文中的所有项目：把“下一跳”字段中的地址都改为 X，并把所有的“距离”字段的值加 1。

(2) 对修改后的 RIP 报文中的每一个项目，重复以下步骤：

若项目中的目的网络不在路由表中，则把该项目加到路由表中。

否则

若下一跳字段给出的路由器地址是同样的，则把收到的项目替换原路由表中的项目。

否则

若收到项目中的距离小于路由表中的距离，则进行更新

否则

什么也不做。

(3) 若 3 分钟还没有收到相邻路由器的更新路由表，则把此相邻路由器记为不可达路由器，即将距离置为 16（距离为 16 表示不可达）。

(4) 返回

9.RIP 协议的优缺点

RIP 存在一个问题是当网络出现故障时，要经过比较长的时间才能将此信息传送到所有的路由器。

RIP 协议最大的优点就是实现简单，开销较小。

RIP 限制了网络的规模，它能使用的最大距离为 15（16 表示不可达）。

路由器之间交换的路由信息是路由器中的完整路由表，因而随着网络规模的扩大，开销也就增加。

10.内部网关协议 OSPF 基本特点

“开放”表明 OSPF 协议不是受某一家厂商控制，而是公开发表的。

“最短路径优先”是因为使用了 Dijkstra 提出的最短路径算法 SPF

OSPF 只是一个协议的名字，它并不表示其他的路由选择协议不是“最短路径优先”。

是分布式的链路状态协议。

11.OSPF 三个要点

- 向本自治系统中所有路由器发送信息，这里使用的方法是洪泛法。
- 发送的信息就是与本路由器相邻的所有路由器的链路状态。

  “链路状态”就是说明本路由器都和哪些路由器相邻，以及该链路的“度量”(metric)。
- 只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送此信息。

12.链路状态数据库：由于各路由器之间频繁地交换链路状态信息，因此所有的路由器最终都能建立一个链路状态数据库。这个数据库实际上就是全网的拓扑结构图，它在全网范围内是一致的（这称为链路状态数据库的同步）。

13.外部网关协议 BGP：是不同自治系统的路由器之间交换路由信息的协议

14.路由器：是一种具有多个输入端口和多个输出端口的专用计算机，其任务是转发分组。也就是说，将路由器某个输入端口收到的分组，按照分组要去的目的地（即目的网络），把该分组从路由器的某个合适的输出端口转发给下一跳路由器。下一跳路由器也按照这种方法处理分组，直到该分组到达终点为止。

输入端口分组的处理：数据链路层剥去帧首部和尾部后，将分组送到网络层的队列中排队等待处理。这会产生一定的时延。

输出端口对分组的处理：当交换结构传送过来的分组先进行缓存。数据链路层处理模块将分组加上链路层的首部和尾部，交给物理层后发送到外部线路

分组丢弃：若路由器处理分组的速率赶不上分组进入队列的速率，则队列的存储空间最终必定减少到零，这就使后面再进入队列的分组由于没有存储空间而只能被丢弃。路由器中的输入或输出队列产生溢出是造成分组丢失的重要原因。

★因特网的路由选择协议 ICMP

1.目的是提高数据报交付成功的机会。

ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告。

ICMP 不是高层协议，而是 IP 层的协议。

ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去

2. ICMP 报文

ICMP 报文的种类有两种，即 ICMP 差错报告报文和 ICMP 询问报文。

ICMP 报文的前 4 个字节是统一的格式，共有三个字段：即类型、代码和检验和。接着的 4 个字节的内容与 ICMP 的类型有关。

3.CMP 差错报告报文共有 5 种：**终点不可达、源站抑制、时间超 、参数问题、改变路由（重定向）**

4.不应发送 ICMP 差错报告报文的几种情况

- 对 ICMP 差错报告报文不再发送 ICMP 差错报告报文。
- 对第一个分片的数据报片的所有后续数据报片都不发送 ICMP 差错报告报文。
- 对具有多播地址的数据报都不发送 ICMP 差错报告报文。
- 对具有特殊地址（如 127.0.0.0 或 0.0.0.0）的数据报不发送 ICMP 差错报告报文。

5.常用的 ICMP 询问报文有 2 种

- 回送请求和回答报文
- 时间戳请求和回答报文

6.ICMP 应用：PING，用来测试两个主机之间的连通性，是应用层直接使用网络层 ICMP 的例子，没有通过传输层的 TCP 或 UDP。

★因特网的路由选择协议 ICMP

1.IP 多播：可明显减少网络中资源的消耗

(1) 多播使用组地址，IP 使用 D 类地址支持多播。多播地址只能用于目的地址，而不能用于源地址。

(2) 永久组地址——由因特网地址与编码管理委员会 IANA 负责指派。

(3) 动态的组成员

(4) 使用硬件进行多播

2.IP 多播需要两种协议

为了使路由器知道多播组成员的信息，需要利 用 网 际 组 管 理 协 议 IGMP

连接在局域网上的多播路由器还必须和因特网上的其他多播路由器协同工作，以便把多播数据报用最小代价传送给所有的组成员。这就需要使用多播路由选择协议

3.几种多播路由选择协议：距离向量多播路由选择协议 DVMRP、基于核心的转发树 CBT、开放最短通路优先的多播扩展 MOSPF、协议无关多播-稀疏方式 PIM-SM、协议无关多播-密集方式 PIM-DM。

4.组播路由协议在路由器之间交流组信息。

5.网际组管理协议 IGMP

本地使用范围

IGMP 并非在因特网范围内对所有多播组成员进行管理的协议。

IGMP 不知道 IP 多播组包含的成员数， 也不知道这些成员都分布在哪些网络上。

IGMP 协议是让连接在本地局域网上的多播路由器知道本局域网上是否有主机（严格讲，是主机上的某个进程）参加或退出了某个多播组。

两个阶段：

第一阶段：当某个主机加入新的多播组时，该主机应向多播组的多播地址发送 IGMP 报文，声明自己要成为该组的成员。本地的多播路由器收到 IGMP 报文后，将组成员关系转发给因特网上的其他多播路由器。

第二阶段：因为组成员关系是动态的，因此本地多播路由器要周期性地探询本地局域网上的主机，以便知道这些主机是否还继续是组的成员。 只要对某个组有一个主机响应，那么多播路由器就认为这个组是活跃的。 但一个组在经过几次的探询后仍然没有一个主机响应，则不再将该组的成员关系转发给其他的多播路由器。

具体措施：

在主机和多播路由器之间的所有通信都是使用 IP 多播。

多播路由器在探询组成员关系时，只需要对所有的组发送一个请求信息的询问报文，而不需要对每一个组发送一个询问报文。默认的询问速率是每 125 秒发送一次。

当同一网络上连接有几个多播路由器时，能够迅速和有效地选择其中的一个来探询主机的成员关系

6.多播路由选择的基本思想：能够将组播数据包传送到组播组中的每个主机，同时在路由器转发过程中避免出现路由环路。实际上是为组播组构造一颗组播转发树，组播树连接着组播组中所有主机所在的子网，组播数据包通过组播树中的路由器复制并转发，最后一跳路由器连接组播组中的主机

第七章 传输层

1.传输层的任务：将数据从进程传递到进程。实现**进程之间的数据传递**。

2.传输层之间传输的报文叫做传输协议数据单元（TPDU）。TPDU 有效载荷是应用层的数据。

3. 单机系统中的进程通信方法：进程。从进程的观点看，操作系统的核心则是控制和协调这些进程的运行，解决进程之间的通信

4.网络环境与单机系统内部的进程通信的区别

- 网络中主机的高度自治性；
- 不是在同一个主机系统之中，没有一个统一的高层进行控制与管理；
- 网络中一台主机对其他主机的活动状态、位于其他主机系统中的各个进程状态、这些进程什么时间参与网络活动、希望与网络中哪一台主机的什么进程通信等一概无从知道。

5. 网络环境中完整的进程标识（三元组）应该是：主机地址、进程端口、进程使用的传输层协议（TCP/UDP）

6. 进程使用的传输层协议（多重协议的识别）：TCP/IP 协议族的传输层有 TCP 协议和 UDP 协议；

应用层进程会选择传输层 TCP,UDP 中的一个进行数据传输；

7. 一对通信的进程的标识（五元组）：双方使用的传输层协议、A 所在的主机地址、A 进程端口、B 所在的主机地址、B 进程端口

8. 进程间相互作用模式：Client/Server 模型。每一次通信由客户进程随机启动；服务器进程处于等待状态，及时响应客户服务请求。

采用原因：

- 网络资源分布的不均匀性
- 网络资源分布的不均匀性表现在硬件、软件和数据等三个方面;
- 网络资源分布的不均匀性是客观存在的，同时也是网络应用系统设计者的设计思想的体现;
- “资源共享”就是因为网络不同结点之间在硬件配置、计算能力、存储能力，以及数据分布等方面存在着差距与不均匀性；
- 能力强、资源丰富的充当服务器，能力弱或需要某种资源的成为客户。

9.服务器处理并发请求的基本方案：**并发服务器、重复服务器**。

并发服务器：核心是一个守护程序（daemon），守护程序在系统启动时启动，在没有客户服务请求到达时，

并发服务器处于等待状态。并发服务器拥有一个全网唯一的进程地址，网络中的客户进程可以根据该地址，向服务器提出服务请求。

重复服务器：通过设置一个请求队列来存储客户机的服务请求；服务器采用先来先服务的原则来顺序处理客户机的服务请求

★传输控制协议 TCP

1. TCP 是一种面向连接的、可靠的传输层协议，建立在不可靠的网络层 IP 协议之上，IP 不能提供任何可靠性机制，TCP 的可靠性完全由自己实现。

2. TCP 采用的最基本的可靠性技术是：**确认与超时重传、滑动窗口机制进行流量控制**

3. TCP 报文可靠传输包含 3 个步骤

（1）建立连接（三次握手）

（2）报文传输

差错控制：校验，错误重传机制

流量控制：滑动窗口机制

（3）传输闭连接（TCP 连接的拆除通过“四次握手”完成）

4. 差错控制：TCP 采用校验、确认以及超时重传，进行差错控制。发送方会对发送数据进行处理生成校验码，并设置在校验码字段中，随数据一起发送；接收方对数据进行校验，判断数据传输是否出现错误；接收方对正确接收到的数据进行确认；发送方发送数据时，启动定时器，超时未接收到确认，则重传数据

5. 流量控制：TCP 采用滑动窗口进行流量控制，通过窗口大小来告诉对方，在没有收到确认前，最多可以发送的数据量

6. TCP 的超时重传机制：采用单一定时器。发送 TCP 分段时，如果没有重传定时器开启，那么开启；如果已有重传定时器开启，不再开启。收到一个非重复 ACK 时，如果有数据在传输中，重新开启重传定时器；如果没有数据在传输中，则关闭重传定时器。收到重复 ACK 时，超过 3 个，则立即重传重复确认的数据；未收到确认造成定时器超时，重传所有发出未确认的分段。

7. TCP 采取了延迟确认的机制

8. TCP 的拥塞控制：网络拥塞的根本原因在于端系统向网络提供的负载大于网络资源容量和处理能力，主要体现在网络转发设备的存储空间有限，网络链路带宽有限以及网络转发设备的处理能力有限等。

9. TCP 拥塞控制的基本策略：发送端通过跟踪传输数据的丢失现象和往返时延的变化确定网络的传输能力，并以此来调整发送数据率。慢启动算法和拥塞避免算法。

★用户报文协议 UDP

1.概念：

- ✓ UDP 是一种无连接的、不可靠的传输层协议；
- ✓ 在完成进程到进程的通信中提供了有限的差错检验功能；
- ✓ 设计比较简单的 UDP 协议的目的是希望以最小的开销来达到网络环境中的进程通信目的；
- ✓ 进程发送的报文较短，同时对报文的可靠性要求不高，那么可以使用 UDP 协议。

2.UDP 校验：UDP 报头中的校验是可选的。

3.UDP 检验和的检验范围：伪头部、UDP 头、应用层数据

4.UDP 端口号：TCP/IP 协议族中用端口号来标识进程；端口号是在 0 到 65535 之间的整数；客户程序随机选取的临时端口号；每一种服务器程序被分配了确定的全局一致的熟知端口号；每一个客户进程都知道相应的服务器进程的熟知端口号。

指标	TCP	UDP
是否连接	面向连接	无连接
传输可靠性	可靠	不可靠
速度	较慢	较快
传输质量	较高	较差

第八章 应用层

★WWW 服务

1. WWW (World Wide Web)又称为万维网，简称为 Web, 是 Internet 技术发展中的一个重要的里程碑;，并非某种特殊的计算机网络，是一个大规模的、联机式的信息储藏所，提供分布式服务。

2. WWW 中的信息描述 - 超媒体与超文本。万维网是分布式超媒体(hypermedia)系统，它是超文本(hypertext)系统的扩充，通过 HTML（超文本标记语言）描述超媒体和超文本。

3.工作方式：客户/服务器方式工作

4.解决的问题

统一使用 HTML 语言描述 Web 页面。

使用统一资源定位符 URL 来标志万维网上的各种文档。使每一个文档在整个因特网的范围内具有惟一的标识符 URL。

在万维网客户程序与万维网服务器程序之间进行交互所使用的协议，是超文本传送协议 HTTP

★统一资源定位符 URL

1.格式

- 是对可以从因特网上得到的资源的位置和访问方法的一种简洁的表示。
- URL 给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。
- URL 相当于一个文件名在网络范围的扩展，是与因特网相连的机器上任何可访问对象的一个指针。
- 从访问的角度来看，URL 描述了以某种方式向某个进程请求访问某个文档。

2.一般形式：<URL 的访问方式>://<主机>:<端口>/<路径>

访问方式即 FTP、HTTP

<主机> 是存放资源的主机在因特网中的域名

端口和路径有时可省略

3. HTTP 之请求消息 Request：由请求行、请求头、空行和请求数据(请求体）四个部分组成

4. HTTP 之响应消息 Response：由状态行、消息报头、空行和响应正文四部分组成

★域名系统 DNS

1 域名：用字符表示的网络主机名，是一种主机标识符，用于应用层。IP 地址与域名都应该是全网惟一的，并且它们之间具有对应关系。域名到 IP 地址转换由域名系统完成。

2 域名系统：TCP/IP 协议中规定的层次型名字管理机制。域名系统将整个 Internet 划分为多个顶级域，并为每个顶级域规定了通用的顶级域名

一般格式：主机名.三级域名.二级域名.顶级域名

3.域名解析：将域名转换为对应的 IP 地址的过程。完成该功能的软件叫域名解析器;每个本地域名服务器配置一个域名解析器软件;域名解析由分布式环境中众多域名服务器共同完成的；这些服务器形成层次分布。

4.根域名服务器：根域名服务器是最重要的域名服务器。所有的根域名服务器都知道所有的顶级域名服务器的域名和 IP 地址。不管是哪一个本地域名服务器，若要对因特网上任何一个域名进行解析，只要自己无法解析，就首先求助于根域名服务器。在因特网上共有 13 个不同 IP 地址的根域名服务器，它们的名字是用一个英文字母命名，从 a 一直到 m（前 13 个字母）。这样做的目的是为了方便用户，使世界上大部分 DNS 域名服务器都能就近找到一个根域名服务器

5.域名的解析过程

主机向本地域名服务器的查询一般都是采用递归查询。如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。

本地域名服务器向根域名服务器的查询通常是采用迭代查询。当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。

6.名字的高速缓冲：每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少

第九章 网络管理

1.网络管理：包括对硬件、软件和人力的使用、综合与协调，以便对网络资源进行监视、测试、配置、分析、评价和控制，这样就能以合理的价格满足网络的一些需求，如实时运行性能，服务质量等。常简称为网管。

2.网络管理的功能

故障管理　当网络中某个组成失效时，网络管理器必须迅速查找到故障并及时排除

配置管理　配置管理负责初始化网络、并配置网络，以使其提供网络服务

计费管理　计费管理记录网络资源的使用，目的是控制和监测网络操作的费用和代价

性能管理　性能管理用于估价系统资源的运行状况及通信效率等系统性能。其能力包括监视和分析被管网络及其所提供服务的性能机制。

安全管理　包括对授权机制、访问控制、加密和加密关键字的管理，另外还要维护和检查安全日志。

3.管理站：常称为网络运行中心 NOC (Network Operations Center)，是网络管理系统的核心。管理程序在运行时就成为管理进程。

4. 管理站（硬件）或管理程序（软件）都可称为管理者，不是指人而是指机器或软件。

5.网络管理员指的是人。大型网络往往实行多级管理，因而有多个管理者，而一个管理者一般只管理本地网络的设备。

6.代理：在每一个被管设备中都要运行一个程序以便和管理站中的管理程序进行通信。这个程序就是代理。代理程序在管理程序的命令和控制下在被管设备上采取本地的行动。

7.网络管理协议（网管协议）：管理程序和代理程序之间进行通信的规则。网络管理员利用网管协议通过管理站对网络中的被管设备进行管理

8.网络管理的基本原则：若要管理某个对象，就必然会给该对象添加一些软件或硬件，但这种“添加”必须对原有对象的影响尽量小些

9. SNMP 的指导思想

- SNMP 最重要的指导思想就是要尽可能简单。
- SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。
- 在网络正常工作时，SNMP 可实现统计、配置、和测试等功能。当网络出故障时，可实现各种差错检测和恢复功能。
- 虽然 SNMP 是在 TCP/IP 基础上的网络管理协议，但也可扩展到其他类型的网络设备上。

10. SNMP 的网络管理由三个部分组成：SNMP 本身、管理信息结构 SMI、管理信息库 MIB

11.管理信息结构 SMI 的功能

(1) 被管对象应怎样命名；

(2) 用来存储被管对象的数据类型有哪些；

(3) 在网络上传送的管理数据应如何编码。

12.管理信息库 MIB：被管对象必须维持可供管理程序读写的若干控制和状态信息。这些信息总称为管理信息库 MIB 。管理程序使用 MIB 中这些信息的值对网络进行管理（如读取或重新设置这些值）。

13.SNMP：SNMP 定义了管理站和代理之间所交换的分组格式、交换的规程等。所交换的分组包含各代理中的对象（变量）名及其状态（值）。SNMP 负责读取和改变这些数值

SNMP 的操作只有两种基本的管理功能，即：

“读”操作，用 get 报文来检测各被管对象的状况；

“写”操作，用 set 报文来改变各被管对象的状况。

SNMP 是有效的网络管理协议

SNMP 使用无连接的 UDP，因此在网络上传送 SNMP 报文的开销较小。但 UDP 不保证可靠交付。

14.SNMP 的探询操作

- 探询操作——SNMP 管理进程定时向被管理设备周期性地发送探询信息。
- 探询的好处是：

  可使系统相对简单。

  能限制通过网络所产生的管理信息的通信量。
- 但探询管理协议不够灵活，而且所能管理的设备数目不能太多。探询系统的开销也较大。如探询频繁而并未得到有用的报告，则通信线路和计算机的 CPU 周期就被浪费了。

15.陷阱：SNMP 不是完全的探询协议，它允许不经过询问就能发送某些信息。这种信息称为陷阱。

16.过滤：当被管对象的代理检测到有事件发生时，就检查其门限值。代理只向管理进程报告达到某些门限值的事件（即过滤）。过滤的好处是：仅在严重事件发生时才发送陷阱；陷阱信息很简单且所需字节数很少。