

第一章. 概 述

1-02 简述分组交换的要点。

答：(1) 报文分组，加首部
(2) 经路由器储存转发
(3) 在目的地合并
(4) 无需建立连接
(5) 线路利用率高

1-03 试从多个方面比较电路交换、报文交换和分组交换的主要优缺点。

答：(1) **电路交换**：端对端通信质量因约定了通信资源获得可靠保障，对连续传送大量数据效率高。
(2) 报文交换：无须预约传输带宽，动态逐段利用传输带宽对突发式数据通信效率高，通信迅速。
(3) **分组交换**：具有报文交换之高效、迅速的要点，且各分组小，路由灵活，网络生存性能好。

1-12 因特网的两大组成部分（边缘部分与核心部分）的特点是什么？它们的工作方式各有什么特点？路由器 通讯子网 主机 资源子网

答：边缘部分：由各主机构成，用户直接进行信息处理和信息共享；低速连入核心网。
核心部分：由各路由器连网，负责为边缘部分提供高速远程分组交换。

1-13 客户服务器方式与对等通信方式的主要区别是什么？有没有相同的地方？资源子网

答：前者严格区分服务和被服务者，后者无此区别。后者实际上是前者的双向应用。

1-14 计算机网络有哪些常用的性能指标？

答：速率，**带宽**，吞吐量，**时延**，**时延带宽积**，往返时间 RTT，利用率

1-17 收发两端之间的传输距离为 1000km，信号在媒体上的传播速率为 $2 \times 10^8 \text{m/s}$ 。试计算以下两种情况的发送时延和传播时延：

- (1) 数据长度为 107bit, 数据发送速率为 100kb/s。
- (2) 数据长度为 103bit, 数据发送速率为 1Gb/s。

从上面的计算中可以得到什么样的结论？

解：(1) 发送时延： $t_s = 107/105 = 100\text{s}$
传播时延 $t_p = 106/(2 \times 10^8) = 0.005\text{s}$
(2) 发送时延 $t_s = 103/109 = 1\mu\text{s}$
传播时延： $t_p = 106/(2 \times 10^8) = 0.005\text{s}$

结论：若数据长度大而发送速率低，则在总的时延中，发送时延往往大于传播时延。但若数据长度短而发送速率高，则传播时延就可能是总时延中的主要成分。

1-18 假设信号在媒体上的传播速度为 $2 \times 10^8 \text{m/s}$ 。媒体长度 L 分别为：

- (1) 10cm（网络接口卡）
- (2) 100m（局域网）
- (3) 100km（城域网）
- (4) 5000km（广域网）

试计算出当数据率为 1Mb/s 和 10Gb/s 时在以上媒体中正在传播的比特数。

解：(1) 1Mb/s: 传播时延 $=0.1/(2 \times 10^8)=5 \times 10^{-10}$
比特数 $=5 \times 10^{-10} \times 1 \times 10^6=5 \times 10^{-4}$
1Gb/s: 比特数 $=5 \times 10^{-10} \times 1 \times 10^9=5 \times 10^{-1}$
(2) 1Mb/s: 传播时延 $=100/(2 \times 10^8)=5 \times 10^{-7}$
比特数 $=5 \times 10^{-7} \times 1 \times 10^6=5 \times 10^{-1}$
1Gb/s: 比特数 $=5 \times 10^{-7} \times 1 \times 10^9=5 \times 10^2$
(3) 1Mb/s: 传播时延 $=100000/(2 \times 10^8)=5 \times 10^{-4}$
比特数 $=5 \times 10^{-4} \times 1 \times 10^6=5 \times 10^2$
1Gb/s: 比特数 $=5 \times 10^{-4} \times 1 \times 10^9=5 \times 10^5$
(4) 1Mb/s: 传播时延 $=5000000/(2 \times 10^8)=2.5 \times 10^{-2}$
比特数 $=2.5 \times 10^{-2} \times 1 \times 10^6=5 \times 10^4$
1Gb/s: 比特数 $=2.5 \times 10^{-2} \times 1 \times 10^9=5 \times 10^7$

1-19 长度为 100 字节的应用层数据交给传输层传送，需加上 20 字节的 TCP 首部。再交给网络层传送，需加上 20 字节的 IP 首部。最后交给数据链路层的以太网传送，加上首部和尾部共 18 字节。试求数据的传输效率。数据的传输效率是指发送的应用层数据除以所发送的总数据（即应用数据加上各种首部和尾部的额外开销）。

若应用层数据长度为 1000 字节，数据的传输效率是多少？

解：(1) $100/(100+20+20+18)=63.3\%$
(2) $1000/(1000+20+20+18)=94.5\%$

1-20 网络体系结构为什么要采用分层次的结构？试举出一些与分层体系结构的思想相似的日常生活。

答：分层的好处：

①各层之间是独立的。某一层可以使用其下一层提供的服务而不需要知道服务是如何实现的。

②灵活性好。当某一层发生变化时，只要其接口关系不变，则这层以上或以下的各层均不受影响。

③结构上可分割开。各层可以采用最合适的技术来实现

④易于实现和维护。

⑤能促进标准化工作。

与分层体系结构的思想相似的日常生活有邮政系统，物流系统。

1-24 论述具有五层协议的网络体系结构的要点，包括各层的主要功能。P27

物理层：为数据通讯提供可能

逻辑链路层：建立逻辑链路

网络层：在通讯子网中为数据找到最佳路线

运输层：提供端对端的可靠服务

应用层：以各种协议提供给终端用户

第二章 物理层

2-10 常用的传输媒体有哪几种？各有何特点？

答：双绞线

屏蔽双绞线 STP (Shielded Twisted Pair)

无屏蔽双绞线 UTP (Unshielded Twisted Pair)

同轴电缆

50 Ω 同轴电缆

75 Ω 同轴电缆

光缆

无线传输：短波通信/微波/卫星通信

2-13 为什么要使用信道复用技术？常用的信道复用技术有哪些？

答：为了通过共享信道、最大限度提高信道利用率。

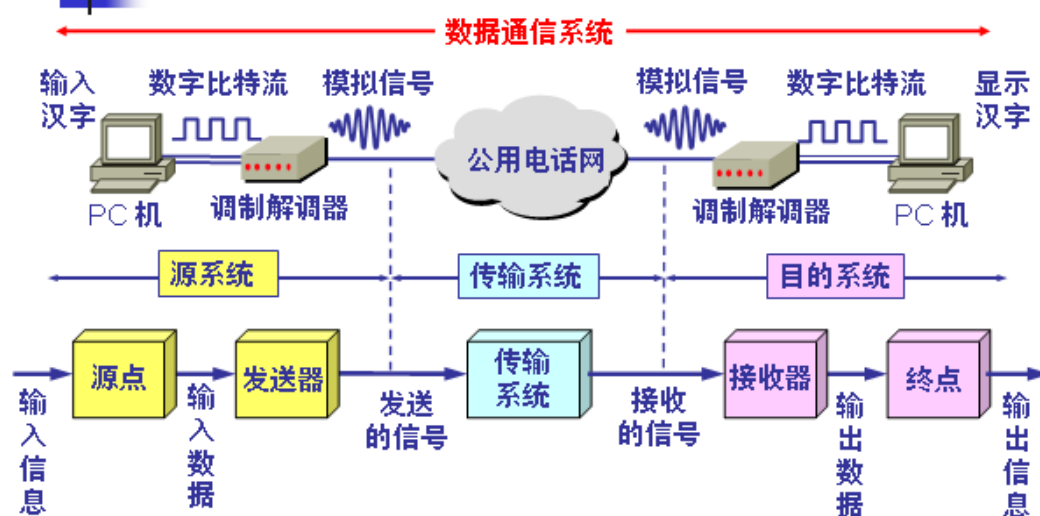
频分、波分带宽比较大；时分快速信道；码分。

关于调制、解调的概念

理解 MODEM 的使用。把数字数据转换为模拟信号成为调制，反之将模拟信号变成数字数据的过程称为解调。模拟信号和数字信号可以相互转化。使用不同的调制技术（按振幅、按频率、按相位）可以将数字信号调制为模拟信号，而采用 PCM(脉码调制)可以将模拟信号转换成数字信号。

2.2 数据通信的基础知识

2.2.1 数据通信系统的模型



第三章 数据链路层

3-01 数据链路层中的链路控制包括哪些

功能?试讨论数据链路层做成可靠的链路层有哪些优点和缺点。

答：链路管理，注意不是电路管理。

帧定界、透明传输

流量控制

差错控制

将数据和控制信息区分开、寻址

可靠的链路层的优点和缺点取决于所应用的环境：对于干扰严重的信道，可靠的链路层可以将重传范围约束在局部链路，防止全网络的传输效率受损；对于优质信道，采用可靠的链路层会增大资源开销，影响传输效率。

3-02 网络适配器的作用是什么？网络适配器工作在哪一层？

答：适配器（即网卡）来实现数据链路层和物理层这两层的协议的硬件和软件
网络适配器工作在 TCP/IP 协议中的网络接口层（OSI 中的数据链路层和物理层）

3-03 数据链路层的三个基本问题(帧定界、透明传输和差错检测)为什么都必须加以解决？

答：帧定界是分组交换的必然要求
透明传输避免消息符号与帧定界符号相混淆
差错检测防止含差错的无效数据帧浪费后续路由上的传输和处理资源

3-04 PPP 协议的主要特点是什么？PPP 适用于什么情况？为什么 PPP 协议不能使数据链路层实现可靠传输？

答：简单，提供不可靠的数据报服务，检错，无纠错，不使用序号和确认机制
PPP 适用于线路质量不太差的情况下、PPP 没有编码和确认机制

3-05 要发送的数据为 1101011011。采用 CRC 的生成多项式是 $P(X) = X^4 + X + 1$ 。试求应添加在数据后面的余数。数据在传输过程中最后一个 1 变成了 0，问接收端能否发现？若数据在传输过程中最后两个 1 都变成了 0，问接收端能否发现？采用 CRC 检验后，数据链路层的传输是否就变成了可靠的传输？

答：作二进制除法，1101011011 0000 10011 得余数 1110，添加的检验序列是 1110。
作二进制除法，两种错误均可发现
仅仅采用了 CRC 检验，缺重传机制，数据链路层的传输还不是可靠的传输。

3-06 要发送的数据为 101110。采用 CRC 生成多项式是 $P(X) = X^3 + 1$ 。试求应添加在数据后面的余数。

答：作二进制除法，101110 000 10011 添加在数据后面的余数是 011

3-07 试说明 10BASE-T 中的“10”、“BASE”和“T”所代表的意思。

答：10BASE-T 中的“10”表示信号在电缆上的传输速率为 10MB/s，“BASE”表示电缆上的信号是基带信号，“T”代表双绞线星形网，但 10BASE-T 的通信距离稍短，每个站到集线器的距离不超过 100m。

3-08 假定 1km 长的 CSMA/CD 网络的数据率为 1Gb/s。设信号在网络上的传播速率为 200000km/s。求能够使用此协议的最短帧长。

答：对于 1km 电缆，单程传播时间为 $1/200000=5$ 为微秒，来回路程传播时间为 10 微秒，为了能够按照 CSMA/CD 工作，最小帧的发射时间不能小于 10 微秒，以 Gb/s 速率工作，10 微秒可以发送的比特数等于 $10 \times 10^{-6} / 1 \times 10^{-9} = 10000$ ，因此，最短帧是 10000 位或 1250 字节长

一 CSMA/CD 载波监听多点接入/碰撞检测 1.先听后发 2 边听边发 3 遇到冲突立即停止发送 4 后退一段时间重发

二字节填充 P73

3-29 10Mb/s 以太网升级到 100Mb/s、1Gb/s 和 10Gb/s 时，都需要解决哪些技术问题？为什么以太网能够在发展的过程中淘汰掉自己的竞争对手，并使自己的应用范围从局域网一直扩展到城域网和广域网？

答：

技术问题：使参数 a 保持为较小的数值，可通过减小最大电缆长度或增大帧的最小长度。

在 100mb/s 的以太网中采用的方法是保持最短帧长不变，但将一个网段的最大电缆的长度减小到 100m，帧间时间间隔从原来 9.6 微秒改为现在的 0.96 微秒

吉比特以太网仍保持一个网段的最大长度为 100m，但采用了“载波延伸”的方法，使最短帧长仍为 64 字节（这样可以保持兼容性）、同时将争用时间增大为 512 字节。并使用“分组突发”减小开销；10 吉比特以太网的帧格式与 10mb/s，100mb/s 和 1Gb/s 以太网的帧格式完全相同。

吉比特以太网还保留标准规定的以太网最小和最大帧长，这就使用户在将其已有的以太网进行升级时，仍能 and 较低速率的以太网很方便地通信。由于数据率很高，吉比特以太网不再使用铜线而只使用光纤作为传输媒体，它使用长距离（超过 km）的光收发器与单模光纤接口，以便能够工作在广域网。

3-30 以太网交换机有何特点？用它怎样组成虚拟局域网？

答：

以太网交换机则为链路层设备，可实现透明交换虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。这些网段具有某些共同的需求。

虚拟局域网协议允许在以太网的帧格式中插入一个 4 字节的标识符，称为 VLAN 标记(tag)，用来指明发送该帧的工作站属于哪一个虚拟局域网。


3-31 网桥的工作原理和特点是什么？网桥与转发器以及以太网交换机有何异同？

答：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。

网桥具有过滤帧的功能。当网桥收到一个帧时，并不是向所有的接口转发此帧，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接口


转发器工作在物理层，它仅简单地转发信号，没有过滤能力

以太网交换机则为链路层设备，可视为多端口网桥



4. 多接口网桥——以太网交换机

- 1990 年问世的**交换式集线器**(switching hub)，可明显地提高局域网的性能。
- 交换式集线器常称为**以太网交换机**(switch)或第二层交换机（表明此交换机工作在数据链路层）。
- 以太网交换机通常都有十几个接口。因此，以太网交换机实质上就是一个**多接口的网桥**，可见交换机工作在数据链路层。



以太网交换机的特点

- 以太网交换机的每个接口都直接与主机相连，并且一般都工作在**全双工方式**。
- 交换机能同时连通许多对的接口，使每一对相互通信的主机都能像独占通信媒体那样，进行无碰撞地传输数据。
- 以太网交换机由于使用了专用的交换结构芯片，其交换速率就较高。



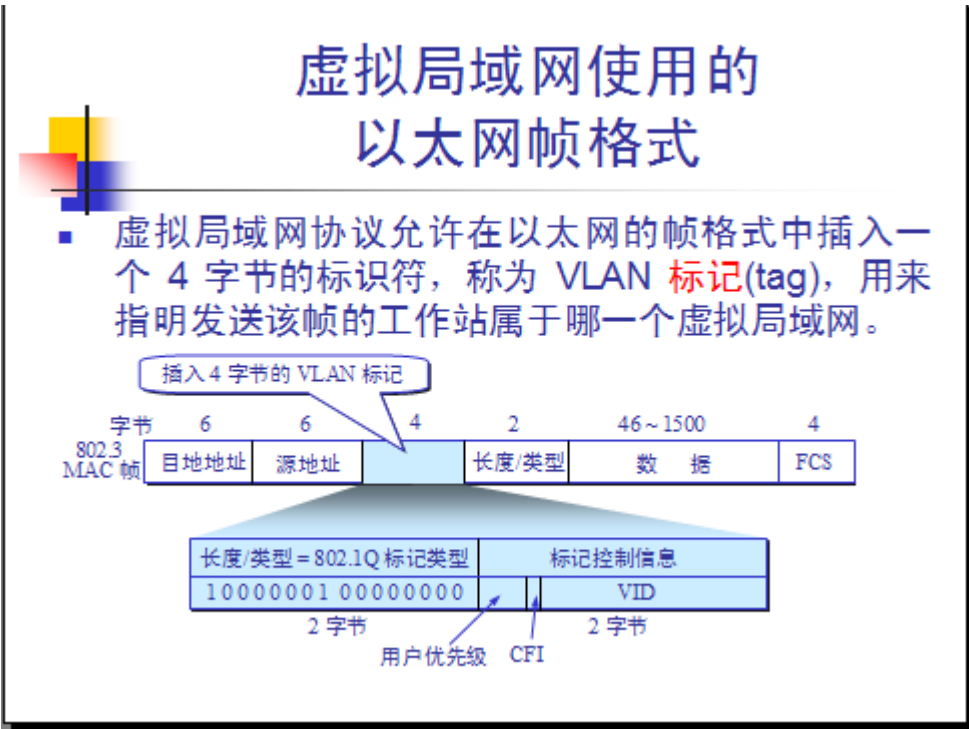
独占传输媒体的带宽

- 对于普通 10 Mb/s 的共享式以太网，若共有 N 个用户，则每个用户占有的平均带宽只有总带宽(10 Mb/s)的 N 分之一。
- 使用以太网交换机时，虽然在每个接口到主机的带宽还是 10 Mb/s，但由于一个用户在通信时是独占而不是和其他网络用户共享传输媒体的带宽，因此对于拥有 N 对接口的交换机的总容量为 $N \times 10$ Mb/s。这正是交换机的最大优点。



利用以太网交换机可以很方便地实现虚拟局域网

- **虚拟局域网** VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。
 - 这些网段具有某些共同的需求。
 - 每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN。
- 虚拟局域网其实只是局域网给用户提供服务的一种服务，而并不是一种新型局域网。



3-32 图 3-35 表示有五个站点分别连接在三个局域网上，并且用网桥 B1 和 B2 连接起来。每一个网桥都有两个接口（1 和 2）。在一开始，两个网桥中的转发表都是空的。以后有以下各站向其他的站发送了数据帧：A 发送给 E，C 发送给 B，D 发送给 C，B 发送给 A。试把有关数据填写在表 3-2 中。

发送的帧	B1 的转发表		B2 的转发表		B1 的处理 (转发？丢弃？登记？)	B2 的处理 (转发？丢弃？登记？)
	地址	接口	地址	接口		
A→E	A	1	A	1	转发，写入转发表	转发，写入转发表
C→B	C	2	C	1	转发，写入转发表	转发，写入转发表
D→C	D	2	D	2	写入转发表，丢弃不转发	转发，写入转发表
B→A	B	1			写入转发表，丢弃不转发	接收不到这个帧

3-33 网桥中的转发表是用自学习算法建立的。如果有的站点总是不发送数据而仅仅接受数据，那么在转发表中是否就没有与这样的站点相对应的项目？如果要向这个站点发送数据帧，那么网桥能够把数据帧正确转发到目的地址吗？

答：没有与这样的站点相对应的项目；
网桥能够利用广播把数据帧正确转发到目的地址

第四章 网络层

1.网络层向上提供的服务有哪两种？是比较其优缺点。

网络层向运输层提供“面向连接”虚电路（Virtual Circuit）服务或“无连接”数据报服务。前者预约了双方通信所需的一切网络资源。优点是能提供服务质量的承诺。即所传送的分组不出错、丢失、重复和失序（不按序列到达终点），也保证分组传送的时限，缺点是路

由器复杂，网络成本高；后者无网络资源障碍，尽力而为，优缺点与前者互易

3.作为中间设备，转发器、网桥、路由器和网关有何区别？

中间设备又称为中间系统或中继(relay)系统。

物理层中继系统：转发器(repeater)。

数据链路层中继系统：网桥或桥接器(bridge)。

网络层中继系统：路由器(router)。

网桥和路由器的混合物：桥路器(brouter)。

网络层以上的中继系统：网关(gateway)。

4.试简单说明下列协议的作用：IP、ARP、RARP 和 ICMP。

IP 协议：实现网络互连。使参与互连的性能各异的网络从用户看起来好像是一个统一的网络。网际协议 IP 是 TCP/IP 体系中两个最主要的协议之一，与 IP 协议配套使用的还有四个协议。

ARP 协议：是解决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问题。

RARP：是解决同一个局域网上的主机或路由器的硬件地址和 IP 地址的映射问题。

ICMP：提供差错报告和询问报文，以提高 IP 数据交付成功的机会

IGMP：用于探寻、转发本局域网内的组成员关系。

7.试说明 IP 地址与硬件地址的区别，为什么要使用这两种不同的地址？

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 位的标识符。从而把整个因特网看成为一个单一的、抽象的网络。

在实际网络的链路上传送数据帧时，最终还是必须使用硬件地址。

MAC 地址在一定程度上与硬件一致，基于物理、能够标识具体的链路通信对象、IP 地址给予逻辑域的划分、不受硬件限制。

9.（1）子网掩码为 255.255.255.0 代表什么意思？

有三种含义

其一是一个 A 类网的子网掩码，对于 A 类网络的 IP 地址，前 8 位表示网络号，后 24 位表示主机号，使用子网掩码 255.255.255.0 表示前 8 位为网络号，中间 16 位用于子网段的划分，最后 8 位为主机号。

第二种情况为一个 B 类网，对于 B 类网络的 IP 地址，前 16 位表示网络号，后 16 位表示主机号，使用子网掩码 255.255.255.0 表示前 16 位为网络号，中间 8 位用于子网段的划分，最后 8 位为主机号。

第三种情况为一个 C 类网，这个子网掩码为 C 类网的默认子网掩码。

（2）一网络的现在掩码为 255.255.255.248，问该网络能够连接多少个主机？

255.255.255.248 即 11111111.11111111.11111111.11111000.

每一个子网上的主机为 $(2^3)=6$ 台

掩码位数 29，该网络能够连接 8 个主机，扣除全 1 和全 0 后为 6 台。

（3）一 A 类网络和一 B 网络的子网号 subnet-id 分别为 16 个 1 和 8 个 1，问这两个子网掩码有何不同？

A 类网络：11111111 11111111 11111111 00000000

给定子网号（16 位“1”）则子网掩码为 255.255.255.0

B 类网络 11111111 11111111 11111111 00000000

给定子网号（8 位“1”）则子网掩码为 255.255.255.0 但子网数目不同

(4) 一个 B 类地址的子网掩码是 255.255.240.0。试问在其中每一个子网上的主机数最多是多少？

$$(240)_{10} = (128+64+32+16)_{10} = (11110000)_2$$

Host-id 的位数为 $4+8=12$ ，因此，最大主机数为：

$$2^{12}-2=4096-2=4094$$

$$11111111.11111111.11110000.00000000 \quad \text{主机数 } 2^{12}-2$$

(5) 一 A 类网络的子网掩码为 255.255.0.255；它是否为一个有效的子网掩码？

$$\text{是 } 10111111 \quad 11111111 \quad 00000000 \quad 11111111$$

(6) 某个 IP 地址的十六进制表示 C2.2F.14.81，试将其转化为点分十进制的形式。这个地址是哪一类 IP 地址？

$$C2 \quad 2F \quad 14 \quad 81 \rightarrow (12*16+2).(2*16+15).(16+4).(8*16+1) \rightarrow 194.47.20.129$$

$$C2 \quad 2F \quad 14 \quad 81 \rightarrow 11000010.00101111.00010100.10000001$$

C 类地址

(7) C 类网络使用子网掩码有无实际意义？为什么？

有实际意义。C 类子网 IP 地址的 32 位中，前 24 位用于确定网络号，后 8 位用于确定主机号。如果划分子网，可以选择后 8 位中的高位，这样做可以进一步划分网络，并且不增加路由表的内容，但是代价是主机数相信减少。

10. 试辨认以下 IP 地址的网络类别。

$$(1) 128.36.199.3 \quad (2) 21.12.240.17 \quad (3) 183.194.76.253 \quad (4) 192.12.69.248$$

$$(5) 89.3.0.1 \quad (6) 200.3.6.2$$

(2) 和 (5) 是 A 类，(1) 和 (3) 是 B 类，(4) 和 (6) 是 C 类。

11. IP 数据报中的首部检验和并不检验数据报中的数据。这样做的最大好处是什么？坏处是什么？

在首部中的错误比在数据中的错误更严重，例如，一个坏的地址可能导致分组被投寄到错误的主机。许多主机并不检查投递给它们的分组是否确实是要投递给它们，它们假定网络从来不会把本来是要前往另一主机的分组投递给它们。

数据不参与检验和的计算，因为这样做代价大，上层协议通常也做这种检验工作，从前，从而引起重复和多余。因此，这样做可以加快分组的转发，但是数据部分出现差错时不能及早发现。

12. 当某个路由器发现一 IP 数据报的检验和有差错时，为什么采取丢弃的办法而不是要求源站重传此数据报？计算首部检验和为什么不采用 CRC 检验码？

答：纠错控制由上层（传输层）执行

IP 首部中的源站地址也可能出错请错误的源地址重传数据报是没有意义的

不采用 CRC 简化解码计算量，提高路由器的吞吐量

15. 什么是最大传送单元 MTU？它和 IP 数据报的首部中的哪个字段有关系？

答：IP 层下面数据链里层所限定的帧格式中数据字段的最大长度，与 IP 数据报首部中的总长度字段有关系

16. 在因特网中将 IP 数据报分片传送的数据报在最后的目的地主机进行组装。还可以有另一种

做法，即数据报片通过一个网络就进行一次组装。是比较这两种方法的优劣。

在目的站而不是在中间的路由器进行组装是由于：

(1) 路由器处理数据报更简单些；效率高，延迟小。

(2) 数据报的各分片可能经过各自的路径。因此在每一个中间的路由器进行组装可能总会缺少几个数据报片；

(3) 也许分组后面还要经过一个网络，它还要给这些数据报片划分成更小的片。如果在中间的路由器进行组装就可能会组装多次。

(为适应路径上不同链路段所能许可的不同分片规模，可能要重新分片或组装)

17. 一个 3200 位长的 TCP 报文传到 IP 层，加上 160 位的首部后成为数据报。下面的互联网由两个局域网通过路由器连接起来。但第二个局域网所能传送的最长数据帧中的数据部分只有 1200 位。因此数据报在路由器必须进行分片。试问第二个局域网向其上层要传送多少比特的数据（这里的“数据”当然指的是局域网看见的数据）？

答：第二个局域网所能传送的最长数据帧中的数据部分只有 1200bit，即每个 IP 数据片的数据部分 $<1200-160(\text{bit})$ ，由于片偏移是以 8 字节即 64bit 为单位的，所以 IP 数据片的数据部分最大不超过 1024bit，这样 3200bit 的报文要分 4 个数据片，所以第二个局域网向上传送的比特数等于 $(3200+4\times 160)$ ，共 3840bit。

18. (1) 有人认为：“ARP 协议向网络层提供了转换地址的服务，因此 ARP 应当属于数据链路层。”这种说法为什么是错误的？

因为 ARP 本身是网络层的一部分，ARP 协议为 IP 协议提供了转换地址的服务，数据链路层使用硬件地址而不使用 IP 地址，无需 ARP 协议数据链路层本身即可正常运行。因此 ARP 不再数据链路层。

(2) 试解释为什么 ARP 高速缓存每存入一个项目就要设置 10~20 分钟的超时计时器。这个时间设置的太大或太小会出现什么问题？

答：考虑到 IP 地址和 Mac 地址均有可能是变化的（更换网卡，或动态主机配置）

10—20 分钟更换一块网卡是合理的。超时时间太短会使 ARP 请求和响应分组的通信量太频繁，而超时时间太长会使更换网卡后的主机迟迟无法和网络上的其他主机通信。

(3) 至少举出两种不需要发送 ARP 请求分组的情况（即不需要请求将某个目的 IP 地址解析为相应的硬件地址）。

在源主机的 ARP 高速缓存中已经有了该目的 IP 地址的项目；源主机发送的是广播分组；源主机和目的主机使用点对点链路。

19. 主机 A 发送 IP 数据报给主机 B，途中经过了 5 个路由器。试问在 IP 数据报的发送过程中总共使用了几次 ARP？

6 次，主机用一次，每个路由器各使用一次。

20. 设某路由器建立了如下路由表：

目的网络	子网掩码	下一跳
128.96.0.0	255.255.0.0	R3
128.96.39.0	255.255.255.128	接口 m0
128.96.39.128	255.255.255.128	接口 m1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3

* (默认) ——— R4

现共收到 5 个分组，其目的地址分别为：

- (1) 128.96.39.10 最长网络前缀
- (2) 128.96.40.12 特定主机路由 128.96.40.12 255.255.255.128 R2
- (3) 128.96.40.151
- (4) 192.153.17
- (5) 192.4.153.90

(1) 分组的目的站 IP 地址为：128.96.39.10。先与子网掩码 255.255.255.128 相与，得 128.96.39.0，可见该分组经接口 0 转发。

(2) 分组的目的 IP 地址为：128.96.40.12。

① 与子网掩码 255.255.255.128 相与得 128.96.40.0，不等于 128.96.39.0。

② 与子网掩码 255.255.255.128 相与得 128.96.40.0，经查路由表可知，该项分组经 R2 转发。

(3) 分组的目的 IP 地址为：128.96.40.151，与子网掩码 255.255.255.128 相与后得 128.96.40.128，与子网掩码 255.255.255.192 相与后得 128.96.40.128，经查路由表知，该分组转发选择默认路由，经 R4 转发。

(4) 分组的目的 IP 地址为：192.4.153.17。与子网掩码 255.255.255.128 相与后得 192.4.153.0。与子网掩码 255.255.255.192 相与后得 192.4.153.0，经查路由表知，该分组经 R3 转发。

(5) 分组的目的 IP 地址为：192.4.153.90，与子网掩码 255.255.255.128 相与后得 192.4.153.0。与子网掩码 255.255.255.192 相与后得 192.4.153.64，经查路由表知，该分组转发选择默认路由，经 R4 转发。

注意：特定主机路由优先、都不匹配是使用默认路由

22..一个数据报长度为 4000 字节（固定首部长度）。现在经过一个网络传送，但此网络能够传送的最大数据长度为 1500 字节。试问应当划分为几个短些的数据报片？各数据报片的数据字段长度、片偏移字段和 MF 标志应为何数值？

IP 数据报固定首部长度为 20 字节

	总长度(字节)	数据长度(字节)	MF	片偏移
原始数据报	4000	3980	0	0
数据报片 1	1500	1480	1	0
数据报片 2	1500	1480	1	185
数据报片 3	1040	1020	0	370

24.试找出可产生以下数目的 A 类子网的子网掩码（采用连续掩码）。

(1) 2, (2) 6, (3) 30, (4) 62, (5) 122, (6) 250.

(1) 255.192.0.0, (2) 255.224.0.0, (3) 255.248.0.0, (4) 255.252.0.0, (5) 255.254.0.0, (6) 255.255.0.0

26.有如下的 4 个/24 地址块，试进行最大可能性的聚会。

212.56.132.0/24

212.56.133.0/24

212.56.134.0/24

212.56.135.0/24

212= (11010100)₂, 56= (00111000)₂

132= (10000100)₂,

133= (10000101)₂

134= (10000110)₂,

135= (10000111)₂

所以共同的前缀有 22 位, 即 11010100 00111000 100001, 聚合的 CIDR 地址块是:

212.56.132.0/22

27. 有两个 CIDR 地址块 208.128/11 和 208.130.28/22。是否有那一个地址块包含了另一个地址? 如果有, 请指出, 并说明理由。

208.128/11 的前缀为: 11010000 100

208.130.28/22 的前缀为: 11010000 10000010 000101, 它的前 11 位与 208.128/11 的前缀是一致的, 所以 208.128/11 地址块包含了 208.130.28/22 这一地址块。

28. 已知路由器 R1 的路由表如表 4—12 所示。

表 4-12 习题 4-28 中路由器 R1 的路由表

地址掩码	目的网络地址	下一跳地址	路由器接口
/26	140. 5. 12. 64	180. 15. 2. 5	m2
/24	130. 5. 8. 0	190. 16. 6. 2	m1
/16	110. 71. 0. 0	m0
/16	180. 15. 0. 0	m2
/16	196. 16. 0. 0	m1
默认	默认	110. 71. 4. 5	m0

试画出个网络和必要的路由器的连接拓扑, 标注出必要的 IP 地址和接口。对不能确定的情况应该指明。

图形见课后答案 P380

29. 一个自治系统有 5 个局域网, 其连接图如图 4-55 示。LAN2 至 LAN5 上的主机数分别为: 91, 150, 3 和 15。该自治系统分配到的 IP 地址块为 30.138.118/23。试给出每一个局域网的地址块 (包括前缀)。

30.138.118/23--→30.138.0111 011

分配网络前缀时应先分配地址数较多的前缀

题目没有说 LAN1 上有几个主机, 但至少需要 3 个地址给三个路由器用。

本题的解答有很多种, 下面给出两种不同的答案:

	第一组答案	第二组答案
LAN1	30.138.119.192/29	30.138.118.192/27
LAN2	30.138.119.0/25	30.138.118.0/25
LAN3	30.138.118.0/24	30.138.119.0/24
LAN4	30.138.119.200/29	30.138.118.224/27
LAN5	30.138.118.128/27	30.138.119.128/26

30. 一个大公司有一个总部和三个下属部门。公司分配到的网络前缀是 192.77.33/24。公司的网络布局如图 4-56 示。总部共有五个局域网, 其中的 LAN1-LAN4 都连接到路由器 R1 上, R1 再通过 LAN5 与路由器 R5 相连。R5 和远地的三个部门的局域网 LAN6~LAN8 通过广

域网相连。每一个局域网旁边标明的数字是局域网上的主机数。试给每一个局域网分配一个合适的网络的前缀。

见课后答案 P380

31. 以下地址中的哪一个和 86.32/12 匹配：请说明理由。

(1) 86.33.224. 123; (2) 86.79.65.216; (3) 86.58.119.74; (4) 86.68.206.154。

86.32/12 → 86.00100000 下划线上为 12 位前缀说明第二字节的前 4 位在前缀中。

给出的四个地址的第二字节的前 4 位分别为：0010，0100，0011 和 0100。因此只有 (1) 是匹配的。

32. 以下地址中的哪一个地址 2.52.90.140 匹配？请说明理由。

(1) 0/4; (2) 32/4; (3) 4/6 (4) 152.0/11

前缀 (1) 和地址 2.52.90.140 匹配

2.52.90.140 → 0000 0010.52.90.140

0/4 → 0000 0000

32/4 → 0010 0000

4/6 → 0000 0100

80/4 → 0101 0000

33. 下面的前缀中的哪一个和地址 152.7.77.159 及 152.31.47.252 都匹配？请说明理由。

(1) 152.40/13; (2) 153.40/9; (3) 152.64/12; (4) 152.0/11。

前缀 (4) 和这两个地址都匹配

34. 与下列掩码相对应的网络前缀各有多少位？

(1) 192.0.0.0; (2) 240.0.0.0; (3) 255.224.0.0; (4) 255.255.255.252。

(1) /2; (2) /4; (3) /11; (4) /30。

35. 已知地址块中的一个地址是 140.120.84.24/20。试求这个地址块中的最小地址和最大地址。地址掩码是什么？地址块中共有多少个地址？相当于多少个 C 类地址？

140.120.84.24 → 140.120.(0101 0100).24

最小地址是 140.120.(0101 0000).0/20 (80)

最大地址是 140.120.(0101 1111).255/20 (95)

地址数是 4096。相当于 16 个 C 类地址。

36. 已知地址块中的一个地址是 190.87.140.202/29。重新计算上题。

190.87.140.202/29 → 190.87.140.(1100 1010)/29

最小地址是 190.87.140.(1100 1000)/29 200

最大地址是 190.87.140.(1100 1111)/29 207

地址数是 8。相当于 1/32 个 C 类地址。

37. 某单位分配到一个地址块 136.23.12.64/26。现在需要进一步划分为 4 个一样大的子网。试问：

(1) 每一个子网的网络前缀有多长？

(2) 每一个子网中有多少个地址？

(3) 每一个子网的地址是什么？

(4) 每一个子网可分配给主机使用的最小地址和最大地址是什么？

(1) 每个子网前缀 28 位。

(2) 每个子网的地址中有 4 位留给主机用，因此共有 16 个地址。

(3) 四个子网的地址块是：

第一个地址块 136.23.12.64/28，可分配给主机使用的

最小地址：136.23.12.01000001=136.23.12.65/28

最大地址：136.23.12.01001110=136.23.12.78/28

第二个地址块 136.23.12.80/28，可分配给主机使用的

最小地址：136.23.12.01010001=136.23.12.81/28

最大地址：136.23.12.01011110=136.23.12.94/28

第三个地址块 136.23.12.96/28，可分配给主机使用的

最小地址：136.23.12.01100001=136.23.12.97/28

最大地址：136.23.12.01101110=136.23.12.110/28

第四个地址块 136.23.12.112/28，可分配给主机使用的

最小地址：136.23.12.01110001=136.23.12.113/28

最大地址：136.23.12.01111110=136.23.12.126/28

4-41 假定网络中的路由器 B 的路由表有如下的项目（这三列分别表示“目的网络”、“距离”和“下一跳路由器”）

N1	7	A
N2	2	C
N6	8	F
N8	4	E
N9	4	F

现在 B 收到从 C 发来的路由信息（这两列分别表示“目的网络”“距离”）：

N2	4
N3	8
N6	4
N8	3
N9	5

试求出路由器 B 更新后的路由表（详细说明每一个步骤）。

路由器 B 更新后的路由表如下：

N1	7	A	无新信息，不改变
N2	5	C	相同的下一跳，更新
N3	9	C	新的项目，添加进来
N6	5	C	不同的下一跳，距离更短，更新
N8	4	E	不同的下一跳，距离一样，不改变
N9	4	F	不同的下一跳，距离更大，不改变

40. 假定网络中的路由器 A 的路由表有如下的项目（格式同上题）：

N1	4	B
N2	2	C
N3	1	F

N4	5	G
到从 C 发来的路由信息 (格式)		
N1	2	
N2	1	
N3	3	
N4	7	

路由器 A 更新后的路由表如下:

注意：原路由项如有直连的，直连优先。

OSPF（链路状态）根据链路状态计算最佳路由

在开始向输出链路传输分组的第一个比特之前,必须接受到整个分组,这种机制称为存储转发机制;还有一种是只要接受了分组中的目的地址就开始转发,这种机制称为直通交换。

[illegible]

Place the mentioned types of connection devices in a table as below.

Type of equipment:	Operates on layer:
Hub	
Switch	

Router	
Bridge	
Reapter	
NIC	

使用交换机（或网桥）和使用路由器是连接两个不同网络的两种办法。交换式网络实现在数据链路层，它不需要理解网络层的协议，整个网络互联是以数据链路层的地址为基础的，而路由式网络是在网络层的互联，它需要理解网络层的协议。

关于一些常用术语的归纳和总结

①IP Datagram ②Bits ③frame ④Bridge ⑤ARP
⑥port number ⑦Routing ⑧TCP ⑨UDP ⑩Segment

Physical Layer: _____

DataLink Layer: _____

Network Layer: _____

Transport Layer: _____

第五章 传输层

5-02 试说明运输层在协议栈中的地位和作用，运输层的通信和网络层的通信有什么重要区别？为什么运输层是必不可少的？

答：

运输层处于面向通信部分的最高层，同时也是用户功能中的最低层，向它上面的应用层提供服务；

运输层为应用进程之间提供端到端的逻辑通信，但网络层是为主机之间提供逻辑通信（面向主机，承担路由功能，即主机寻址及有效的分组交换）。

各种应用进程之间通信需要“可靠或尽力而为”的两类服务质量，必须由运输层以复用和分用的形式加载到网络层。

5-03 当应用程序使用面向连接的 TCP 和无连接的 IP 时，这种传输是面向连接的还是面向无连接的？

答：都是。这要在不同层次来看，在运输层是面向连接的，在网络层则是无连接的。

5-05 试举例说明有些应用程序愿意采用不可靠的 UDP，而不用采用可靠的 TCP。

答：VOIP：由于语音信息具有一定的冗余度，人耳对 VOIP 数据报损失由一定的承受度，但对传输时延的变化较敏感。

有差错的 UDP 数据报在接收端被直接抛弃，TCP 数据报出错则会引起重传，可能带来较大的时延扰动。

因此 VOIP 宁可采用不可靠的 UDP，而不愿意采用可靠的 TCP。

5-06 接收方收到有差错的 UDP 用户数据报时应如何处理？

答：丢弃

5-07 如果应用程序愿意使用 UDP 来完成可靠的传输，这可能吗？请说明理由

答：可能，但应用程序中必须额外提供与 TCP 相同的功能。

5-08 为什么说 UDP 是面向报文的，而 TCP 是面向字节流的？

答：发送方 UDP 对应用程序交下来的报文，在添加首部后就向下交付 IP 层。UDP 对应用层交下来的报文，**既不合并，也不拆分，而是保留这些报文的边界。**

接收方 UDP 对 IP 层交上来的 UDP 用户数据报，**在去除首部后就原封不动地交付上层的应用进程**，一次交付一个完整的报文。

发送方 TCP 对应用程序交下来的报文数据块，**视为无结构的字节流（无边界约束，可拆分或进行合并）**，但维持各字节

5-09 端口的作用是什么？

答：端口的作用是对 TCP/IP 体系的**应用进程进行统一的标志**，使运行不同操作系统的计算机的**应用进程能够互相通信**。

熟知端口，数值一般为 0~1023.标记常规的服务进程；

登记端口号，数值为 1024~49151，标记没有熟知端口号的非常规的服务进程；

5-10 试说明运输层中伪首部的作用。

答：运输层用来进行数据报的校验和的计算。

5-11 某个应用进程使用运输层的用户数据报 UDP，然后继续向下交给 IP 层后，又封装成 IP 数据报。既然都是数据报，可否跳过 UDP 而直接交给 IP 层？哪些功能 UDP 提供了但 IP 没提供？通过端口

答：不可跳过 UDP 而直接交给 IP 层

IP 数据报**承担主机寻址，提供报头检错**；只能**找到目的主机而无法找到目的进程**。

UDP 提供**对应用进程的复用和分用功能**，以及提供**对数据报部分的差错检验**。

5-12 一个应用程序用 UDP，到 IP 层把数据报在划分为 4 个数据报片发送出去，结果前两个数据报片丢失，后两个到达目的站。过了一段时间应用程序重传 UDP，而 IP 层仍然划分为 4 个数据报片来传送。结果这次前两个到达目的站而后两个丢失。试问：在目的站能否将这两次传输的 4 个数据报片组装成完整的数据报？假定目的站第一次收到的后两个数据报片仍然保存在目的站的缓存中。

答：不行

重传时，IP 数据报的**标识字段会有另一个标识符**。

仅当标识符相同的 IP 数据报片才能组装成一个 IP 数据报。

前两个 IP 数据报片的标识符与后两个 IP 数据报片的标识符不同，因此不能组装成一个 IP 数据报。

5-13 一个 UDP 用户数据的数据字段为 8192 字节。在数据链路层要使用以太网来传送。试问应当划分为几个 IP 数据报片？说明每一个 IP 数据报字段长度和片偏移字段的值。

答：6 个

数据字段的长度：前 5 个是 1480 字节，最后一个是 800 字节。

片偏移字段的值分别是：0，1480，2960，4440，5920 和 7400.

5-14 一 UDP 用户数据报的首部十六进制表示是：06 32 00 45 00 1C E2 17.试求源端口、目的端口、用户数据报的总长度、数据部分长度。这个用户数据报是从客户发送给服务器还是服务器发送给客户？使用 UDP 的这个服务器程序是什么？

解：源端口 1586，目的端口 69，UDP 用户数据报总长度 28 字节，数据部分长度 20 字节。

此 UDP 用户数据报是从客户发给服务器（因为目的端口号<1023，是熟知端口）、服务器程序是 TFTP。

TCP 头部和 UDP 头部的区别

见课 P185 、 P194

5-15 使用 TCP 对实时话音数据的传输有没有什么问题？使用 UDP 在传送数据文件时会有什么问题？

答：如果语音数据不是实时播放（边接受边播放）就可以使用 TCP，因为 TCP 传输可靠。接收端用 TCP 讲话音数据接受完毕后，可以在以后的任何时间进行播放。但假定是实时传输，则必须使用 UDP。

UDP 不保证可靠交付，但 UDP 比 TCP 的开销要小很多。因此只要应用程序接受这样的服务质量就可以使用 UDP。

简述 TCP 和 UDP 协议的主要特点和应用场合。

TCP:

- 1、面向连接，提供流量控制和拥塞控制机制。
- 2、可靠交付，提供对报文段的检错、确认、重传和排序等功能。
- 3、报文头部长，传输开销大。
- 4、常用于通讯环境较差的互联网环境，或需要提供可靠的字节流服务的应用场合，如文件传输等。

UDP:

- 1、无连接，无流量控制机制，无确认。
- 2、不可靠交付，只有有限的差错控制机制。
- 3、报文头部短、简单，传输开销小。
- 4、常用于可靠性较高的网络环境中，如局域网；或不要求提供可靠传输的应用场合，如实时通讯。

协议分析举例 P122、P194

Below is an IP datagram in hexadecimal format.

46000112
13372000
17062B21
18181C20
3411B111
03A7F270
20450014
020E2704
A036401F
70102500
32E90000
44657420
65722067
49204C4F

56452053

48464321

2121...

- (1) What IP version is used in this datagram? version 4
- (2) How long is the IP header? 24 bytes
- (3) How long is the whole IP datagram? 0112(Hex) is 274 bytes
- (4) How many bytes are in the IP data area? $274 - 24 = 250$ bytes
- (5) Is the IP datagram fragmented? yes (DF=0)
- (6) If RFC1700 says that TCP has number 6 and UDP has number 17 in the transport protocol field, which transport protocol is used here? TCP
- (7) What is the sender's IP address written in dotted decimal notation?
18181C20(Hex) is 24.24.28.32
- (8) What is the receiver's IP address written in dotted decimal notation?
3411B111(Hex) is 52.17.177.17
- (9) What network classes are the above IP addresses from?
Sender is A class and receiver is A class
- (10) How many bytes is the TCP header? 7 words each 4 bytes is a total 28 bytes
- (11) How many bytes is the TCP user data? $250 - 28 = 222$ bytes
- (12) What is the sender's port number? 8261
- (13) What is the receiver's port number? 20
- (14) How big is the sender's receiving windows (buffer)? 9472 bytes
- (15) If the user data is ASCII-text, what text is sent in this segment?
I—LOVE—SHFC!!!
- (16) What network is the sender belong to? 24.0.0.0
- (17) How many addresses are possible in the sender's network?
 $16M - 2$

5-23 主机 A 向主机 B 连续发送了两个 TCP 报文段，其序号分别为 70 和 100。试问：

- (1) 第一个报文段携带了多少个字节的数据？
- (2) 主机 B 收到第一个报文段后发回的确认中的确认号应当是多少？
- (3) 如果主机 B 收到第二个报文段后发回的确认中的确认号是 180，试问 A 发送的第二个报文段中的数据有多少字节？
- (4) 如果 A 发送的第一个报文段丢失了，但第二个报文段到达了 B。B 在第二个报文段到达后向 A 发送确认。试问这个确认号应为多少？

解：(1) 第一个报文段的数据序号是 70 到 99，共 30 字节的数据。

(2) 确认号应为 100。

(3) 80 字节。

(4) 70

5-37 在 TCP 的拥塞控制中，什么是慢开始、拥塞避免、快重传和快恢复算法？这里每一种算法各起什么作用？“乘法减小”和“加法增大”各用在什么情况下？

答：慢开始：

在主机刚刚开始发送报文段时可先将拥塞窗口 cwnd 设置为一个最大报文段 MSS 的数值。在每收到一个对新的报文段的确认后，将拥塞窗口增加至多一个 MSS 的数值。用这样的方法逐步增大发送端的拥塞窗口 cwnd，可以分组注入到网络的速率更

加合理。

拥塞避免：

当拥塞窗口值大于慢开始门限时，停止使用慢开始算法而改用拥塞避免算法。拥塞避免算法使发送的拥塞窗口每经过一个往返时延 RTT 就增加一个 MSS 的大小。

快重传算法规定：

发送端只要一连收到三个重复的 ACK 即可断定有分组丢失了，就应该立即重传丢手的报文段而不必继续等待为该报文段设置的重传计时器的超时。

快恢复算法：

当发送端收到连续三个重复的 ACK 时，就重新设置慢开始门限 ssthresh 与慢开始不同之处是拥塞窗口 cwnd 不是设置为 1，而是设置为 ssthresh 若收到的重复的 ACK 为 n 个 ($n > 3$)，则将 cwnd 设置为 ssthresh 若发送窗口值还容许发送报文段，就按拥塞避免算法继续发送报文段。若收到了确认新的报文段的 ACK，就将 cwnd 缩小到 ssthresh

乘法减小：

是指不论在慢开始阶段还是拥塞避免阶段，只要出现一次超时（即出现一次网络拥塞），就把慢开始门限值 ssthresh 设置为当前的拥塞窗口值乘以 0.5。当网络频繁出现拥塞时，ssthresh 值就下降得很快，以大大减少注入到网络中的分组数。

加法增大：

是指执行拥塞避免算法后，在收到对所有报文段的确认后（即经过一个往返时间），就把拥塞窗口 cwnd 增加一个 MSS 大小，使拥塞窗口缓慢增大，以防止网络过早出现拥塞。

5-38 设 TCP 的 ssthresh 的初始值为 8(单位为报文段)。当拥塞窗口上升到 12 时网络发生了超时，TCP 使用慢开始和拥塞避免。试分别求出第 1 次到第 15 轮次传输的各拥塞窗口大小。你能说明拥塞控制窗口每一次变化的原因吗？

答：拥塞窗口大小分别为：1, 2, 4, 8, 9, 10, 11, 12, 1, 2, 4, 6, 7, 8, 9.

5-39 TCP 的拥塞窗口 cwnd 大小与传输轮次 n 的关系如下所示：

cwnd	1	2	4	8	16	32	33	34	35	36	37	38	39
n	1	2	3	4	5	6	7	8	9	10	11	12	13
cwnd	40	41	42	21	22	23	24	25	26	1	2	4	8
n	14	15	16	17	18	19	20	21	22	23	24	25	26

- (1) 试画出如图 5-25 所示的拥塞窗口与传输轮次的关系曲线。
- (2) 指明 TCP 工作在慢开始阶段的时间间隔。
- (3) 指明 TCP 工作在拥塞避免阶段的时间间隔。
- (4) 在第 16 轮次和第 22 轮次之后发送方是通过收到三个重复的确认还是通过超时检测到丢失了报文段？
- (5) 在第 1 轮次，第 18 轮次和第 24 轮次发送时，门限 ssthresh 分别被设置为多大？
- (6) 在第几轮次发送出第 70 个报文段？
- (7) 假定在第 26 轮次之后收到了三个重复的确认，因而检测出了报文段的丢失，那么拥塞窗口 cwnd 和门限 ssthresh 应设置为多大？

答：(1) 拥塞窗口与传输轮次的关系曲线如图所示（课本后答案）：

- (2) 慢开始时间间隔：【1, 6】和【23, 26】
- (3) 拥塞避免时间间隔：【6, 16】和【17, 22】

- (4) 在第 16 轮次之后发送方通过收到三个重复的确认检测到丢失的报文段。在第 22 轮次之后发送方是通过超时检测到丢失的报文段。
- (5) 在第 1 轮次发送时，门限 `ssthresh` 被设置为 32
在第 18 轮次发送时，门限 `ssthresh` 被设置为发生拥塞时的一半，即 21。
在第 24 轮次发送时，门限 `ssthresh` 是第 18 轮次发送时设置的 21
- (6) 第 70 报文段在第 7 轮次发送出。
- (7) 拥塞窗口 `cwnd` 和门限 `ssthresh` 应设置为 8 的一半，即 4。

在 TCP 协议中发送方的窗口大小是由什么决定的。RTT 的概念是什么？

答：接受方允许的窗口 `rwnd` 和拥塞窗口 `cwnd`。例如：假定在没有发生拥塞的情况下，在一条往返时间 RTT 为 10ms 的线路上采用 SLOW START 控制策略。如果接受窗口的大小为 30KB，最大报文段 MSS 为 2KB。那么需要 40ms 发送方才能发送出一个完全窗口。

关于 TCP 协议采用的滑动窗口机制的理解

答：TCP 协议采用可变发送窗口的方式进行流量控制。滑动窗口协议规定，只要发送窗口未滿，发送方就可以继续发送报文段；每发送一个报文段，就创建该报文段的重传计时器，当计时器超时还未收到确认，发送方就重传该报文段。由于发送窗口的限制，发送方在未经确认之前，最多能发送的报文段的数量等于发送窗口的大小。比如：如果发送端的发送窗口值为 1024，意味着发送端可以在收到一个确认之前可以发送 1024 个字节。

实际上，滑动窗口的作用不仅仅在于流量控制，还提供了一这定程度上的拥塞控制。因为拥塞通常发生在通过网络传输的分组数量开始接近网络对分组的处理能力时。TCP 协议通过调节发送窗口的大小可调节分组的发送量。TCP 协议规定，发送窗口大小 = $\text{Min}[\text{接收端窗口}, \text{拥塞窗口}]$ ，其中拥塞窗口正是对网络拥塞状况的反映。

5-46 试用具体例子说明为什么在运输连接建立时要使用三次握手。说明如不这样做可能会出现什么情况。

答：

3 次握手完成两个重要的功能，既要双方做好发送数据的准备工作（双方都知道彼此已准备好），也要允许双方就初始序列号进行协商，这个序列号在握手过程中被发送和确认。

假定 B 给 A 发送一个连接请求分组，A 收到了这个分组，并发送了确认应答分组。按照两次握手的协定，A 认为连接已经成功地建立了，可以开始发送数据分组。可是，B 在 A 的应答分组在传输中被丢失的情况下，将不知道 A 是否已准备好，不知道 A 建议什么样的序列号，B 甚至怀疑 A 是否收到自己的连接请求分组，在这种情况下，B 认为连接还未建立成功，将忽略 A 发来的任何数据分组，只等待连接确认应答分组。

而 A 发出的分组超时后，重复发送同样的分组。这样就形成了死锁。

第六章 应用层

6-01 因特网的域名结构是怎么样的？

答：

- (1) 域名的结构由标号序列组成，各标号之间用点隔开：
... . 三级域名 . 二级域名 . 顶级域名

各标号分别代表不同级别的域名。

6-02 域名系统的主要功能是什么？域名系统中的本地域名服务器、根域名服务器、顶级域名服务器以及权限域名服务器有何区别？

答：

域名系统的主要功能：将域名解析为主机能识别的 IP 地址。

因特网上的域名服务器系统也是按照域名的层次来安排的。每一个域名服务器都只对域名体系中的一部分进行管辖。

共有四种类型的域名服务器：根域名服务器、顶级域名服务器、权限域名服务器、本地域名服务器。工作过程如下：

(1) 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。

(2) 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。

当一个本地域名服务器不能立即回答某个主机的查询时，该本地域名服务器就以 DNS 客户的身份向某一个根域名服务器查询。若根域名服务器有被查询主机的信息，就发送 DNS 回答报文给本地域名服务器，然后本地域名服务器再回答发起查询的主机。但当根域名服务器没有被查询的主机的信息时，它一定知道某个保存有被查询的主机名字映射的授权域名服务器的 IP 地址。**通常根域名服务器用来管辖顶级域。**根域名服务器并不直接对顶级域下面所属的所有的域名进行转换，但它一定能够找到下面的所有二级域名的域名服务器。**每一个主机都必须在授权域名服务器处注册登记。**通常，**一个主机的授权域名服务器就是它的主机 ISP 的一个域名服务器。**授权域名服务器总是能够将其管辖的主机名转换为该主机的 IP 地址。因特网允许各个单位根据本单位的具体情况将本域名划分为若干个域名服务器管辖区。一般就在各管辖区中设置相应的授权域名服务器。

域名和 IP 地址的对应关系如何？

尽管 DNS 能够完成域名到 IP 地址的映射，但实际上两者并非一一对应的。如果一个主机通过两块网卡连接在两个网络上，就具有两个 IP 地址，但这两个 IP 地址可能就映射到同一个域名上。同样，一个主机可以具有两个域名管理机构分配的域名，那么这两个域名就可能具有相同的 IP 地址。

6-05 文件传送协议 FTP 的主要工作过程是怎样的？

答：

(1) FTP 使用客户服务器方式。一个 FTP 服务器进程可同时为多个客户进程提供服务。

FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求；另外有若干个从属进程，负责处理单个请求。

主进程的工作步骤：

- 1、打开熟知端口（端口号为 21），使客户进程能够连接上。
- 2、等待客户进程发出连接请求。

- 3、启动从属进程来处理客户进程发来的请求。从属进程对客户进程的请求处理完毕后即终止，但从属进程在运行期间根据需要还可能创建其他一些子进程。
- 4、回到等待状态，继续接受其他客户进程发来的请求。主进程与从属进程的处理是并发地进行。

FTP 使用两个 TCP 连接。

控制连接在整个会话期间一直保持打开，FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。

实际用于传输文件的是“数据连接”。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建“数据传送进程”和“数据连接”，用来连接客户端和服务器的数据传送进程。

数据传送进程实际完成文件的传送，在传送完毕后关闭“数据传送连接”并结束运行。

与电子邮件应用相关的协议有哪些？

发送邮件的协议：SMTP

读取邮件的协议：POP3 和 IMAP

MIME 在其邮件首部中说明了邮件的数据类型(如文本、声音、图像、视像等)，使用 MIME 可在邮件中同时传送多种类型的数据。

不要将邮件读取协议 POP 或 IMAP 与邮件传送协议 SMTP 弄混。

发信人的用户代理向源邮件服务器发送邮件，以及源邮件服务器向目的邮件服务器发送邮件，都是使用 SMTP 协议。

而 POP 协议或 IMAP 协议则是用户从目的邮件服务器上读取邮件所使用的协议。

- **mac 地址**是在**数据链路层**包裹在以太网头部中的，它主要用来识别**同一个链路中的不同计算机**。Mac 地址即网卡号，每块网卡出厂的时候，都有一个全世界独一无二的 MAC 地址，长度是 **48 个二进制位**，通常用 **12 个十六进制数**表示。该地址由 IEE E 负责分配,通常分为两个部分:地址的前 3 个字节代表厂商代码,后三个字节由厂商自行分配。
- **IP 地址**又称逻辑地址，是在**网络层的 IP 头部**里，用于**识别网络中互联的主机和路由器**，其实主要是确认子网，通过子网掩码确认某个 IP 地址所在的子网，而后再在子网内部确认 mac 地址就能找到准确的用户了。这个地址是 **32 位**的二进制数,包含两个部分:网络部分和主机(节点)部分
- **端口号**是在**传输层**包含在 TCP/UDP 头部中的，用于**识别应用程序**。一台主机上能运行多个程序，那么接收到的消息到底是哪个程序的呢？就需要端口号来确认。**16 位**

端口号有两种：

- 固定的端口号，是形如 http,telnet,ftp 等广为使用的应用协议所使用的端口号是固定的
- 动态分配的端口号，这个时候服务端要确定监听端口号，接受服务的客户端没必要确定端口号

端口号由传输层协议决定，因此不同传输协议可以使用相同的端口号，所以 TCP 和 UDP 可以使用同一个端口号

冲突检测即发送站点在发送数据时要边**发送**边监听信道，若监听到信道有**干扰信号**，则表示产生了冲突，于是就要停止发送数据，计算出退避等待时间，然后使用 **CSMA** 方法继续尝试发送。计算退避等待时间采用的是“二进制指数退避算法”。

载波侦听多路访问/碰撞检测 (CSMA/CD)

此方案要求设备在发送帧的同时要对信道进行侦听，以确定是否发生碰撞，若在发送数据过程中检测到碰撞，则进行如下碰撞处理操作：^[1]

1. 发送特殊阻塞信息并立即停止发送数据：特殊阻塞信息是连续几个字节的全 1 信号，此举意在强化碰撞，以使得其它设备能尽快检测到碰撞发生。^[1]
2. 在固定时间（一开始是 1 contention period times）内等待随机的时间，再次发送。^[1]
3. 若依旧碰撞，则采用截断二进制指数退避算法进行发送。即十次之内停止前一次“固定时间”的两倍时间内随机再发送，十次后则停止前一次“固定时间”内随机再发送。尝试 16 次之后仍然失败则放弃发送。^[1]

此方案应用于

- 以太网（DIX Ethernet V2）标准，IEEE 802.3 标准^[1]

载波侦听多路访问/碰撞避免(CSMA/CA)

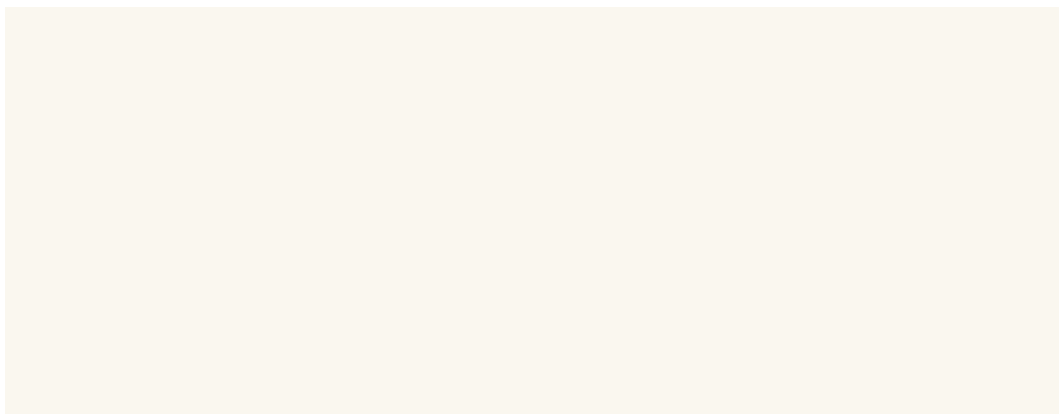
此种方案采用主动避免碰撞而非被动侦测的方式来解决碰撞问题。可以满足那些不易准确侦测是否有碰撞发生的需求，如无线域名。^[1]

CSMA/CA 协议主要使用两种方法来避免碰撞：^[1]

1. 设备欲发送讯框（Frame），且讯框听到通道空闲时，维持一段时间后，再等待一段随机的时间依然空闲时，才提交数据。由于各个设备的等待时间是分别随机产生的，因此很大可能有所区别，由此可以减少碰撞的可能性。^[1]
2. **RTS-CTS 三向握手**（英语：handshake）：设备欲发送讯框前，先发送一个很小的 **RTS**（Request to Send）讯框给最近的接入点（Access Point），等待目标端回应 **CTS**（Clear to Send）帧后，才开始发送。此方式可以确保接下来发送数据时，不会发生碰撞。同时由于 RTS 帧与 CTS 帧都很小，让发送的无效开销变小。^[1]

此方案应用于

- 无线局域网的 IEEE 802.11 标准。^[1]



英文缩写: **Best Effort**

中文译名: 尽力服务

分 类: IP 与多媒体

解 释: 标准的因特网服务模式。在[网络接口](#)发生拥塞时, 不顾及用户或应用, 马上丢弃数据包, 直到业务量有所减少为止。

尽力服务 (BE Service)是定义在 IEEE 802.16 WiMAX 中五类 [QoS](#) 服务类型的一种。802.16 服务支持五类 QoS 类型: UGS (非恳求授权服务), rtPS (实时[轮询](#)服务), ertPS (扩展的实时轮询业务), nrtPS (非实时轮询服务和 BE (尽力服务))。尽力(BE)服务的目标是提供有效服务并尽力传输。

Best-effort delivery 是指一种网络服务, 在这类服务中不保证将数据传递出去, 或不保证用户的 QoS 水平或一定的[优先级](#)。在最大努力网络中, 所以用户获得最大努力服务, 也就是说用户所获得的[比特率](#)和传输时间是不固定的, 这取决于当前网络的通信荷载的大小。

邮寄服务就使用最大努力邮递的方法来邮递邮件。并不预先规划好邮递一封邮件, 邮局并不预先做好计划。邮递员会尽力邮递一封信件, 如果当前邮局里有很多邮件, 那这些信的邮递可能被推迟。而且在邮递完一封信件后不会通知寄信人。

传统的[电话网](#)不是基于最大努力通信的, 而是基于[电路交换](#)。在一次新通话的连接期间, 在电话交互过程中分配资源, 或者通知用户由于线路忙本次通话失败。在一次成功的通话过程中, 网络过载不会中断该通话的进行, 而是为所有成功的通话保证了一定的带宽。

传统 IP 路由器仅提供最大努力服务。路由器的简易性是 IP 取得如何成功的一个重要因素。与 IP 对应的有 [X.25](#) 和 ATM, 这些都是相对复杂的协议。在 X.25 中, [点对点通信](#)中被检测到错误时会重新传输数据。[ATM 网](#)可以提供一定带宽或延迟的服务。ABR ATM (可[变比特率](#) ATM) 服务提供最大努力服务, 不保证一定水平的 [QoS](#)。

然而, Internet 中摒弃了一些最大努力方案。现代 IP 路由器为某些数据流提供不同的或可保证的 QoS 服务, 例如 [IntServ](#) 或 [DiffServ](#) 协议。这类协议可以用于容量有限的网络中, 这些网络为延迟敏感型服务和需要[恒定比特率](#)的服务 (如 IP 电话、[IP 电视](#)) 提供预留的资源。

