计算机网络

复习

@wjl

2023 年 6 月 13 日

目录

1 第一章：概述

1. 网络拓扑结构种类，特点

（1）环形拓扑：各节点通过链路相连，头尾相接，形成一个封闭的环形。特点是没有中心节点，信息在网络中循环传输。

（2）总线拓扑：所有节点通过主干链路相连，主干链路的两端有一个中心节点。特点是结构简单，但主干链路过载易造成网络瓶颈，网络容易出现故障。

（3）星形拓扑：每个节点通过链路都直接连接到中心节点。特点是结构也比较简单，中心节点过载也易造成网络瓶颈，中心节点故障会造成整个网络瘫痪。

（4）树形拓扑：节点之间无环，通过分支链路相连，类似树的枝桠结构。特点是结构清晰，易于管理，但网络差错容易造成信息阻塞，网络扩充困难。

（5）网状拓扑：节点通过多条链路相连，节点度较高，网络连接较为复杂。特点是网络可靠性高，冗余度大，容量大，但结构复杂，难以管理并消耗大量资源。

（6）分层拓扑：节点按照从高到低的层次相连，低层节点只能通过高层节点间接相连。特点是结构清晰，管理容易，但高层节点容易过载成为瓶颈。

2. 计算机网络的性能指标（知道基本概念，例如时延带宽积、吞吐量、时延等)

（1）速率：比特率（b/s, kb/s, Mb/s, Gb/s）

（2）带宽：数字信道所能传送的“最高数据率”（b/s, kb/s, Mb/s, Gb/s）

（3）吞吐量：在单位时间内通过某个网络（或信道、接口）的数据量

（4）时延：

1）发送时延：主机或路由器发送数据帧所需要的时间

2）传播时延：电磁波在信道中传播一定的距离需要花费的时间

3）处理时延：主机或路由器在收到分组时要花费一定的时间进行处理

4）排队时延：分组在进入路由器后要先在输入队列中排队等待处理

（5）时延带宽积：链路的时延带宽积又称为以比特为单位的链路长度

时延带宽积 = 传播时延 × 带宽

（6）往返时间 RTT

（7）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）

2）网络利用率则是全网络的信道利用率的加权平均值

3. 计算机网络体系结构 (3 种，各多少层，有那些层？)

（1）OSI 七层（应用层、表示层、会话层、运输层、网络层、数据链路层、物理层）。

（2）TCP/IP 四层（应用层、运输层、网际层、网络接口层）。

（3）五层协议（应用层、传输层、网络层、数据链路层、物理层）。

4. PCI, SDU, PDU 之间的关系

（1）协议控制信息 PCI：(N) 实体为了协调其共同操作使用 (N-1) 连接而交换的信息。

（2）协议数据单元 PDU：在一个 (N) 协议中规定的数据单元。

（3）服务数据单元 SDU：(N) 接口数据的总额，在从 (N) 连接的一端传送到另一端时，它的本体收到保护。

5. 电路交换、报文交换和分组交换的主要优缺点

（1）电路交换：整个报文的比特流连续地从源点直达终点，好像在一个管道中传送。

（2）报文交换：整个报文先传送到相邻结点，全部存储下来后查找转发表，转发到下一个结点。

（3）分组交换：单个分组（这只是整个报文的一部分）传送到相邻结点，存储下来后查找转发表，转发到下一个结点。

6. C/S, P2P

（1）客户服务器方式（C/S 方式）即 Client/Server 方式

（2）对等方式（P2P 方式）即 Peer-to-Peer 方式

7. 因特网标准制定阶段，RFC

（1）因特网草案 (Internet Draft) ——在这个阶段还不是 RFC 文档

（2）建议标准 (Proposed Standard) ——从这个阶段开始就成为 RFC 文档

（3）草案标准 (Draft Standard)

（4）因特网标准 (Internet Standard)

2 第二章：物理层

2.1 基本概念

1. 传输媒体的种类，传输基本原理

架空明线、双绞线、对称电缆、同轴电缆、光缆，以及各种波段的无线信道等。

2. 单工、双工、半双工通信

（1）单向通信：又称为单工通信，即只能有一个方向的通信而没有反方向的交互

（2）双向交替通信：又称为半双工通信，即通信的双方都可以发送信息，但不能双方同时发送或接收

（3）双向同时通信：又称为全双工通信，即通信的双方可以同时发送和接收信息

3. 传输介质标注

传输介质是网络物理层用于传输数据的实际介质：

（1）双绞线 (Twisted Pair)：最常用的传输介质之一，由双绞的铜线组成。常用于短距离通信，速度较慢。

（2）同轴电缆 (Coaxial Cable)：由同轴主体和绝缘层组成。速度中等，可用于中等距离。

（3）光纤 (Fiber Optic)：用轻质玻璃纤维传输光信号。速度极快，距离超长。

（4）无线电波：通过空中的电磁波实现无线通信。速度受 RF 频段限制。用于移动通信与 WLAN。

（5）卫星通信：使用人造卫星来中继和反射电磁波，实现超长距离通信。

4. 不归零码、曼彻斯特与差分曼彻斯特的特点

（1）**不归零制**：正电平代表 1，负电平代表 0。

（2）**曼彻斯特编码**：位周期中心的向上跳变代表 0，位周期中心的向下跳变代表 1。

（3）**差分曼彻斯特编码**：在每一位的中心处始终都有跳变。位开始边界有跳变代表 0，而位开始边界没有跳变代表 1。

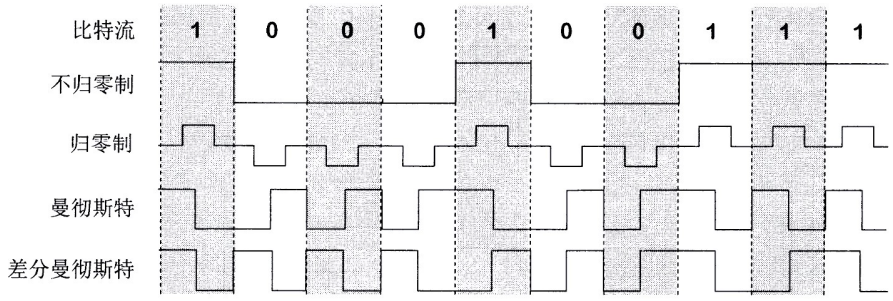


图 1: 数字信号常用的编码方式

（4）从信号波形中可以看出，曼彻斯特编码产生的信号频率比不归零制高。从自同步能力来看，不归零制不能从信号波形本身中提取信号时钟频率（这叫做没有自同步能力），而曼彻斯特编码具有自同步能力。

5. 信道复用技术，TDM, FDM, WDM, CDM 的基本概念

信道复用技术是指在有限的传输介质上建立多个独立的信道，以提高传输效率的技术。

（1）时分复用 (TDM)：在时间轴上划分多个时隙，各个信号轮流使用不同的时隙传输，实现信道复用。特点是结构简单，但带宽利用率较低。

（2）频分复用 (FDM)：在频率轴上划分多个频段，各个信号使用不同的载波频率传输，实现信道复用。特点是可以实现无交叉信号传输，但频带利用率较低。

（3）波分复用 (WDM)：在光频轴上划分多个波段，各个光信号使用不同波长的光载波传输，实现光纤复用。特点是大幅提高光纤带宽利用率，但需要光源及相关设备支持。

（4）码分复用 (CDM)：在码轴上划分多个码域，各个信号使用不同的编码方式传输，在接收端解码分离，实现信道复用。特点是理论上可以实现无限信道复用，但编码和解码较为复杂。

2.2 习题

1. 物理层要解决哪些问题？物理层的主要特点是什么？

物理层考虑的是怎样才能在连接各种计算机的传输媒体上传输数据比特流，而不是指具体的传输媒体。现有的计算机网络中的硬件设备和传输媒体的种类非常繁多，而通信手段也有许多不同方式。物理层的作用正是要尽可能地屏蔽掉这些传输媒体和通信手段的差异，使物理层上面的数据链路层感觉不到这些差异，这样就可使数据链路层只需要考虑如何完成本层的协议和服务，而不必考虑网络具体的传输媒体和通信手段是什么

在物理层上所传数据的单位是比特。发送方发送 1（或 0）时，接收方应当收到 1（或 0）而不是 0（或 1）。因此物理层要考虑用多大的电压代表“1”或“0”，以及接收方如何识别出发送方所发送的比特。物理层还要确定连接电缆的插头应当有多少根引脚以及各引脚应如何连接。

2. 物理层的接口有哪几个方面的特性？各包含些什么内容？

（1）**机械特性**：指明接口所用接线器的形状和尺寸、引脚数目和排列、固定和锁定装置等

（2）**电气特性**：指明在接口电缆的各条线上出现的电压的范围

（3）**功能特性**：指明某条线上出现的某一电平的电压的意义

（4）**过程特性**：指明对于不同功能的各种可能事件的出现顺序

3. 数据在信道中的传输速率受哪些因素的限制？信噪比能否任意提高？香农公式在数据通信中的意义是什么？“比特/每秒”和“码元/每秒”有何区别？

带宽、信噪比

信噪比不能任意提高

只要信息传输速率低于信道的极限信息传输速率，就一定存在某种办法来实现无差错的传输

“比特/秒”和“码元/秒”是不完全一样的，因为比特和码元所代表的意思并不相同。在使用二进制编码时，一个码元对应于一个比特。在这种情况下，“比特/秒”和“码元/秒”在数值上是一样的。但一个码元不一定总是对应于一个比特。根据编码的不同，一个码元可以对应于几个比特，但也可以是几个码元对应于一个比特。

4. 假定某信道受奈氏准则限制的最高码元速率为 20000 码元/秒。如果采用振幅调制，把码元的振幅划分为 16 个不同等级来传送，那么可以获得多高的数据率 (b/s)?

$C = 20000 * log_2 16 = 80000bps$

5. 用香农公式计算一下，假定信道带宽为 3100Hz，最大信息传输速率为 35kb/s，那么若想使最大信息传输速率增加 60%，问信噪比 S/N 应增大到多少倍？如果在刚才计算出的基础上将信噪比 S/N 再增大到 10 倍，问最大信息速率能否再增加 20%?

$$\frac{S/N_2}{S/N_1} = \frac{2^{1.6*(C_1/W)} - 1}{2^{C_1/W} - 1} = 109$$

信噪比增大到 109 倍

$$\frac{C_3}{C_2} = \frac{log_2[1 + 109 * 10 * (2^{C_1/W} - 1)]}{log_2[1 + 109 * (2^{C_1/W} - 1)]} = 1.18$$

最大信息速率只能增加 18%

6. 共有四个站进行码分多址 CDMA 通信。四个站的码片序列为：

A: (-1 -1 -1 +1 +1 -1 +1 +1)　B: (-1 -1 +1 -1 +1 +1 +1 -1)

C: (-1 +1 -1 +1 +1 +1 -1 -1)　D: (-1 +1 -1 -1 -1 -1 +1 -1)

现收到这样的码片序列：(-1 +1 -3 +1 -1 -3 +1 +1)。问哪个站发送数据了？发送数据的站发送的是 1 还是 0?

$A \cdot (-1+1-3+1-1-3+1+1) = 1$

$B \cdot (-1+1-3+1-1-3+1+1) = -1$

$C \cdot (-1+1-3+1-1-3+1+1) = 0$

$D \cdot (-1+1-3+1-1-3+1+1) = 1$

A, D 发送了 1，B 发送了 0，C 没发送

7. 为什么在 ADSL 技术中，在不到 1MHz 的带宽中却可以使传送速率高达每秒几个兆比特?

靠先进的编码，使得每秒传送一个码元就相当于每秒传送多个比特。

3 第三章：数据链路层

3.1 基本概念

1. PPP 协议，概念理解

（1）一个将 P 数据报封装到串行链路的方法。PPP 既支持异步链路（无奇偶检验的 8 比特数据），也支持面向比特的同步链路。P 数据报在 PPP 帧中就是其信息部分。这个信息部分的长度受最大传送单元 MTU 的限制。

（2）一个用来建立、配置和测试数据链路连接的链路控制协议 LCP。

（3）一套网络控制协议 NCP，其中的每一个协议支持不同的网络层协议。

2. 零比特插入/删除

在发送端，先扫描整个信息字段，只要发现有 5 个连续 1，则立即填入一个 0。经过这种零比特填充后的数据可以保证在信息字段中不会出现 6 个连续 1。

接收端在收到一个帧时，先找到标志字段 F 以确定一个帧的边界，接着对比特流进行扫描，每当发现 5 个连续 1 时，就把这 5 个连续 1 后的一个 0 删除，还原成原来的比特流。

保证了透明传输：在所传送的数据比特流中可以传送任意组合的比特流，而不会引起对帧边界的错误判断。

3. CSMA/CD 协议原理

（1）“多点接入”：说明是总线型网络，许多计算机以多点接入的方式连接在一根总线上。协议的实质是“载波监听”和“碰撞检测”。

（2）“载波监听”：用电子技术检测总线上有没有其他计算机也在发送。载波监听就是检测信道。在发送前检测信道，是为了获得发送权。在发送中检测信道，是为了及时发现有没有其他站的发送和本站发送的碰撞。

（3）“碰撞检测”：即适配器边发送数据边检测信道上的信号电压的变化情况，以便判断自己在发送数据时其他站是否也在发送数据。当几个站同时在总线上发送数据时，总线上的信号电压变化幅度将会增大（互相叠加）。当适配器检测到的信号电压变化幅度超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了碰撞。

4. 以太网帧的格式，长度

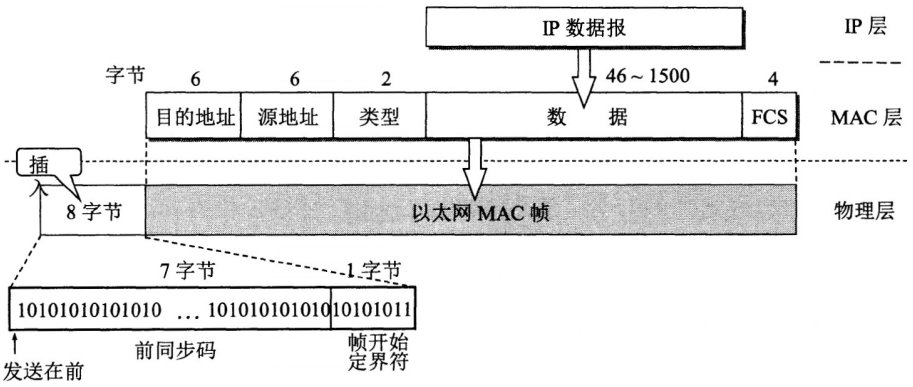


图 2: 以太网 V2 的 MAC 帧格式

数据字段的长度在 46 - 1500 字节之间，MAC 帧首部和尾部的长度共有 18 字节，有效的 MAC 帧长度为 64 - 1518 字节之间。

在传输媒体上实际传送的要比 MAC 帧还**多 8 个字节**，当一个站刚开始接收 MAC 帧时，为了接收端迅速实现位同步，从 MAC 子层向下传到物理层时还要在帧的前面插入 8 字节。

5. 网络中的设备有哪些类型，各自工作在什么层次上

（1）终端设备、服务器：应用层（2）防火墙：网络层和传输层（3）路由器：网络层（4）网桥、交换机：数据链路层（5）Modem、集线器、中继器：物理层

6. 虚拟局域网基本原理，标准是什么?

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。每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的计算机属于哪一个 VLAN。

802.3ac 标准定义了以太网的帧格式的扩展，以便支持虚拟局域网。

7. 网桥如何转发数据? 网桥的基本工作原理?

网桥对收到的帧根据其 MAC 帧的目的地址进行转发和过滤。当网桥收到一个帧时，并不是向所有的接口转发此帧，而是根据此帧的目的 MAC 地址，查找网桥中的地址表，然后确定将该帧转发到哪一个接口，或者是把它丢弃（即过滤）。

3.2 习题

1. 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?

110101101100000 / 10011 余数 01110　传送的数据为 110101101101110

110101101101100 / 10011 余数 00111　110101101101000 / 10011 余数 00011　不可靠

2. PPP 协议使用同步传输技术传送比特串 0110111111111100。试问经过零比特填充后变成怎样的比特串? 若接收端收到的 PPP 帧的数据部分是 000111011111010111110110，问删除发送端加入的零比特后变成怎样的比特串?

0110111111111100 填充 011011111011111000

000111011111010111110110 删除 000111011111111111110

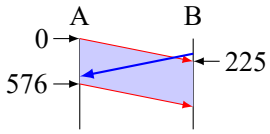
3. PPP 协议的工作状态有哪几种? 当用户要使用 PPP 协议和 ISP 建立连接进行通信需要建立哪几种连接? 每一种连接解决什么问题?

“链路终止”，“链路静止”，“链路建立”，“鉴别”，“网络层协议”，“链路打开”。链路静止时，用户 PC 机和 ISP 的路由器之间并不存在物理层的连接。链路建立时，建立链路层的 LCP 连接。鉴别时，只允许传送 LCP 协议的分组、鉴别协议的分组以及监测链路质量的分组。网络层协议时，PPP 链路的两端的网络控制协议 NCP 根据网络层的不同协议无相交换网络层特定的网络控制分组。链路打开时，链路的两个 PPP 端点可以彼此向对方发送分组。

4. 假定在使用 CSMA/CD 协议的 10Mb/s 以太网中某个站在发送数据时检测到碰撞，执行退避算法时选择了随机数 r=100。试问这个站需要等待多长时间后才能再次发送数据? 如果是 100Mb/s 的以太网呢?

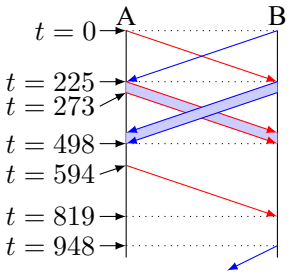
10Mb/s：$51.2\mu s * 100 = 5.12ms$　100Mb/s：$5.12\mu s * 100 = 512\mu s$

5. 假定站点 A 和 B 在同一个 10Mb/s 以太网网段上。这两个站点之间的传播时延为 225 比特时间。现假定 A 开始发送一帧，并且在 A 发送结束之前 B 也发送一帧。如果 A 发送的是以太网所容许的最短的帧，那么 A 在检测到和 B 发生碰撞之前能否把自己的数据发送完毕? 换言之，如果 A 在发送完毕之前并没有检测到碰撞，那么能否肯定 A 所发送的帧不会和 B 发送的帧发生碰撞? （提示：在计算时应当考虑到每一个以太网帧在发送到信道上时，在 MAC 帧前面还要增加若干字节的前同步码和帧定界符）



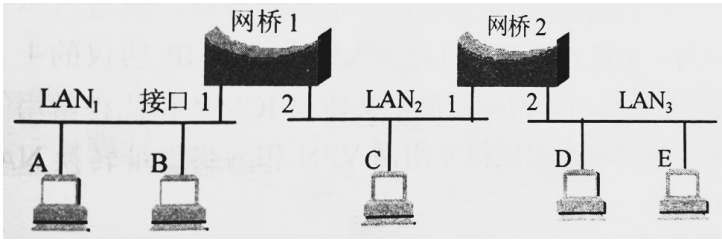
设在 $t=0$ 时 A 开始发送，在 $t=(64+8)*8=576$ 比特时间，A 应当发送完毕。$t=225$ 比特时间，B 就检测出 A 的信号。只要 B 在 $t=224$ 比特时间之前发送数据，A 在发送完毕之前就一定检测到碰撞，就能够肯定以后也不会再发送碰撞了。如果 A 在发送完毕之前并没有检测到碰撞，那么就能够肯定 A 所发送的帧不会和 B 发送的帧发生碰撞。

6. 在上题中的站点 A 和 B 在 $t=0$ 时同时发送了数据帧。当 $t=225$ 比特时间，A 和 B 同时检测到发生了碰撞，并且在 $t=225+48=273$ 比特时间完成了干扰信号的传输。A 和 B 在 CSMA/CD 算法中选择不同的 r 值退避。假定 A 和 B 选择的随机数分别是 $r_A=0$ 和 $r_B=1$。试问 A 和 B 各在什么时间开始重传其数据帧？A 重传的数据帧在什么时间到达 B？A 重传的数据会不会和 B 重传的数据再次发生碰撞？B 会不会在预定的重传时间停止发送数据？



A 在 $t=273$ 时，立刻开始检测信道，此时信道并不空闲，在 $t=273+225=498$ 时 B 最后 1bit 的干扰信号传送到 A，随后 A 检测到信道开始空闲，空闲持续 96 后，即 $t=498+96=594$ 时，A 开始发送数据。A 开始发送的 1bit 在 $t=594+225=819$ 时到达 B，根据退避算法，B 在发送完干扰信号后再过一个竞争周期，即 $t=273+512=785$ 时才开始监听信道，如果信道持续空闲 96，B 将在 $t=785+96=881$ 时开始发送，虽然在 $t=785$ 时 A 的数据未到达 B，信道为空，但 $t=819$ 时，B 监听到 A 的信号，因此 B 取消预定发送，再次退避。

7. 下图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下表中。



发送的帧	B1 的转发表		B2 的转发表		B1 的处理	B2 的处理
	地址	接口	地址	接口	（转发？丢弃？登记?）	（转发？丢弃？登记?）
A → E	A	1	A	1	转发	转发
C → B	C	2	C	1	转发	转发
D → C	D	2	D	2	丢弃	转发
B → A	B	1			丢弃	接收不到

4 第四章：网络层

4.1 基本概念

1. 虚电路、数据报的联系与区别

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	到达终点的时间不一定按发送顺序
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

图 3: 虚电路服务与数据报服务的对比

2. ARP 协议的基本原理，应用范围

ARP 协议的基本原理是地址解析，用于得到网络中其他设备的 MAC 地址。

（1）IP 地址到 MAC 地址的转换：根据 IP 地址获取对应设备的 MAC 地址，从而实现 IP 地址与 MAC 地址的对应关系，为数据的转发做准备。

（2）本地网络内部通信：只在本地网络内部使用，用于本地网络中不同设备之间的 IP 地址到 MAC 地址的映射，不能跨越路由器进行 ARP 广播。

（3）广播查询方式：ARP 协议采用广播的查询方式，将 ARP 请求报文广播给整个本地网络段中的所有设备，要查询的设备会响应自己的 IP 地址和 MAC 地址，其他设备忽略。

（4）映射表维护：每个设备根据收到的 ARP 响应报文建立和维护一个 ARP 缓存表，用于记录 IP 地址与 MAC 地址的对应关系，实现快速查询。表项会定期更新或清除过期项。

（5）安全漏洞：ARP 协议采用的是广播方式和缓存表维护，容易遭到 ARP 攻击。

3. 特殊 IP 地址

表 1: 特殊 IP 地址

网络号	主机号	源地址使用	目的地址使用	代表
0	0	可以	不可以	本网络上的本主机
0	host-id	可以	不可以	本网络上的某台主机 host-id
全 1	全 1	不可以	可以	只在本网络上进行广播
net-id	全 1	不可以	可以	对 net-id 上的所有主机广播
127	any(not 0 or 1)	可以	可以	用于本地软件回环测试

4. 根据路由器收到的 IP 数据包和路由表，知道如何转发数据报，会根据路由表画出网络拓扑结构

5. CIDR 地址块划分，注意：主机 IP 不能用网络地址和广播地址，IP 地址点分十六进制和点分十进制表示

CIDR 把 32 位的 IP 地址划分为前后两个部分。前面部分是“网络前缀”，用来指明网络，后面部分则用来指明主机。其记法是：IP 地址:= < 网络前缀 >, < 主机号 >。

CIDR 使用“斜线记法”，在 IP 地址后面加上斜线“/”，然后写上网络前缀所占的位数。

CIDR 把网络前缀都相同的连续的 P 地址组成一个“CIDR 地址块”。只要知道 CDR 地址块中的任何一个地址，就可以知道这个地址块的起始地址（即最小地址）和最大地址，以及地址块中的地址数。

6. ICMP 协议的用途

（1）测试网络的连通性（2）通知发送方目的主机不可达（3）重定向网络流量（4）通知超时（5）参数问题（6）时戳请求/响应（7）路由器通告

7. IP 协议首部各字段含义，尤其是 IP 地址，TTL 字段，各字段用途是什么?

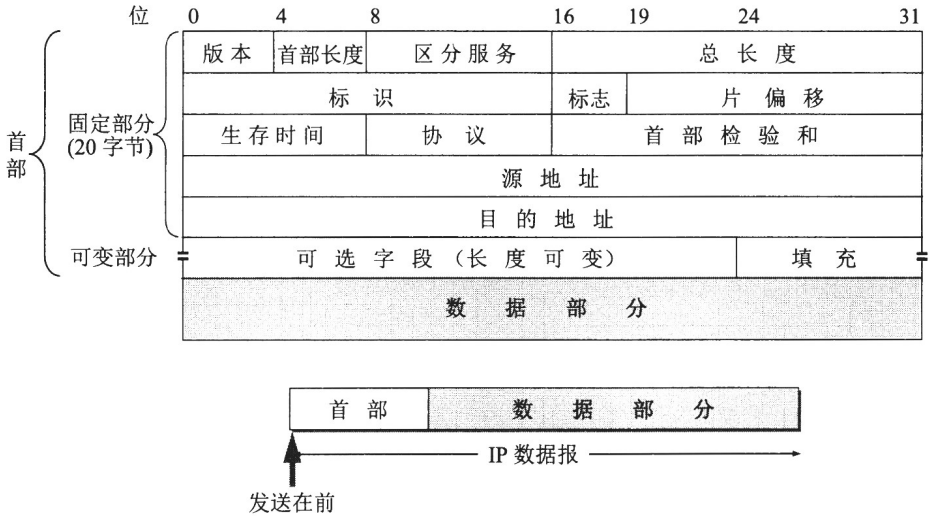


图 4: IP 数据报的格式

生存时间：占 8 位，生存时间字段 TTL(Time To Live)，路由器在每次转发数据报之前就把 TTL 值减 1。若 TTL 值减小到零，就丢弃这个数据报，不再转发。TTL 的意义是指明数据报在互联网中至多可经过多少个路由器。数据报能在互联网中经过的路由器的最大数值是 255。若把 TTL 的初始值设置为 1，就表示这个数据报只能在本局域网中传送。

4.2 习题

1. 回答以下问题：

（1）子网掩码为 255.255.255.0 代表什么意思?

（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?

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

（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?

（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?

（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?

（7）C 类网络使用子网掩码有无实际意义？为什么?

（1）网络号 24 位，主机号 8 位

（2）$2^3-2=6$ 台主机

（3）A 类网络：11111111.11111111.00001111.00000000

B 类网络：11111111.11110000.00000000.00000000

（4）$2^12-2=4094$ 台主机

（5）不是

（6）194.47.20.129，属于 C 类 P 地址

（7）有实际意义。扩展网络规模，实现路由管理，提高地址使用率，增强安全性。

2. 设 IP 数据报使用固定首部，其各字段的具体数值如图所示（除 IP 地址外，均为十进制表示）。试用二进制运算方法计算应当写入到首部检验和字段中的数值（用二进制表示）。

<table>
<tr><td>4</td><td>5</td><td>0</td><td colspan="2">28</td></tr>
<tr><td colspan="3">1</td><td>0</td><td>0</td></tr>
<tr><td colspan="2">4</td><td>17</td><td colspan="2">首部检验和（待计算后写入）</td></tr>
<tr><td colspan="5">10.12.14.5</td></tr>
<tr><td colspan="5">12.6.7.9</td></tr>
</table>

和：01110100 01001110　检验和：10001011 10110001

3. 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）？

数据部分最多为 $1200-160=1040bit$　TCP 交给 IP 的数据 $3200bit=1024+1024+1024+128$，划分为四个数据报，向上传送 $1184+1184+1184+288=3840bit$ 数据

4. 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 数据报的数据部分长度为: $4000-20=3980bit$ 故划分为 3 个数据报片, 其数据字段长度分别为 1480, 1480 和 1020bit。片偏移字段的值分别为 0, $1480/8=185$ 和 $2\times1480/8=370$。MF 字段的值分别为 1，1 和 0。

5. 设某路由器建立了如下路由表:

目的网络	子网掩码	下一跳
128.96.39.0	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

（2）128.96.40.12

（3）128.96.40.151

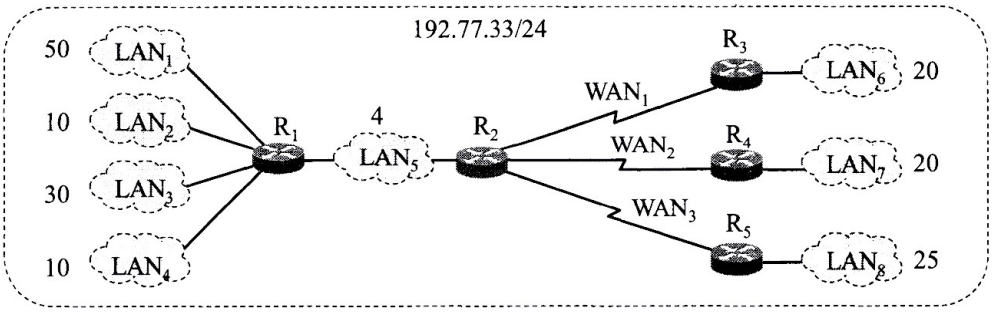
（4）192.4.153.17

（5）192.4.153.90

试分别计算其下一跳。

（1）m0　（2）R2　（3）R4　（4）R3　（5）R4

6. 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所示。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。R2 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。



LAN1 需要前缀/26（主机号 6 位，62 个主机号，R1 的接口占用一个号码）。

LAN3 需要前缀/27（主机号 5 位，30 个主机号，R1 的接口占用一个号码）。

LAN2 和 LAN4 各需要一个前缀/28（主机号 4 位，14 个主机号，R1 的接口占用一个号码）。

LAN6-LAN8（加上路由器）各需要一个前缀/27（主机号 5 位，30 个主机号，R1-R5 的接口各占用一个号码）。

3 个 WAN 各有两个端点，各需要一个前缀/30（主机号 2 位，2 个主机号）。

LAN5 需要前缀/39（主机号 3 位，用 2 个号码分配给路由器 R1 和 R2 的一个接口）。

7. 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。

10011000 00000111　10011000 00011111　152.0/11

8. 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）

N1	7	A	无新信息，因此不改变
N2	5	C	C 到 N2 的距离增大了，因此必须更新
N3	9	C	新的项目，应添加进来
N6	5	C	选择 C 为下一跳距离更短（与 F 相比），更新
N8	4	E	下一跳是 E 或 C，距离一样，因此不改变，下一跳仍为 E
N9	4	F	如下一跳是 C，则距离更大，因此不改变，下一跳仍为 F

9. 什么是 VPN？VPN 有什么特点和优缺点？VPN 有几种类别？

VPN(Virtual Private Network) 虚拟专用网络，是在公共网络上建立的一条专用连接线路，用于连接分布在不同地理位置的用户和公司内部的私有网络。

优点：（1）安全：通过加密技术保护传输数据的安全性（2）低成本：通过公共网络传输数据，避免租用专线，降低成本（3）可扩展性：易于在现有网络基础上增加新的连接。

缺点：（1）速度较慢：相比专线连接, 速度较慢（2）依赖公网：服务质量无法保证，容易受到公网质量的影响（3）管理复杂：服务越多，管理难度越大。

三种主要类别：（1）远程访问 VPN：用于连接远程用户与企业内部网络（2）站点间 VPN：用于连接不同地理位置的分公司或办事处的网络（3）网络间 VPN：用于连接不同组织的网络。

10. 什么是 NAT？NAPT 有哪些特点？NAT 的优点和缺点有哪些？

NAT(Network Address Translation) 网络地址转换，是一种转换内网私有 IP 地址与外网公有 IP 地址的技术。它可以实现内网主机与外网的通信，同时隐藏内网的 IP 地址。

特点：（1）可以实现大量内网主机共享少量公网 IP （2）可以隐藏内网的真实 IP 地址，提高安全性（3）端口号的变换可以 maximizing 同时连接数量。

优点：（1）缓解 IPv4 地址短缺问题（2）隐藏内网 IP 地址，增强网络安全性（3）实现网络路由管理中心管理（4）无需修改内网主机 IP 地址和路由配置。

缺点：（1）降低网络的透明度，增加诊断和配置难度（2）不支持内网主机公网访问（3）单点故障和性能瓶颈在 NAT 设备上（4）对某些应用程序不友好（5）存在安全性问题，NAT 设备易成为入侵目标。

11. 简述 IPV6 地址格式以及分类

（1）128 位地址长度，用 16 进制表示，分为 8 组，每组包含 4 个十六进制数字。

（2）去除了 IPv4 地址中的“.”分隔符，采用“:”分隔每个 16 位分组。

（3）可以简写的规则：1）可以去除一个或多个全 0 分组，且只能去除一次。2）若有两个或更多连续的全 0 分组，只能去除一次。3）不能只保留一个全 0 分组。

（4）按地址空间大小划分为 3 类：全球单播地址、局域网传送地址和链接本地地址：1）全球单播地址：全球路由可达，类似 IPv4 的公网地址。2）局域网传送地址：仅在局域网内路由，类似 IPv4 的私有地址。3）链接本地地址: 仅在一个网络链接内有效，用于自动配置。

12. 简述 IPV4 和 IPV6 共存的过渡技术

（1）双协议栈：在完全过渡到 IPv6 之前，使一部分主机（或路由器）装有双协议栈：一个 IPv4 和一个 IPv6。因此双协议栈主机（或路由器）既能够和 IPv6 的系统通信，又能够和 IPv4 的系统通信。双协议栈主机在和 IPv6 主机通信时采用 IPv6 地址，而和 IPv4 主机通信时则采用 IPv4 地址。

（2）隧道技术：在 IPv6 数据报要进入 IPv4 网络时，把 IPv6 数据报封装成为 IPv4 数据报。当 IPv4 数据报离开 IPv4 网络中的隧道时，再把数据部分（即原来的 IPv6 数据报）交给主机的 IPv6 协议栈。

13. 简述 IPV6 报文扩展机制

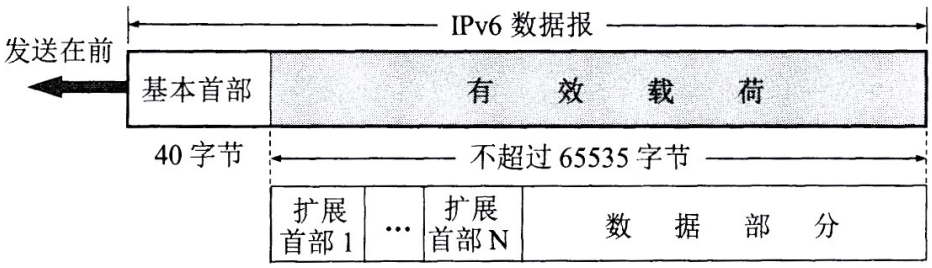


图 5: 具有多个可选扩展首部的 Pv6 数据报的一般形式

IPv6 数据报由两大部分组成，即基本首部和后面的有效载荷。有效载荷也称为净负荷。有效载荷允许有零个或多个扩展首部，再后面是数据部分。所有的扩展首部并不属于 IPv6 数据报的首部。取消了选项字段，而用扩展首部来实现选项功能。

5 第五章：运输层

1. TCP 流量控制和 TCP 拥塞控制，基本原理，之间的区别

拥塞控制就是防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。拥塞控制所要做的都有一个前提，就是网络能够承受现有的网络负荷。拥塞控制是一个全局性的过程，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。

流量控制往往是指点对点通信量的控制，是个端到端的问题（接收端控制发送端）。流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。

TCP 拥塞控制的主要原理是：通过调整发送方的数据发送速率，以避免网络拥塞并充分利用网络资源。

TCP 拥塞控制主要包括四个算法：

（1）**慢启动**：TCP 连接初始时，发送方的拥塞窗口设为 1，每收到一个 ACK, 拥塞窗口增大为原来的二倍。当窗口达到 ssthresh 时，切换到拥塞避免算法。

（2）**拥塞避免**：发送方以线性增长的方式增加拥塞窗口，直到出现丢包。一旦出现丢包，发送方重置拥塞窗口，进入快重传状态。

（3）**快重传**：一旦出现 3 个连续的重复 ACK，发送方立即重传丢失的数据包。这可以较快恢复拥塞窗口，加快数据恢复。

（4）**快恢复**：当发送方收到一个 ACK，确认重传的数据包已被接收，发送方将发送窗口增加为最初丢失前的一半。这可以较快打开发送窗口，加快拥塞恢复。

2. 滑动窗口（重点），流量控制（重点）

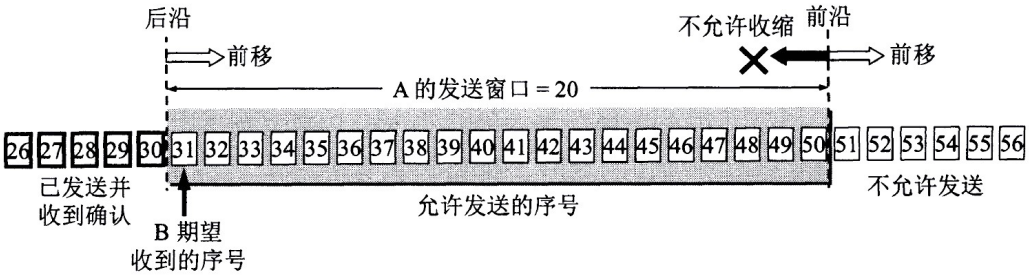


图 6: 滑动窗口

流量控制：发送方的发送窗口不能超过接收方给出的接收窗口的数值。

3. TCP 连接与释放各几次握手?

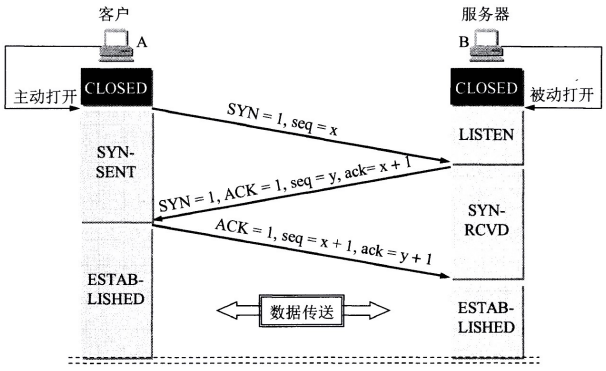


图 7: TCP 连接

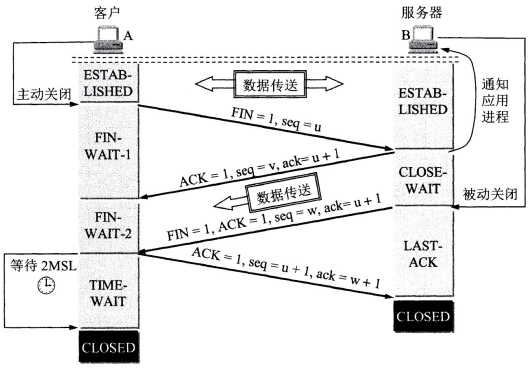


图 8: TCP 释放

4. UDP 了解

用户数据报协议 UDP 只在 IP 的数据报服务之上增加了很少一点的功能，这就是复用和分用的功能以及差错检测的功能。

UDP 的主要特点是：

（1）UDP 是无连接的，即发送数据之前不需要建立连接，因此减少了开销和发送数据之前的时延。

（2）UDP 使用尽最大努力交付，即不保证可靠交付，因此主机不需要维持复杂的连接状态表。

（3）UDP 是面向报文的。发送方的 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 一次交付一个完整的报文。因此，应用程序必须选择合适大小的报文。

（4）UDP 没有拥塞控制，因此网络出现的拥塞不会使源主机的发送速率降低。

（5）UDP 支持一对一、一对多、多对一和多对多的交互通信。

（6）UDP 的首部开销小，只有 8 个字节，比 TCP 的 20 个字节的首部要短。

6 第六章

DNS(Domain Name System)：域名系统
FTP(File Transfer Protocol)：文件传送协议
TFTP(Trivial File Transfer Protocol)：简单文件传送协议
TELNET：远程终端协议
URL(Uniform Resource Locator)：统一资源定位符
WWW(World Wide Web)：万维网
HTTP(HyperText Transfer Protocol)：超文本传送协议
SMTP(Simple Mail Transfer Protocol)：简单邮件传送协议
POP3(Post Office Protocol)：邮局协议版本 3
MIME(Multipurpose Internet Mail Extensions)：通用互联网邮件扩充
IMAP(Internet Message Access Protocol)：网际报文存取协议
DHCP(Dynamic Host Configuration Protocol)：动态主机配置协议
SNMP(Simple Network Management Protocol)：简单网络管理协议
知道中英文全称，基本概念