author: NP_123

np123greatest@gmail.com

2023 年 6 月 3 日

目录

1 物理层

1.1 Basic Concept

- 信道：将数据从一个位置传递到另一个位置需要某种形式的路径或媒体。
- 单工通信、半双工通信、全双工通信
- 带通调制：调幅、调频、调相
- 码间串扰：由于噪声干扰和衰减, 接收端收到的信号波形失去了码元之间的清晰界限
- 奈式准则：在带宽为 W 的低通信道中，若不考虑噪声影响，则码元传输的最高速率是 $2W$。传输速率超过此上限，就会出现严重的码间串扰问题，使接收端对码元的判决成为不可能。
- 信噪比：$10\log_{10}(S/N)$(似乎没提到)
- 香农公式：信道的极限信息传输速率 C 是 $C = W\log_2(1 + S/N)$
- 导引型传输媒体：双绞线、同轴电缆、光缆
- 多模光纤：近距离传输
- 单模光纤：远距离传输

1.2 信道复用技术

1.2.1 频分复用

频分复用的所有用户在同样的时间占用不同的带宽资源（请注意，这里的“带宽”是频率带宽）
波分复用就是光的频分复用，它使用一根光纤来同时传输多个光载波信号

1.2.2 时分复用

时分复用的所有用户是在不同的时间占用同样的频带宽度。

1.2.3 统计时分复用

关键：每一个 STDM 帧的时隙数小于连接在集中器中的用户数，STDM 帧不是固定分配时隙

1.2.4 码分复用 (基本概念)

令向量 S 表示站 S 的码片向量，令 T 表示其他任何站的码片向量。

$$\mathbf{S} \cdot \mathbf{T} \equiv \frac{1}{m} \sum_{i=1}^{m} S_i T_i = 0$$

且任何一个码片向量和该码片向量自己的规格化内积都是 1
接收端只需要知道 **S** 站特有的码片序列，与接收到的未知信号求内积和的运算。根据叠加原理，所有其他站的信号都被过滤掉，而只剩下 S 站发送的信号。

1.3 Basic Formula

1. 吞吐量：单位时间内通过某个网络的实际数据量
2. 发送时延：主机或路由器发送数据帧所需要的时间

$$\text{发送时延} = \frac{\text{数据帧长度}(bit)}{\text{发送速率}(bit/s)}$$

3. 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

$$\text{传播时延} = \frac{\text{信道长度}}{\text{电磁波在信道上的传播速率}}$$

4. 总时延 = 发送时延 + 传播时延 + 处理时延 + 排队时延
5. 时延带宽积 = 传播时延 $\times$ 带宽
6. 利用率 U：若 D_0 表示网络空闲时的时延，D 表示网络当前的时延

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

1.4 Important concepts

- 应用层：应用层交互的数据单元称为**报文**
- 运输层：对于 TCP 来说是**报文段**。对于 UDP 来说是**用户数据报**
- 网络层：IP 数据报、分组、数据报、包
- 数据链路层：(MAC) 帧

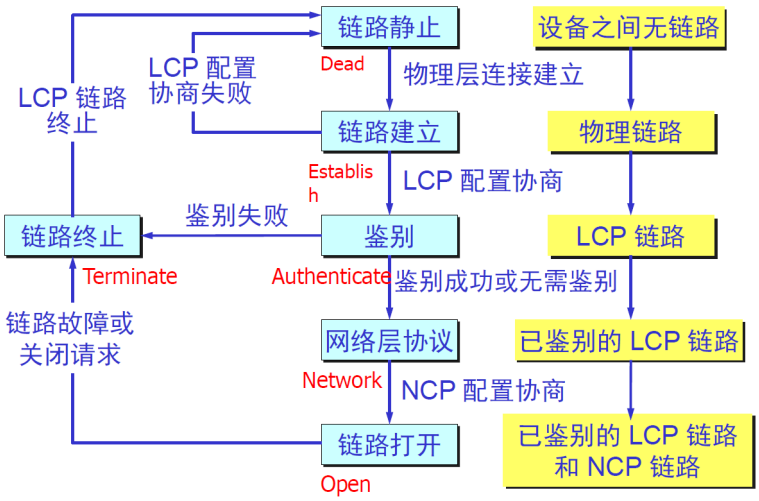
2 数据链路层

2.1 PPP 协议-使用点对点协议的数据链路层

2.1.1 PPP 协议的帧格式

1. 首部标志字段 F(0x7E)：是 PPP 帧的定界符，若连续两帧之间有两个标志字段，就表示是一个空帧，应当丢弃。
2. 地址字段 A(0xFF)：无意义
3. 控制字段 C(0x03)：无意义
4. 协议 (2B)
5. 信息部分 (不超过 1500B)
6. 尾部 FCS(2B)
7. 尾部标志字符 F(0x7E)

2.1.2 其他细节



- 字节填充：将标志符、ASCII 码填充
- 零比特填充：只要发现有 5 个连续的 1，就立即填入一个 0

2.2 以太网-使用广播信道的数据链路层

2.2.1 局域网的数据链路层

静态划分信道和动态媒体接入控制 (多点接入)：信道并非在用户通信时固定分配给用户，分为以下两类：

随机接入：所有用户可以随机地发送信息，但是需要碰撞检测

受控接入：分散控制的令牌环局域网和集中控制的多点线路**探询 (轮询)**

以太网的两个标准：802.3、DIX Ethernet V2(三个公司标准)

数据链路层的两个子层：**逻辑链路控制 LLC(作用已经消失了)、媒体接入控制 MAC**

2.2.2 CSMA/CD 协议

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

载波监听，多点接入；(with"/") 碰撞检测

特点：许多计算机都连接到一根总线 (bus) 上，在具有广播特性的总线上实现了一对一的通信

2.2.3 碰撞检测

二进制指数类型退避算法：发生碰撞的站在停止发送数据后，要推迟（退避）一个随机时间才能再发送数据。

1. 确定基本退避时间，一般是取为争用期 2τ
2. 定义重传次数 $k, k \leq 10$ 即

$$k = \text{Min}[\text{重传次数}, 10]$$

从整数集合 $[0, 1, \cdots, (2^k - 1)]$ 中随机地取出一个数，记为 r。重传所需的时延就是 r 倍的基本退避时间。

3. 当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告。

- 1 比特时间是**发送** 1 比特所需的时间，在 10Mbit/s 半双工以太网中，1 比特时间 =0.1μs
- 人为干扰信号：32bit 或者 48bit；
- 帧最小间隔 9.6μs；
- 以太网规定的最小帧长 64B，即 512bit。

2.2.4 以太网的信道利用率 (没有提到)

- 参数 α

$$\alpha = \frac{\tau}{T_0}$$

α 越大，表明争用期所占的比例增大，明显降低了信道利用率。

- 信道利用率的最大值 S_{max}

$$S_{max} = \frac{T_0}{T_0 + \tau} = \frac{1}{1 + \alpha}$$

2.2.5 以太网的 MAC 帧格式

1. 前同步码 + 帧开始定界符 (7B+1B)：以太网不需要帧结束定界符，也不需要使用字节插入来保证透明传输
2. 目的地址 (6B)
3. 源地址 (6B)

4. 类型 (2B)：标志上一层使用的是什么协议

5. 数据 (46 ～ 1500B)：故有效的 MAC 帧的长度为 64 ～ 1518B

2.2.6 在物理层扩展以太网

用**集线器/中继器**组成更大的局域网都在一个碰撞域中

2.2.7 在数据链路层扩展以太网

~~交换机淘汰了网桥~~(功能相似)，工作在数据链路层。并且使各网段成为隔离开的碰撞域。好处：

1. 过滤通信量

2. 扩大了物理范围

3. 提高了可靠性

4. 可互连不同物理层、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。

2.2.8 透明网桥

“透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的。

自学习：查找转发表中与收到帧的源地址有无相匹配项目。如没有，就在转发表中增加一个项目（源地址、进入的接口和时间）。如有，则更新原有项目。

转发帧规则：查找转发表中与收到帧的目的地址有无相匹配的项目。

- 如没有，则通过所有其他接口进行转发（但进入网桥的接口除外）。
- 如有，则按转发表中给出的接口进行转发。
- 若转发表给出的接口就是该帧进入网桥的接口，则应丢弃这个帧（不需要经过网桥进行转发）。

生成树协议 STP：整个连通的网络中不存在回路，即在任何两个站之间只有一条路径。

全双工方式，具有 N 个端口的以太网交换机碰撞域共有 N 个。

独占传输媒体的带宽：拥有 N 对接口的交换机的总容量为 $N \times 10\text{Mb}/s$。

2.2.9 虚拟局域网 VLAN

虚拟局域网其实只是局域网给用户提供的一种服务，而并不是一种新型局域网

1. IEEE 802.1Q 标签类型 (2B)

2. 没什么用...(2bit)

3. VLAN 标识符 (12bit)：唯一标志了 802.1Q 帧属于哪一个 VLAN

3 网络层

3.1 面向连接 vs. 无连接 (老师：搞清楚)

- 传统电信网认为面向连接：建立虚电路 (Virtual Circuit)，以保证双方通信所需的一切网络资源。虚电路表示这只是一条逻辑上的连接，分组都沿着这条逻辑连接按照存储转发方式传送，而并不是真正建立了一条物理连接。
- 互联网采用的设计思路：网络层向上只提供简单灵活的、无连接的、尽最大努力交付的数据报服务。

特点	虚电路服务	数据报服务
可靠通信由网络来保证	1	0
连接的建立	必须有	不需要
终点地址	每个分组使用短的虚电路号	每个分组都有终点地址
分组的转发	按照同一路由进行转发	每个分组独立选择路由转发
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	故障节点会丢失分组，路由变化
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	由网络或用户主机负责	用户主机负责

3.2 不同的网络层次使用不同的中间设备

1. 物理层：转发器 (repeater)，集线器，中继器
2. 数据链路层：网桥 (bridge)，交换机（Switch）
3. 网络层：路由器 (router)
4. 网络层以上：网关 (gateway)：**严格定义**：用网关连接两个不兼容的系统需要在高层进行协议的转换

   路由器主要用于连接相同协议的网络，而网关可以连接使用不同协议的网络

3.3 A、B、C、D、E 类 IP 地址

- A 类地址：网络号 8 位-0

  1.0.0.1 － 126.255.255.254
- B 类地址：网络号 16 位-10

  128.1.0.1 － 191.255.255.254
- C 类地址：网络号 24 位-110

  192.0.1.1 － 223.255.255.254
- D 类地址：多播地址-1110

  224.0.0.0-239.255.255.255
- E 类地址：保留为今后使用-1111

3.4 ARP(地址解析协议) 的四种情况

ARP 只缓存本局域网中的硬件地址信息

1. **发送方是主机**，要把 IP 数据报发送到本网络上的另一个主机。这时用 ARP 找到目的主机的硬件地址。
2. **发送方是主机**，要把 IP 数据报发送到另一个网络上的一个主机。这时用 ARP 找到本网络上的一个路由器的硬件地址。
3. **发送方是路由器**，要把 IP 数据报转发到本网络上的一个主机。这时用 ARP 找到目的主机的硬件地址。
4. **发送方是路由器**，要把 IP 数据报转发到另一个网络上的一个主机。这时用 ARP 找到本网络上的一个路由器的硬件地址。

3.5 IP 数据报首部

1. 版本 (4-bit)：对于 IPv4，值为 4
2. 首部长度 (4-bit)：范围 0101(5 行-20B)-1111(15 行-60B)

   * 注：如果首部长度不是 4B 的整数倍时，利用最后的填充字段加以填充
3. 区分服务 (8-bit)：用来获得更好的服务，一般情况下不适用
4. 总长度 (16-bit)：数据报最大长度为 $2^{16}-1=65535B$，但是实际传输中极少遇到。因为：

   数据链路层中 $MTU=1500B$，所以如果数据包长度大于 MTU，则需要进行分片处理。

   规定主机和路由器必须能接受长度不超过 512(normal-lenth) + 60(IP-head) + 4 = $576B$ 的数据报若主机需要发送长度超过 576 字节的数据报时，应当先了解一下，目的主机能否接受所要发送的数据报长度。否则就要进行分片。
5. 标识 (16-bit)：计数器，在分片时每个数据报片标识一样，用来重装为原来的数据报。

6. 标志 (3-bit)：empty-MF(More Fragment)-DF(Don't Fragment)

   $MF = 0$ 代表这是若干数据报片中的最后一个；$DF = 0$ 时才允许分片

7. 片偏移 (13-bit)：某片在原分组中的相对位置 (以 $8B$ 为偏移单位)，**在分片后的数据包中标识一样**。

8. 生存时间 (8-bit)：路由器在每次转发数据报之前就把 TTL 值减一，若减小到零，就丢弃这个数据报。

9. 协议 (8-bit)：携带的数据使用何种协议。

协议名	ICMP	IGMP	IP	TCP	EGP	IGP	UDP	IPv6	ESP	OSPF
协议字段值	1	2	4	6	8	9	17	41	50	89

10. 首部检验和 (16-bit)：**只检验数据报的首部，不包括数据部分**。反码算数运算求和，在接收端若结果为 0，则保留；否则，丢弃该数据报。

11. 源地址 (32-bit)

12. 目的地址 (32-bit)

3.6 使用子网掩码的分组转发过程

1. 提取 IP 地址：从收到的分组的首部 (IP 首部) 提取目的 IP 地址 D。

2. 是否在本网络上：**确定目的主机是否连接在本网络上？如果是的话那么就直接交付**。先用各网络 (路由器相连接的网络)的子网掩码和 D 逐位相“与”，看是否和相应的**网络地址**匹配。若匹配，则将分组直接交付 (直接将数据报交付给目的主机，不经过任何路由器)。否则就是间接交付 (将数据报交付给路由器)，执行 3。

目的网络地址	子网掩码	下一跳
128.30.33.0	255.255.255.128	直接交付，接口 0
128.30.33.128	255.255.255.128	直接交付，接口 1
128.30.36.0	255.255.255.0	R_2
其他	其他	默认路由下一跳，接口 3

3. 是否为主机路由：若路由表中有目的地址为 D 的特定**主机路由 (子网掩码为 255.255.255.255，且主机路由在转发表中都放在最前面。)**，则将分组传送给指明的下一跳路由器 (目的 IP 地址恰好与路由表中地址一样)；否则，执行 4.

4. 查找路由表：对路由表中的每一行的子网掩码和 D 逐位相“与”，若其结果与该行的目的网络地址匹配，则将分组传送给该行指明的下一跳路由器 (间接交付，**查找转发表的过程就是寻找前缀匹配的过程。**)

   在这里有规则**最长前缀匹配**：转发表通常为了快速查找，将前缀最长的排在第一行。如果一个分组在转发表中可以找到多个匹配的前缀，那么应当选择前缀最长的一个作为匹配的前缀 (地址块小，路由越具体)。

   ~~在这里有方法**二叉线索树**：每一个叶节点对应一个唯一前缀，并且包含所对应的网络前缀和子网掩码。当搜索到一个叶节点时，进行 4. 的操作，若不匹配则丢弃该分组。；否则，执行 5(都查不到，只能交给默认路由~~

5. 是否有默认路由：若路由表中有一个默认路由 (**特殊前缀 0.0.0.0/0**)，则将分组传送给路由表中所指明的默认路由器 (间接交付)；否则，执行 6.

6. GG：报告转发分组出错

3.7 IP 地址演化 2->3->2(没提到)

ARPANET 的早期

$$\text{IP 地址} ::= < \text{网络号 (net-id)} >, < \text{主机号 (host-id)} >$$

划分子网后的 IP 地址 (三级编址)

$$\text{IP 地址} ::= < \text{网络号 (net-id)} >, < \text{子网号 (subnet-id)} >, < \text{主机号 (host-id)} >$$

无分类编制 CIDR(两级编址)

$$\text{IP 地址} ::= < \text{网络前缀 (network-prefix)} >, < \text{主机号 (host-id)} >$$

对于 CIDR 编址来说，没有子网掩码的概念了，而使用前缀长度。

重要概念-路由聚合 (构成超网)：使得路由表中的一个项目可以表示很多个原来传统分类地址的路由，极大地减少了路由表的项目数。

3.8 ICMP(网际控制报文协议)

- ICMP 文件头：

  类型 (8-bit)；代码 (8-bit)；检验和 (16-bit)

- ICMP 差错报告报文

  终点不可达；时间超过；参数问题；改变路由（重定向）(Redirect)

- ICMP 询问报文

  回送请求和回答报文：测试目的站是否可达以及了解其有关状态

  时间戳请求和回答报文：请求某台主机或路由器回答当前日期和时间

- ICMP 的前 8 字节是为了得到 TCP 首部中的源端口和目的端口

3.9 内部网关协议 RIP()

- 优点：实现简单，开销较小

- 缺点：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）

  当网络出现故障时，要经过较长的时间才能将此信息传送到所有路由器。

  交换的路由信息是路由器中的完整路由表，因而网络规模扩大，开销也就增加

- 特点：好消息传播得快，而坏消息传播得慢

3.10 内部网关协议 OSPF

OSPE 使用层次结构的区域划分，在上层的区域叫做主干区域，标识符规定为 0.0.0.0 主干区域的作用是用来连通在下层的区域。从其它区域来的信息都由**区域边界路由器**进行概括。

主干区域内还有有一个路由器专门和本自治系统外的其他自治系统交换路由信息，**自治系统边界路由器**。

1. OSPF 对于不同类型的业务可计算出不同的路由。
2. 负载均衡。将通信量分配给多条相同代价的路径。
3. 所有交换的分组都具有鉴别的功能，仅在可信赖的路由器之间交换链路状态信息
4. 每个链路状态带有一个 32 位的序号

3.11 外部网关协议 BGP(老师：不重要)

3.11.1 BGP 所使用的环境遇到的问题

- 因特网规模太大，AS 之间要寻找最佳路由不现实
- 自治系统之间的路由选择必须考虑有关策略

解决方法：比较合理的做法是在 AS 之间交换“可达性”信息，力求寻找一条能够到达目的网络且比较好的路由

3.11.2 BGP 发言人

介绍：每一个自治系统的管理员要选择至少一个路由器作为该自治系统的“BGP 发言人”。

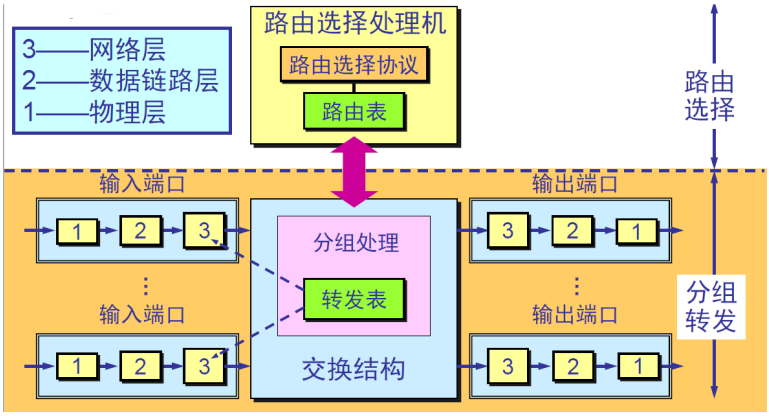
两个 BGP 发言人通过一个共享网络连接在一起，BGP 发言人往往就是 BGP 边界路由器，但也可以不是 BGP 边界路由器。

BGP 发言人交换网络可达性信息 (到达某个网络所要经过的一系列 AS。)。各 BGP 发言人就根据所采用的策略从收到的路由信息中找出到达各 AS 的较好路由。

3.12 路由器的构成 (老师：可能出的题被张老师删掉了)

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

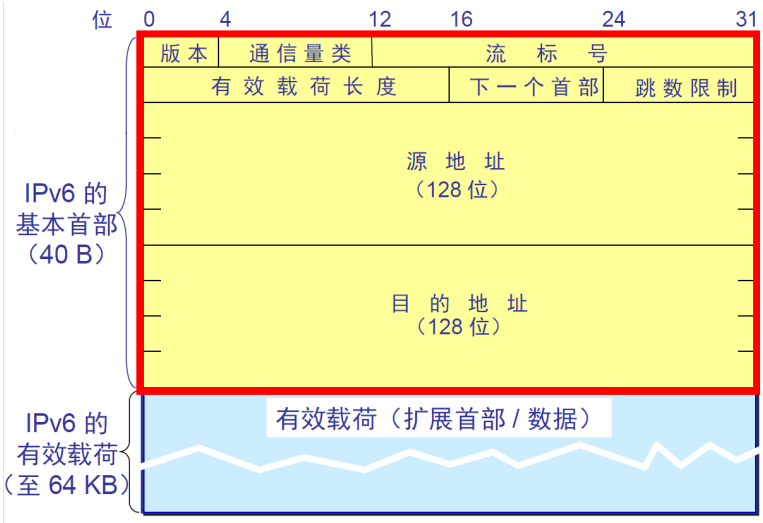
- 转发：路由器根据转发表将用户的 IP 数据报从合适的端口转发出去。
- 路由选择：按照分布式算法，根据从各相邻路由器得到的关于网络拓扑的变化情况，动态地改变所选择的路由。
- **路由表和转发表的区别**：路由表是根据路由选择算法得出的。而转发表是从路由表得出的。
- 分组丢弃：若路由器处理分组的速率赶不上分组进入队列的速率，则队列的存储空间最终必定被填满，这就使后面进入队列的分组由于没有存储空间而只能被丢弃；路由器中的输入或输出队列产生溢出是造成分组丢失的重要原因。
- 交换结构



- 通过存储器：目的地址的查找和分组在存储器中的缓存都是在输入端口进行的。
- 通过总线：数据报从输入端口通过共享总线直接传送到合适的输出端口，而不需要路由选择处理机的干预 (只能由一个分组在总线上传输，转发带宽受总线速率限制。)
- 通过互连网络：无阻塞的交换结构，分组可以转发到任何一个输出端口，只要这个输出端口没有被别的分组占用。

3.13 IPv6(基本概念弄懂)

3.13.1 IPv6 的基本首部



1. 版本 (4-bit)：对于 IPv6，值为 6
2. 通信量类 (8-bit)：与 IPv4 的区分服务相似。
3. 流标号 (20-bit)：“流”是互联网络上从特定源点到特定终点的一系列数据报，“流”所经过的路径上的路由器都保证指明的服务质量。**所有属于同一个流的数据报都具有同样的流标号。**
4. 有效载荷长度 (16-bit)：除了基本首部以外的字节数（扩展首部算在有效载荷以内）。最大值 (65535B)
5. 下一个首部 (8-bit)：相当于 IPv4 的协议字段或可选字段：

(a) 当 IPv6 数据报没有扩展首部时，下一个首部字段的作用和 IPv4 的协议字段一样，指出了基本首部后面的数据应交付 IP 层上面的哪一个高层协议

(b) 当出现扩展首部时，下一个首部字段的值就标识后面第一个扩展首部的类型。

6. 条数限制 (8-bit)
7. 源地址 (128-bit)
8. 目的地址 (128-bit)

3.13.2 其他知识

- IPv6 不在路由器中分片，只允许在网络边缘的主机中 (源点) 进行分片。
- 全球单播地址的等级结构:书中和 ppt 有冲突，问黄健华
- IPv6 地址压缩：00AA 可以简写为 AA

3.14 ~~IP 多播~~

3.14.1 ~~基本概念~~

~~多播地址只能用于目的地址，而不能用于源地址~~
~~IP 多播可以分为两种：一种是只在本局域网上进行硬件多播；另一种是在互联网的范围进行多播~~
~~总之，多播数据报可以由没有加入多播组的主机发出，也可以通过没有组成员接入的网络。~~

3.14.2 ~~网际组管理协议 IGMP~~

~~运行于主机和与主机直接相连的组播路由器之间~~
~~IGMP 实现的功能是双向的：~~

- ~~一方面，通过 IGMP 协议，主机通知本地路由由器希望加入并接收某个特定组播组的信息~~
  ~~新的主机要加入组播组，主动发送报告消息；当主机要离开组播组时，发送离开组消息~~
  ~~通过上述机制，在组播路由器里建立起一张表，记录了各个接口所对应的子网上都有哪些组的成员。当路由器接收~~
  ~~的数据报文后，只向那些有 G 的成员的接口转发数据报文~~
- ~~另一方面，路由器通过 IGMP 协议查询局域网内某个组的成员是否处于活动状态~~
- ~~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，等等。~~

3.14.3 ~~多播路由选择协议~~

~~多播路由选择实际上就是要找出以源主机为根结点的多播转发树。~~
~~转发多播数据报使用的方法~~

1. ~~洪泛与剪除：反向路径广播 RPB 和剪除：检查数据报是否是从源点经最短路径传送来的。若是则转发，否则就~~
2. ~~隧道技术：若路由器 R_1 和 R_2 之间的网络不支持多播。路由器 R_1 就对多播数据报进行再次封装，即再加上普通~~
3. ~~基于核心的发现技术：这种方法对每一个多播组 G 指定一个核心 (core) 路由器，给出它的 IP 单播地址。~~

3.15 VPN、NAT(老师：概念)

IPv4 专用地址块 (专用 IP 地址也叫做可重用地址)：

1. 10.0.0.0 到 10.255.255.255
2. 172.16.0.0 到 172.31.255.255
3. 192.168.0.0 到 192.168.255.255

- 虚拟专用网 VPN：所有通过互联网传送的数据都必须加密
- 网络地址转化 NAT：至少有一个有效的外部全球 IP 地址，所有使用本地地址的主机在和外界通信时，都要在 NAT 路由器上将其本地地址转换成全球 IP 地址，才能和互联网连接。

3.16 易错点

- 多归属主机 (multihomedhost)

  当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号 net-id 必须是不同的。

- 由于一个路由器至少应当连接到两个网络，因此一个路由器至少应当有两个不同的 IP 地址。
- 如果 net-id 是具体的网络号，而 host-id 是全 1，就叫做**定向广播**，因为这是对 net-id 指明的网络上的所有主机进行广播的一种地址。
- IP 数据报中不仅头部的内容，数据的内容也要是 32bit 的整数倍，否则需要用 0 填充。
- 在网络分配本网络的主机号时，不允许重复使用子网中的任何一个地址。

  例：网络 11.1.2.0/24 是网络 11.0.0.0/8 的一个子网。网络 11.0.0.0/8 给它的一台主机分配 IP 地址 11.1.2.3 是不被允许的。

- IPv4 进行首部检测，但是 IPv6 不进行，这是因为当初设计 IPv4 的时候没有考虑到在数据链路层已经完成了对数据部分的全部检测。

4 运输层

4.1 Basic Concept

运输层向它上面的应用层提供通信服务，它属于面向通信部分的最高层，同时也是用户功能中的最低层。

一般位于**网络边缘**的主机的协议栈才有运输层，而网络核心部分中的路由器在转发分组时都只用到下三层的功能。运输层为相互通信的应用进程提供了**逻辑通信** (只要应用层报文交给下面的运输层，运输层就可以把这报文传送到对方的运输层。“好像是这样通信，但事实上并非真的这样通信”)

4.1.1 复用和分用 (老师：重点)

- 复用：发送方不同的应用进程都可以使用同一个运输层协议传送数据。
- 分用：接收方的运输层在剥去报文的首部后能把这些数据正确交付目的应用进程。

4.1.2 网络层和运输层的区别

网络层为主机之间的通信提供服务，而运输层在网络层的基础上为应用进程之间的通信提供服务。一个到机器为止，一个到进程为止

运输层还要对收到的报文进行差错检测

4.1.3 端口

- 端口号只具有**本地意义**：只是为了标志本计算机应用层中的各个进程在和运输层交互时的层间接口。在互联网不同计算机中，相同的端口号是没有关联的。
- 服务器端使用的端口号：

  熟知端口，数值一般为 0 ～ 1023：http：80, ftp：21，SMTP：25, https: 443

  登记端口号，数值一般为 1024 49151
- 客户端使用的端口号 (短暂端口号)：49152 65535

4.2 用户数据报协议 UDP

4.2.1 主要特点 (老师：都要好好复习，记住)

- 无连接的
- 尽最大努力交付的
- 面向报文的 (保留这些报文的边界：应用层交给 UDP 多长的报文，UDP 就照样发送。如果太长交给 IP 层分片)
- 没有拥塞控制
- 支持一对一、一对多、多对一和多对多的交互通信 (多播)
- 首部开销小 (8B)

4.2.2 首部格式

- 伪首部 (12B)：用来计算检验和
- 源端口 (2B)：需要对方回信时选用，不需要时可用全 0
- 目的端口 (2B)：终点交付报文时使用
- 长度 (2B)：当只有首部时，最小值为 8
- 检验和 (2B)：有错就丢弃

4.2.3 计算 UDP 检验和

既检查了 UDP 用户数据报的源端口号和目的端口号以及 UDP 用户数据报的数据部分，又检查了 IP 数据报的源 IP 地址和目的地址。

4.3 运输控制协议 TCP

4.3.1 主要特点

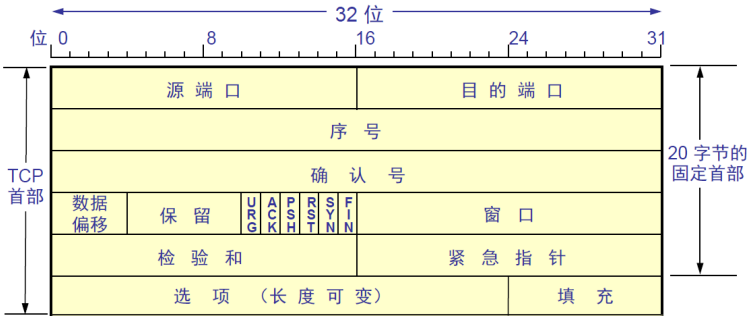
1. 面向连接的运输层协议
2. 每条 TCP 连接只能有两个端点 (点对点)
3. 提供可靠交付的服务：无差错、不丢失、不重复，并且按需到达
4. 提供全双工通信
5. 面向字节流：TCP 把应用程序交下来的数据仅仅看成是一连串的无结构的字节流。
6. TCP 连接是一条虚连接

每一条 TCP 连接唯一地被通信两端地两个端点所确定

$$\text{TCP 连接} ::= \text{socket}_1, \text{socket}_2 = (\text{IP}_1 : \text{port}_1, \text{IP}_2 : \text{port}_2)$$

4.4 四个计时器 (很重要，书中没有总结)

1. 超时计时器：在每发送完一个分组时设置一个超时计时器，实现**超时重传**
2. 持续计时器：只要 TCP 连接的一方收到对方的零窗口通知，就启动持续计时器。若持续计时器的时间到期，就发送一个零窗口的**探测报文段**。对方在确认这个探测报文段时给出了现在的窗口值。
3. 时间等待计时器：经过设置好的时间 2MSL 后，A 才进入到 CLOSED 状态。设置它的原因
4. 保活计时器：服务器每收到一次客户的数据，就重新设置保活计时器，时间的设置通常是两小时。若两小时没有收到客户的数据，服务器就发送一个探测报文段，以后则每隔 75 秒钟发送一次。若 10 个探测报文段仍无响应，则关闭连接



4.5 首部格式

1. 源端口 (2B)
2. 目的端口 (2B)
3. 序号 (4B)：序号使用 mod2^{32} 计算。TCP 连接中传送的字节流中的每一个字节都按顺序编号。
4. 确认号 (4B)：期望收到对方下一个报文段的第一个数据字节的序号。

   若确认号 $= N$，则表明到序号 $N-1$ 为止的所有数据都已正确收到。
5. 数据偏移 (首部长度)(1B)：TCP 首部最大值为 60B(选项长度不能超过 40B)
6. 保留 (6-bit)：今后使用，目前置为 0
7. 紧急 URG：高优先级的数据，与紧急指针字段配合使用
8. 确认 ACK：在连接建立后所有传送的报文段都必须把 ACK 置为 1。
9. 推送 PSH：尽快交付接收应用进程。
10. 复位 RST：出现严重差错，重新建立连接；拒绝非法报文段，拒绝打开连接。
11. 同步 SYN
12. 终止 FIN
13. 窗口 (2B)：接收窗口，作为接收方让发送方设置其发送窗口的依据。

    窗口字段明确指出了现在允许对方发送的数据量。窗口值经常在动态变化着。
14. 检验和 (2B)：检验和字段检验的范围包括首部和数据这两部分。在计算检验和时，要在 TCP 报文段的前面加上 12 字节的伪首部。
15. 紧急指针 (2B)：指出在本报文段中紧急数据共有多少个字节 (紧急数据结束后就是普通数据)

补充：TCP-MSS 的原理：建立 tcp 连接的两端在三次握手时会协商 tcp mss 大小
MSS 是 TCP 报文段中**数据字段**的最大长度

4.6 TCP 可靠传输

- TCP 标准强烈不赞成发送窗口前沿向后收缩
- 可用窗口：允许发送但尚未发送的字节数
- 发送缓存用来暂时存放：
  1. 发送应用程序传送给发送方 TCP 准备发送的数据
  2. TCP 已发送出但尚未收到确认的数据
- 接收缓存用来暂时存放：
  1. 按序到达的、但尚未被接收应用程序读取的数据
  2. 不按序到达的数据

4.7 拥塞控制

$$\sum \text{对资源的需求} > \text{可用资源}$$

4.7.1 拥塞控制和流量控制的区别

拥塞控制就是防止过多的数据注入到网络中，使网络中的路由器或链路不至于过载 (全局性过程)

流量控制往往是指点对点流通量的控制，是个端到端的问题。要做的是抑制发送端发送数据的速率，以便接收端来得及接受。

4.7.2 TCP 拥塞控制的四个算法 (老师：配合使用，关系，要搞清楚，出了好多题目)

1. 慢开始：由小到大逐渐增大注入到网络中的数据字节 (拥塞窗口数值)
2. 拥塞避免：每经过一个往返时间 RTT，发送方的拥塞窗口 cwnd 的大小就加一
3. 快重传：要求对方立即发送确认，即使收到了失序的报文段也要立即发出对已收到的报文段的重复确认；发送方只要一连收到 3 个确认，就立即重传 (即" 快重传")
4. 快恢复：令 ssthresh=cwnd/2；cwnd=ssthresh。并开始执行拥塞避免算法

$$\text{发送方窗口的上限值} = \text{Min}[\text{rwnd}, \text{cwnd}]$$

4.7.3 主动队列管理 AQM(没提到)

许多 TCP 连接在同一时间突然都进入到慢开始状态，叫做**全局同步**。

主动队列管理 AQM：实现方法：随机早期检测，维持两个参数：队列长度最小门限和最大门限。出现早期征兆时，就以概率 p 丢弃个别的分组。

4.8 超时重传时间的选择 (似乎没提到)

超时重传时间 RTO

$$RTO = RTT_S + 4 \times RTT_D$$

其中 RTT_S 是 RTT 的一个加权平均往返时间：以后每测量到一个新的 RTT 样本，就按下式重新计算一次 RTT_S：

$$\text{新的}RTT_S = (1-\alpha) \times (\text{旧的}RTT_S) + \alpha \times (\text{新的}RTT\text{样本})$$

RTT_D 是 RTT 的偏差的加权平均值：第一次测量时，RTT_D 值取为测量到的 RTT 样本值的一半。以后测量时：

$$\text{新的}RTT_D = (1-\beta) \times (\text{旧的}RTT_D) + \beta \times |RTT_S - \text{新的}RTT\text{样本}|$$

修正的 Karn 算法：报文段每重传一次，就把 RTO 增大一些：

$$\text{新的}RTO = \gamma \times \text{旧的}RTO$$

一般而言：$\alpha = 0.125, \beta = 0.25$

4.9 TCP 运输连接管理

4.9.1 为什么三次握手，不是两次？

为了防止已失效的连接请求报文段突然又传送到了 B，因而产生错误。

4.9.2 为什么 TIME-WAIT 状态必须等待 2MSL 的时间呢？

1. 为了保证 A 发送的最后一个 ACK 报文段能够到达 B。如果 B 没有收到 A 发送的最后一个 ACK 报文，B 会超时重传 FIN_ACK 报文，此时 A 在收到后重传最后一个 ACK 报文，并且重置 2MSL 计时器。
2. 防止已失效的连接请求报文段出现在本链接中。

4.9.3 一些细节

- 三次握手时，前两次握手消耗一个序号，第三次握手不消耗序号。
- TCP 建立连接后传输数据，以及四次挥手时，对方所有的确认报文段都不消耗序号。
- 接收端在发送第二个 SYN,ACK 报文后才进入 SYN-RCVD 阶段
- 一般而言，发送的 seq 等于上一个接收到的报文的 ack
- B 结束 TCP 连接的时间比 A 早

5 无线网络 WLAN

5.1 无线局域网的组成

- 接入点 AP：无线局域网的中心，链路层设备。也叫做无线接入点 (WAP)
- 基本服务集 BSS：无线局域网的最小构件，包括一个接入点和若干个移动站
- 服务集标识符 SSID：每个 AP 分配到的不超过 32 字节的名字
- 基本服务集标识 BSSID：接入点 AP 的 MAC 地址
- 扩展服务集 ESS：基本服务集通过接入点 AP 连接到一个**分配系统 DS**，然后再连接到另一个基本服务集。
- 扩展服务集标识符号 ESSID：ESS 的标识符，不超过 32 字符的字符串名字。
- 门户 (portal)：扩展服务集 ESS 可以为无限用户提供到 802.x 局域网的接入。
- 建立关联：一个移动站若要加入一个基本服务集 BSS，需要 ～。表示这个移动站加入了选定的 AP 所属的子网，并和这个接入点 AP 创建了一个虚拟线路。

被动扫描的过程：(似乎不要)

1. AP 周期性发出**信标帧** (SSID、支持的速率等)
2. 移动站扫描信道，选择愿意加入的 AP 所在的 BSS，向 AP 发送**关联请求帧**
3. AP 同意发来的关联请求，发送**关联响应帧**

主动扫描的过程：(似乎不要)

1. 移动站主动发出广播的**探测请求帧**，让所有能够收到此帧的 AP 都能够知道有移动站要求建立关联
2. AP 回答**探测响应帧**
3. 移动站向 AP 发送**关联请求帧**
4. AP 向移动站发送**关联相应帧**

移动自组网络：自组网络是没有固定基础设施（即没有 AP）的无线局域网。这种网络由一些处于平等状态的移动站之间相互通信组成的临时网络。

无线传感器网络 WSN：由大量传感器结点通过无线通信技术构成的自组网络；是移动自组网中的一个子集

5.2 802.11 局域网的 MAC 层协议

5.2.1 CSMA/CA 协议

无线局域网却不能简单地搬用 CSMA/CD 协议的两 (书中：3) 个原因

1. CSMA/CD 协议要求一个站点在发送本站数据的同时，还必须不间断地检测信道，但在无线局域网的设备中要实现这种功能就花费过大。书中说：无线局域网的适配器无法实现碰撞检测。

2. 即使能够实现碰撞检测功能，并且在发送数据时检测到信道是空闲的，在接收端仍然有可能发生碰撞。

3. 即使能够在硬件上实现无线局域网的碰撞检测功能，也无法检测出隐蔽站问题带来的碰撞。

- CSMA/CA(Collision Avoidance)：碰撞避免，协议的设计是要尽量减少碰撞发生的概率
- 隐蔽站问题 (老师没提到)：未能检测出媒体上已存在的信号的问题
- 暴露站问题 (老师没提到)：无线局域网中，只要不发生干扰，可允许多个站同时通信
- 分布协调功能 (DCF，必须实现)：短帧间间隔 (SIFS,28μs)、分布协调功能帧间间隔 (DIFS,128μs)
  各个站通过争用信道来获取发送权，因此 DCF 向上提供争用服务
- 点协调功能 (PCF)：使用集中控制的接入算法把发送数据权轮流交给各个站，以避免碰撞的产生所以自组网络没有 PCF 子层。

5.2.2 时间间隔 DIFS 的重要性

物理层用硬件实现 **1. 载波监听**。

2. 虚拟载波监听：源站将它要占用信道的时间（包括目的站发回确认帧所需的时间）通知给所有其他站，以便使其他所有站在这一段时间都停止发送数据。可以大大减少碰撞的机会。

网络分配向量 NAV：必须经过多少时间才能完成数据帧的这次传输，才能使信道转入到空闲状态。

凡在空闲时间想发送数据的站点，必须等待时间 DIFS 后才能发送，保证了高优先级的 ACK 确认帧 (其他站短暂停留后 (SIFS) 发送) 优先发送

5.2.3 争用信道的过程 (老师：原理仔细看，应该有好几个题目)

征用窗口 CW：由许多时隙 (当下一个时隙开始时，每个站点都能检测出在前一个时隙开始时信道是否忙) 构成。

退避算法：在 $0 \sim$ CW 个时隙中随机生成一个退避时隙数。第 i 次退避就在 2^{2+i} 个时隙中随机选择一个。

检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧，则**不使用退避算法。必须经过争用期公平竞争的情况：**

1. 要发送数据时检测到信道忙

2. 已发出的数据帧未收到确认，重传数据帧

3. 接着发送后续的数据帧 (防止一个站长期垄断发送权)

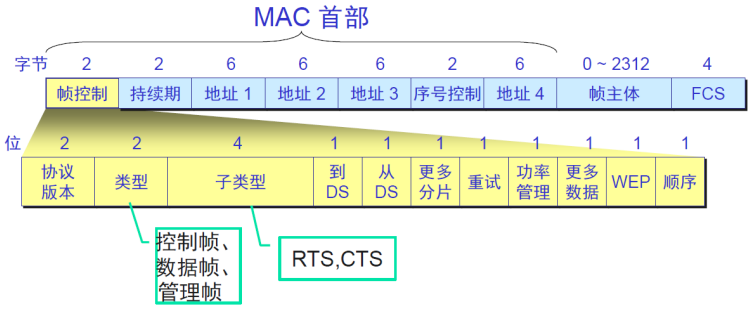
5.2.4 对信道进行预约

请求发送 RTS (Request To Send)：包括源地址、目的地址和这次通信（包括相应的确认帧）所需的持续时间。

允许发送 CTS(Clear To Send)：包括这次通信所需的持续时间（从 RTS 帧中将此持续时间复制到 CTS 帧中）。

5.3 802.11 局域网的 MAC 帧 (老师：只要知道它有三种帧，格式了解一下就行)

802.11 帧共有三种类型，即控制帧、数据帧和管理帧（扫描、认证和连接过程。Beacon 帧）下面是数据帧的主要字段。



5.4 无限个人区域网 WPAN

- WPAN 是把属于个人使用的电子设备用无线技术连接起来的自组网络，不需要使用接入点 AP。
- 网络的范围大约在 10 m 左右
- 无线个人区域网 WPAN 和个人区域网 PAN (Personal Area Network) 并不完全等同
- 最早使用的 WPAN 是蓝牙系统

WPAN 和 WLAN 的区别

- WPAN 是以个人为中心来使用的无线人个区域网，特点是无线连接、低功率、小范围、低速率和低价格。
- 但 WLAN 却是同时为许多用户服务的无线局域网，它是一个大功率、中等范围、高速率的局域网。

5.5 蜂窝移动通信网

把整个网络服务区划分成许多小区 (蜂窝)，每个小区设置一个基站。