**《计算机网络》**

# 概述

**1. 计算机网络的定义**

  计算机网络是一个将分散的、具有独立功能的计算机系统，通过通信设备与线路连接起来，由功能完善的软件实现资源共享和信息传递的系统。

**计算机网络组成**

物理组成：硬件、软件、协议；

工作方式：边缘部分（由主机构成，用户直接进行信息处理和信息共享，低俗联入核心网）和核心部分（由路由器构成，负责为边缘部分提供高速远程分组交换）

功能组成：通信子网（物理层、数据链路层、网络层）和资源子网。

单独一个计算机是不能构成计算机网络的。

英特网草案、建议标准、草案标准、因特网标准。

**2. 计算机网络的功能**

1. 数据通信——计算机网络的最基本的功能，包括连接控制、传输控制、差错控制、流量控制、路由选择、多路复用等
2. 资源共享——计算机网络的主要目的
3. 分布式处理
4. 提高可靠性
5. 负载均衡

注意：计算机网络和分布式系统主要区别不在于它的物理结构，而是在于高层软件上。

**3. 计算机网络的拓扑结构的类型**

1. 星型（优点：网络结构简单，便于控制，建网容易，易于扩展；缺点：中心结点的可靠性问题是网络可靠性的瓶颈）局域网
2. 环型（优点：结构简单，实现容易，数据传输延迟确定；缺点：每两个结点之间的通信线路都是网络可靠性的瓶颈。常用于城域网。）
3. 总线型（优点：结构简单灵活，可扩充，设备投入量少，成本低，安装使用方便；缺点：某个工作站点出现故障时，对整个网络系统影响较大，另外实时性差，当结点通信量增加时，性能会急剧下降）
4. 树型（成本低，易扩充，管理方便，故障隔离容易；根节点依赖性大，发送故障全网不能工作。树型结构适用于相邻层通信较多的情况）
5. 全互联型（优点：无需路由选择，通信方便；缺点：网络连接复杂，仅在结点少。距离很近的环境中使用）
6. 网状拓扑结构（又称无规则型结构，常在结点数较多且地域范围大的环境使用。常用于广域网。优点：可靠性高，易扩充，组网灵活；缺点：费用高，结构复杂，必须采用路由选择算法与流量控制方法）
7. 广播式网络和点对点网络，区分的方式是 是否有路由选择和存储转发，广播式网络要网络层。

**4. OSI/RM及其了解各层的功能**

**物理层**  
  尽可能的屏蔽一些硬件设备和传输媒体的差异，在物理媒体之上为上一层提供一个传输原始比特流的物理连接，确定了与传输媒体的接口的一些特性，机械特性、电气特性、功能特性和规程特性。

**数据链路层**  
  两个相邻结点间的线路上无差错地传送以帧为单位的数据，每一帧包括数据和必要的控制信息。其中介质访问控制层（MAC）、逻辑链路控制层（LLC）属于该层。

|  |
| --- |
| 网络层 |
| LLC |
| MAC |
| 物理层 |

局域网对于LLC子层是透明的

**网络层（主机对主机） 该层支持无连接和面向连接**  
  将传输层传下来的分组，选择合适的路由器，准确无误的发送到目的主机的传输层。

**传输层（进程对进程）该层只支持面向连接**  
  负责向两台主机进程之间提供可靠的端到端通信。

**会话层**  
  两个节点间建立、维护和释放面向用户的连接，并对会话进行管理和控制，保证会话数据可靠传送。

**表示层**  表示层负责数据格式转换，数据的加密和解密，数据的压缩和解压，以实现不同通信系统间的信息交换。

**应用层（用户对用户）**  
  是网络体系中的最高层，直接为用户的应用进程提供服务，如电子邮件，网页浏览等。

**用发送电子邮件的例子讲述**OSI**的工作原理：**

在发电子邮件过程中，首先在应用层编辑的信件，把编辑好的信件发送给表示层，表示层会对信件进行加密，也可以不加密，为了提供传输速度，表示层会将信件进行压缩，然后再传到会话层，会话层就会把信息发给你，并提示你要给别人发信息了，要你准备好，然后再把信息发给传输层，传输层会把信件进行分段，加上报头发给网络层，网络层会对数据段再次进行封装并加入报头形成数据报，选择合适的路径发送给数据链路层，数据链路层会将数据报封装成帧（就是常说的以太网MAC帧），然后把这个信息发送到物理层形成比特流，最后发送到传输媒体（比如网线），这是信件就变成比特流在网线上传输了，此时完成了你的计算机发送过程，你朋友的计算机接受该电子邮件就是此过程反过来。

|  |  |  |
| --- | --- | --- |
|  | **网络层** | **传输层** |
| **OSI** | **无连接和面向连接** | **面向连接** |
| **TCP/IP** | **无连接** | **无连接和面向连接** |

**5. TCP/IP参考模型**

应用层—传输层—网际层—网络接口层

**6. 计算机网络协议、接口和服务的概念**

**网络协议：**是一种规则，是控制两个对等实体进行通信的规则，是水平的。

1. 语义—需要发出何种控制信息，完成何种动作以及做出何种响应；
2. 语法—数据与控制信息的结构或格式；
3. 同步—规定了事件的执行顺序。

本层及本层以下的协议可以不同，但高层协议必须相同。高层协议可以管底层协议，底层协议管不到上层。

**接口：**  
  同一结点网络协议内相邻层之间交换信息的连接点。服务访问点：SAP

**服务：**  
  服务是指下层为相邻上层通过接口提供服务。是垂直的。

N层是N+1层的服务提供者，是N-1层的用户。

**7. 计算机网络的主要性能指标**

**带宽**  
  计算机网络中的带宽指单位时间内网络中的某信道所能通过的“最高数据率”。单位是“比特每秒”。

**吞吐量**  
  表示单位时间内通过某个网络（或信道、接口）的实际数据量或有效数据量。

受瓶颈链路影响，吞吐量应该选最小带宽=min{R1，R2，R3}

**时延**  
（1）发送时延  
  主机发送数据帧所需要的时间。

发送时延=

（2）传播时延  
  电磁波在信道中传播一定距离所需要花费的时间。

传播时延=

**时延带宽积：**链路上可容纳的比特数，即能够发送的数据量

时延带宽积=传播时延×带宽

**往返时延RTT（Round-Trip Time）**  
  在停止等待工作方式下：

有效数据率（吞吐量）=

**信道利用率**

信道利用率=

对于停止等待的情况：

信道利用率=

对于后退N帧的情况：WT+1≦2n

信道利用率=

对于选择重传批量发送的情况：WT+WR≦2n ，WT=WR，WT≦2n-1

信道利用率=

（在发送完第一帧后，后续发送数据时间与第一帧数据传播时间同时进行，一般传播时间大于发送所有数据的时间，则之后的n-1帧发送时间不再考虑）

**必须弄清楚，不要混淆的是：**

1. **对于高速网络链路，我们提高的仅仅是发送速率而不是比特在链路上的传播速率，提高发送速率只是减小了数据的发送延时。**
2. 电磁波在通信线路上的传播速率取决于线路的介质材料，与数据发送速率无关。
3. **提高数据的发送速率只是减少了发送时延。**
4. 发送速率指的是某个点或接口发送速率，而传播速率指某段传输线路上比特的传播速率。
5. 通常所说的“光纤信道的传输速率高”指的是可以用很高的速率向光纤信道发送数据，指的是发送速率，而光纤信道的传播速率实际上还要比铜线传播速率要低。
6. “数据的发送速率越高，其传送总时延就越小”，是错的，因为数据传送的总时间=发送时延+传播时延+处理时延+排队时延，四项组成，不能仅考虑一项。
7. **发送时延与传输信道的长度无关；而传播时延与发送速率无关。信号传送的距离越远，传播时延越大。**
8. **信道利用率不是越大越好，信道或网络利用率过高会产生非常大的时延，利用率接近最大值1时，网络延时趋近于无穷大。**

# 物理层

**1. 物理层特性**

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：电压范围10v～15v
3. 功能特性：某一电平的电压的意义。规定高电压为1，低电压为0
4. 规程特性：指明对于不同功能的各种可能事件的出现顺序。

例1：某网络物理层规定，信号电平用+10V～+15V表示0，-10V～-15V表示1，电线长度限于15米以内，这体现物理层接口的**电气特性**

例2:当描述一个物理层接口引脚出高电平时的含义时，属于功能特性

**2. 奈奎斯特定理和香农定理**

**奈奎斯特定理：**  
  在理想低通信道下的最高码元传输速率Cmax=f采样×log2N=2f×log2N，其中f

 是理想低通信道下的带宽，单位是赫兹（Hz）。

注意：带宽=最高频率-最低频率。

例：一个模拟信道的信号功率为0.62W，噪声功率0.02W，频率范围为3.5MHz～3.9MHz，该信道最高数据传输率为：2Mbit/s

f带宽=3.9-3.5MHz=0.4MHz；在奈奎斯特的C=0.4×2×log2N，N可以无限大，所以在理想状态下(注意题中若是无噪声)传输速率可以无限大；在香农定理：=31，

C=W带宽×log2(1+31)=0.4M×5=2Mbit/s

二者取最小，为2Mbit/s

**香农定理：**

1. 模拟信道极限信息传输速率：

C=Wlog2(1+S/N)bit/s ；W信道带宽

信噪比（S/N）db=10log10(S/N) ，其中 W 为信道的带宽（Hz），S 为信道内所传信号的平均功率，N 为信道内部的高斯噪声功率。

**Log2103=10**

**香农公示表明，信道的带宽或信道中的信噪比越大，信息的极限传输速率就越高。香农公式的意义在于：只要信息传输速率低于信道的极限信息传输速率，就一定穿在某种方法来实现无差错传输。**

注意：当奈奎斯特和香农定理都可以用时，两种都要计算，然后去最小值。

**3. 光纤的优点及其两种模式**

**优点：**  
  光纤具有体积小、重量轻、传输距离远、传输速度高、频带宽、信号衰减小、抗雷电和噪音和电磁干扰性能好，并且具有很好的保密性能。

**两种模式：**

1. LED(发光二极管)—多模光纤—频带较窄，传输特性较差；全反射，适合近距离。包层低折射率，光纤高折射率，折射率越大角度越小，当入射角足够大时，发生全反射
2. ILD(激光)—单模光纤—频带较宽，传输特性好，光在其中沿直线传播，适合距离远。

**双绞线**：

双绞线即可以传输数字信号，也可以传输模拟信号。**传输距离大概100米**

绞合可以减少相邻导线的电磁干扰，双绞线外层用金属丝编织成的屏蔽层可以抗电磁干扰。

双绞线能够传送高速数据的主要措施是把双绞线的绞合度做得非常精确，这样不仅是特性阻抗均匀以减少失真，还大大减少了电磁波辐射和无线电频率的干扰

放大器——放大模拟信号；中继器——整形数字信号。

**同轴电缆**：它比双绞线抗干扰能力强，传输距离更远。

50欧姆同轴电缆用于传送基带数字信号；75欧姆传送宽带信号。**传输距离大概500米。**

**架空明线**(铜线或铁线)：早期大量使用，但通信质量差，受天气气候影响较大，有的已经停止使用，但是我国一些农村和偏远地区仍然使用的是架空明线。

**非导引型传输媒体(微波)**：**两种方式地面微波接力和卫星通信**

微波接力的特点：1.通信信道容量大，传输质量较高；

2.建设投资少，易于跨山区、江河；

微波接力的缺点：1.相邻站必须直视，不能有障碍物；

2.微波传播受恶劣天气影响；

3.与电缆相比，微波通信屏蔽性和保密性较差；

4.维护中继站需要更多的人力物力。

注意：**卫星通信**传播时延较大并不等于卫星信道传送数据的时延较大，卫星通信保密性不好。因为传送数据总时延=传播时延+发送时延+处理时延+排队时延等。

还有**红外通信、激光通信**他们可用于近距离笔记本电脑相互传送数据。

**4. 三种基本的调制方法**

  公有的调制方法名称：一是模拟调制法，二是键控法。

1. 幅移键控法（ASK)：通过改变载波信号振幅来表示数字信号1、0；ASK信号实现容易，技术简单，但容易受增益变化的影响，抗干扰能力差；可用相干检测法进行解调。
2. 频移键控法（FSK）:通过改变载波信号角频率来表示数字信号1、0；FSK实现容易，技术简单，抗干扰能力强，是目前最常用的调制技术；可用相干检测法、鉴频法等进行解调。
3. 相移键控法（PSK）：通过改变载波信号相位值来表示数字信号1、0；PSK有较强的抗干扰能力，且比FSK更有效；解调原理类似于ASK解调。
4. 正交调幅QAM：通过改变相位和振幅。

**5. 曼彻斯特编码和差分曼彻斯特编码**

**曼彻斯特编码：**  
  目前应用最广泛的编码方式之一，其编码规则是每一位的中间有一个跳变，从低到高表示0，从高到低表示1。优点是位中间的跳变既可以作为数据，又可以作为时钟，无需另发同步信号，不含直流分量；缺点是效率较低。1个码元携带2bit，1log2N=2bit

**Baud=2bit/s**

**Baud×log2N=2bit/s(N为脉冲变化数)**

**差分曼彻斯特编码：**  
  是前者的改进。不同在于每比特中间的跳变仅仅作为同步用，每比特的值根据其边界是否发生跳变来决定，0跳变，1不变。抗干扰能力更强，但需要更复杂的设备，且同样有效率低的问题。

**6. 两种数字传输系统（T1，E1）**

  脉冲编码调制（PCM），北美和日本的24路PCM（T1速率1.544Mbit/s）和欧洲的30/32路PCM(E1速率2.048Mbit/s)。我国采用E1标准

**7. PCM的缺点**

  PCM脉码调制数字传输系统缺点：**速率标准不统一；不是同步传输。**

最初在数字传输系统中使用的传输标准是脉冲编码调制PCM。由于PCM的速率标准不统一和不同步传输的缺点，所以现在高速的数字传输系统使用同步光纤网SONET(美国标准)或同步数字系列SDH(国际标准)

# 数据链路层

**1. 数据链路层的功能**

1. 帧同步：接收方确定收到的比特流中一帧的开始位置和结束位置
2. 透明传输：**透明表示某个实际存在的事物看起来却好像不存在一样；表示无论什么样的比特组合，都能按照原样没有差错的通过数据链路层。**
3. 差错控制：CRC差错控制
4. 流量控制：
5. 链路管理：负责数据链路的建立、维持、释放，主要用于面向连接的服务

**2. 常见的组帧的方法**

1. 字符计数法：计数段包含自身所占一个字节
2. 含字节填充的分界符法
3. 含位填充的分界标志法
4. 物理层编码违例法

**3. 循环冗余校验码的原理**

  发送方和接收方预先商定一个除数p，发送方在发送数据前，在帧的数据部分后面追加一个校验和，使得追加之后的帧能够被除数p除尽；接收方用接收到的帧除以除数p，如果余数不为零，则表明传输过程中有错误。2r≧r+k+1(r为校验码位数)

注意：在数据链路层使用CRC校验，能够实现比特差错的传输，但这不是可靠传输，因为它只保证比特不出错，但是不能解决帧丢失、帧重复、帧时序等问题

**4. 多帧滑动窗口与后退N帧协议**

  发送端在传出一个数据帧后，不等待确认信号的到来，就接着发送下一个数据帧。在经过一个往返时间之后，相应数据帧的确认信号（ACK）才到达发送端，这时发送端已经发出了后继的N-1个数据帧。当收到ACK帧后，就继续发送新数据帧，一旦收到否定确认帧（NAK），发送端就要回退N步，重新发送那个出错的数据帧以及后继的N-1个已经发送过的数据帧。

**5. 多路复用技术的一般形式**

1. 频分多路复用（FDM）:当介质可用带宽超过要传信号的带宽。可直接传输模拟信号。
2. 时分多路复用（TDM）:当每路信号需要占据介质的全部有效带宽，且介质可到达的传输速率超过所有要传输数字信号的总数据率时。可传输数字信号。
3. 统计时分复用（STDM):又称为异步时分复用，是动态时间分配
4. 波分多路复用（WDM）:不同波长的光信号
5. 码分多路复用（CDM）：常用。同样的时间使用相同的频率，**挑选不同的码型，用户直接不会造成干扰，**相当于每个人讲不同国家的语言。优点：抗干扰能力强、保密性强、语音质量好，减少成本；主要用于无线通信系统，比如CDMA的手机。负载重时，信道利用率高；缺点：负载低时，信道利用率低，无数据传输时，划分信道有额外的开销。
6. 空分多址(SDM)：是利用空间分割来构成不同信道的技术空分多址是一种信道增容的方式，可以实现频率的重复使用，有利于充分利用频率资源。空分多址还可以与其它多址方式相互兼容，从而实现组合的多址技术。了解即可

补充：CDMA

(1)任意两个不同站的码片正交，即内积=0

例题：某个CDMA站接收到一个碎片序列(-1+1-3+1-1-3+1+1)

A站码片(-1-1-1+1+1-1+1+1)

内积为1表示发送了1bit，为-1表示发送了0bit，为0表示没有发送数据

站点A:（1-1+3+1-1+3+1+1）/8=1，即发送了1bit

1. **CSMA/CD协议**

随机访问介质中，随机接入的有4种：ALOHA协议、CSMA、CSMA/CD、CSMA/CA。

①CSMA（载波侦听多路访问）：半双工通信

1）1-坚持CSMA：一直监听，直到监听到信道空闲时，立即发送数据；

2）p-坚持CSMA：当监听到空闲时，以p概率发送数据，以概率1-p延迟一段时间并重新监听；

3）非坚持CSMA：当监听到信道空闲时立即发送数据，若不空闲，则延迟一段随机的时间再重新监听。

②CSMA/CD（带冲突检测的载波侦听多路访问）：在局域网以太网中广泛使用。**以太网提供无连接，不进行编号，不要求确认，不可靠服务，对有差错帧是否重传由高层决定；冲突现象不可避免,都只是尽可能的避免。太网使用曼彻斯特调制速率Baud=2传输速率**

工作原理：**不管在发送前还是发送中，每个站必须不停检测信道，所以用的是1-坚持CSMA。**每个站在发送数据之前先要检测一下总线上是否有其他计算机在发数据，若有，暂时不发数据，以免发生冲突；若没有，则发送数据。计算机在发送数据过程中同时检测信道上是否有冲突发生，若有，则采用截断二进制指数退避算法来等待一段时间后再次重发。总体来说：“**先听后发，边听边发，冲突停发，随机重发**”

截断二进制指数类型退避算法：

1. 确定推迟时间2t，t表示发送到检测最大的时间，是往返，所以是2г
2. 定义参数k=min{重发次数，10}
3. 从集合г=（0，1，2，3，……2k-1）随机取一个r，则等待时间为2гt
4. 若重传次数达到16次，则认为网络拥挤，抛弃此帧并向高层报告出错。

最小帧长=总线传播时延×数据传输率×2

**以太网规定：凡长度小于64B的帧都是由于冲突而异常中止的无效帧**。

**经过争用期(51.2us)后，若没有检测到碰撞，才肯定不会发生碰撞。**

**注意：争用期又称为冲突窗口。**

以太网每发完一帧，一定要把已发送的帧暂时保留一下，如果在争用期内发生碰撞，那么还要推迟一段时间再把这个暂时保留帧重传一次。

  在以太网中使用随机争用型介质访问控制方法，即带有冲突检测的载波监听多路访问方法。CSMA/CD方法用来解决多结点如何共享公用总线的问题。

1. **局域网的主要特征**
2. 网络范围较小，最大不超过25km（如学校）
3. 传输速率较高，一般为10-100Mbit/s，甚至到10Gbit/s
4. 误码率低，一般为10-8-10-11，最高可达10-12
5. 结构简单，容易实现，便于系统拓展和逐渐演变，设备位置可灵活调节
6. 一般采用方便的分布式传输控制方式，具有**广播功能**
7. **网络为一个单位所拥有，且地理范围和站点数目均有限。**

双绞线是局域网中的主流传输媒体，当数据率很高时，需要使用光纤。

局域网工作的层次跨越了数据链路层和物理层。

### 8. 以太网物理层和MAC层的功能

**以太网物理层**

计算机与外界局域网相连是通过适配器进行的。适配器(计算机)与局域网之间的通信是**串行传输**方式；计算机内部间的通信是**并行传输**的。当适配器收到有差错的帧，直接丢弃而不必通知计算机。注意：计算机的硬件地址在适配器的ROM中，而软件地址—IP地址则在计算机的存储器中。

**以太网MAC层**

IEEE 802.3局域网中规定MAC地址长度由原来的2B(16bit)增加到6B(48bit)，指在局域网上的每一个计算机中固化在适配器的ROM的地址中.地址的第一个字节最低位为I/G位或G/L，I/G为0，表示单个地址，I/G为1，表示组地址，进行多播。G/L为0是全球管理，G/L为1是本地惯例。

**适配器具有过滤功能，适配器从网络上每收到一个MAC帧就先用硬件检查MAC帧的目的地址，如果是本站的地址则收下，否则丢弃该帧。**

**只有目的地址才能使用广播和多播地址。**

以太网的性质：

1. 逻辑上是总线型局域网，物理上是星型局域网
2. 采用无连接的工作方式，不编号，不确认
3. 采用CSMA/CD，是半双工通信（或单工通信）提供的是不可靠的服务，差错的纠正由传输层TCP完成。
4. 使用曼特斯特编码，调制速率=2×传输速率

以太网物理层：

1. 信号的编码与译码
2. 为进行同步用的前同步码的产生和去除
3. 比特的传输与接收

MAC子层：medium access control媒体接入控制子层

1. 负责物理层上的无差错的通信
2. 将上层传递下来的数据封装成帧进行发送，接收时进行拆封
3. 实现和维护MAC协议
4. 比特差错检测
5. 寻址

### 9. 以太网的帧格式

|  | **7** | **1** | **6** | **6** | **2** | **46-1500** | **4** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 802.3MAC | 前导码 | 帧首定界符 SFD | 目的地址DA | 源地址SA | 长度L | 数据区DATA | 帧校验序列 FCS |
| V2 以太网 | 前导码 | 帧首定界符 SFD | 目的地址DA | 源地址SA | 类型TYPE | LLC协议数据单元 LLC-PDU | 帧校验序列 FCS |

  总线网使用的帧结构有两种标准，IEEE802.3和DIX Ethernet V2 以太网标准。

### 在传输媒体上在MAC帧基础上多加8个字节(前同步码7B+帧开始定界符1B)，前同步码的作用是使接收端的适配器在接受MAC帧时能够迅速调整时钟频率，使接收端和发送端时钟同步；帧开始定界符作用是高速接收端适配器“MAC帧马上要来了，请做好准备”，FSC是不检查前同步码和帧开始定界符的。

802.3——以太网

802.11——无线局域网

802.4——令牌总线网

802.5——令牌环网

802.15——无线个人区域网

802.16——宽带无线接入

### 无效帧有：

(1)帧长度不是整数倍，数据长度要是4倍

### (2)MAC帧有效长度不在64B～1500B(数据长度46B～1500B，要减去前和尾部18B)

(3)收到帧检测序列FCS有差错

### 补充：高速以太网

**1.100BASE-T快速以太网：802.3帧格式；可双工和半双工CSMA/CD；星型拓扑结构；光纤和双绞线都可以用**

1. **吉比特以太网1Gbit/s：802.3帧格式；可双工和半双工CSMA/CD；最短帧长仍然是64B，距离还是100m，采用的是载波延伸，MAC帧长不足512B时，使用特殊字符填充在帧后面。吉比特以太网采用分组突发，当很多短帧要发送时，第一个短帧用载波延伸的方法填充，但后面的短帧可以一个接一个的发送，它们之间留最小间隔即可，直到到达1500B字节为止。当吉比特在全双工方式工作时，不适用分组突发和载波延伸。**

**最短帧长=2××数据率**

1. **10吉比特以太网10GE：与10Mbit/s,100Mbit/s,1Gbit/s的帧格式完全相同802.3，且保留了最小帧长和最大帧长；只能全双工；40GE和100GE也是802.3和最小帧长和最大帧长**

|  |  |  |  |
| --- | --- | --- | --- |
|  | 工作方式 | 帧格式 |  |
| 100BASE-T | 可双工  半双工CSMA/CD | 802.3 | 保留了802.3的最小最大帧长 |
| 1GE | 可双工  半双工CSMA/CD | 802.3 | 保留了802.3的最小最大帧长 |
| 10GE 40/100GE | 全双工 | 802.3 | 保留了802.3的最小最大帧长 |

### 10. 广域网的主要特性

1. 广域网运行在超出局域网地理范围的区域内，城市、国家区域；强调资源共享；
2. 使用各种类型的串行连接来接入广泛地理领域内的宽带；
3. 连接分布在广泛地理领域内的设备；
4. 使用电信运营商的服务。

**广域网和局域网的区别与联系**

|  |  |  |
| --- | --- | --- |
|  | 广域网 | 局域网 |
| 覆盖范围 | 很广，跨区域，城市或国家 | 较小，在一个区域内，学校 |
| 连接方式 | 点对点通信 | 广播通信 |
| OSI层次 | 网络层、数据链路层、物理层 | 数据链路层、物理层 |
| 联系 | 1. 两者都是互联网的重要组成构件，从互联网角度上看，二者平等，没有包含关系 2. 连接在广域网或局域网上的主机在该网内进行通信时，只需要使用其网络的物理地址即可 | |
| 着重点 | 强调资源共享 | 强调数据传输 |

**补充：三种数据传输方式：**

1. **电路交换**

优点：1.通信时延小；

1. 实时性强；
2. 有序传输；
3. 适用范围广（传输模拟信号和数字新信号都可）；
4. 控制简单；
5. 避免冲突

缺点：1.需要建立连接，建立连接时间长（面向连接服务）；

1. 信道利用率低（物理通路被通信双方独占，其他人不能用）；
2. 缺乏统一标准；4.灵活性差（建立的通路中任何一个节点故障，必须重新拨号建立新的连接）。

**2.报文交换：**数据交换的单位是报文，一大块的报文传输。报文携带有目的地址、源地址，采用存储转发方式。

优点：1.无需建立连接；

1. 动态分配线路；
2. 提高可靠性（如果一条线路发生故障，可以选择另外一条）；
3. 提高线路利用率；提供多目标服务（一个报文可以同时发送到多个目的地址）。

缺点：1.引起转发时延（数据进入节点入药经历存储转发）；

2.转发大段报文时，需要网络节点有较大的存储缓存空间。

1. **分组交换：**分为数据报方式和虚电路方式

### 11. 数据报服务的特点

**数据报的特点：**

**1）发送分组前无需建立连接；**

**2）不可靠服务，尽最大努力交付；**

**3）不一定按序交付；**

**4）在多个分组报文中，交换机尚未接受完第二个分组，第一个分组就可以转发出去，不仅减小了延时，还提高了吞吐量；**

**5）当某一台交换机或链路故障时，可相应更新转发表，寻找另一条替代路径转发，对故障适应能力强；**

**6）发送方和接收方不独占某一条链路，资源利用利率高。**

**虚电路：建立一条逻辑上的虚连接，传输数据，结束后要拆除虚电路；**

### 12. 虚电路服务与数据报服务的主要区别

|  |  |  |
| --- | --- | --- |
|  | 数据报 | 虚电路 |
| 建立连接 | 不需要（适用出错率高的系统） | 需要 |
| 地址信息 | 每个分组包含完整的源地址和目的地址 | 每个分组包含一个虚电路号 |
| 状态信息 | 路由器不保留任何有关联的状态信息 | 每个虚电路要求路由器为每个连接建立表项 |
| 分组转发 | 每个分组有独立的路径 | 所有分组都沿着指定的同一路径传输 |
| 路由器失效的影响 | 无影响 | 所有经过次失效的路由器虚电路都终止 |
| 端到端的差错处理 | 由主机负责，传输不可靠 | 有通信子网负责，可靠的服务 |
| 端到端流量控制 | 由主机负责 | 有通信子网负责 |
| 分组顺序 | 不一定按序到达 | 按序到达 |
| 思路 | 可靠通信应该由主机来保证 | 可靠通信由网络来保证 |

### 13. PPP(点对点协议)组成

  PPP协议提供了建立、配置、维护和终止点到点的连接的方法，其帧格式是面向字符的。3个部分组成：

1. 将数据报封装的串行链路的方法。既支持异步链路，也支持面向比特的同步链路
2. 链路控制协议（LCP）。用来建立、配置和测试数据链路连接
3. 一套网络控制协议（NCP）。支持不同的网络层协议。

**PPP功能**：

1. 要身份验证（拨号）
2. 连接时协商IP地址
3. 差错检测（只检错不纠错）
4. 支持多种上层协议

**PPP工作过程：**当用户拨号接入ISP，建立一条物理链路，个人计算机向路由器发送LCP分组（封装成多个PPP帧）。接着进行网络配置，NCP会给新接入的计算机分配一个临时的IP地址，这样该计算机就成为因特网中的一个主机了。

当用户通信完毕时，NCP释放网络层连接，收回原来分配出去的IP地址，接着LCP释放数据链路层连接，最后释放物理层连接

**PPP特点：** 1.字节填充

2.只检错不纠错

3.**没有流量控制**（流量控制由TCP负责）

4.PPP是不可靠协议不需要对帧进行编号

5.PPP只支持全双工链路，因为是点对点协议

**PPP透明传输**：采用字节填充; 真正数据(7E)<->PPP(7D5E);

真正数据(7D)<->PPP(7D5D)

### 14. HDLC的帧结构：使用了编号和确认机制

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 比特 | 8 | 8 | 8 | 可变 | 16 | 8 |
|  | 标志F | 地址A | 控制C | 信息Info | 帧校验序列FCS | 标志F |

注：标志序列为独特的8位序列：01111110，如果一个帧的长度小于32位，则认为是无效的。**HDLC帧分类“无U监S息I=无奸细”**

**HDLC采用后退N帧-选择重发-停等**

**HDLC是面向比特同步协议；PPP面向字节**

### 15. 网桥的概念以及类型

网桥是用于连接两个或两个以上具有相同协议、传输介质及寻址结构局域网间的互联设备，能实现网段间或不同局域网之间互联，网桥对收到的帧根据MAC帧目的地址进行转发和过滤。当网桥收到一个帧时，不会向所有接口转发此帧，而是根据帧的目的地址，查找网桥中的地址表，然后确定将该帧转发到哪个接口，或者把它丢弃。

**网桥优点：**

1. 过滤通信量
2. 扩大物理范围
3. 提高可靠性
4. 可互联不同物理层不同MAC子层和不同速率的以太网

**网桥缺点：**

1. 存储转发增加来时延
2. 在MAC子层**没有流量控制**功能
3. 不同MAC子层的网桥桥接在一起时时延更大
4. 网桥只适合用户数不多和通信量不大的局域网，否则会因广播过多产生网络用塞，形成广播风暴。

**网桥分类**

  1.**透明网桥（选择的不是最佳路由）：**指局域网上的站点并不知道所发送的帧经过哪几个网桥，因为网桥对各站来说是看不见的。透明网桥是即插即用设备，连接到局域网上后需要用**生成树算法spanning tree** 来建立转发表，生成树网桥的优点易于安装，无须人工输入路由信息，但没有最佳利用带宽，消除了兜圈子现象和广播风暴。

  2.**源路由网桥（选择的是最佳路由，路由选择由源站负责）：**源站先以广播方式向欲通信目的站发送一个发送帧。发送帧将在整个局域网中沿着所有可能的路由传送，并记录所经过的路由。当发送帧到达目的站时，就沿原来的路径返回源站，源站在得知这些路由后，在从所有可能的路由中**选择一个最佳路由**。路由信息由网桥地址和LAN标识符的序列组成，包含在帧头中。发送帧除了可以用来确定最佳路由，还可以用来确定整个网络可以通过的帧的最大长度。

注意：透明网桥和源选径网桥提高的最佳路由不一定是经过的路由器最少，也可以是发送帧往返时间最短的路由，这样才能真正的负载平衡。

**以太网交换机：**

总线以太网使用CSMA/CD协议，是半双工方式，有碰撞问题。而以太网交换机采用星形结构，没有碰撞问题，因此不使用CSMA/CD，是全双工方式工作。既然不使用CSMA/CD了，为什么还叫以太网呢？**因为它的帧结构没有变，仍然采用以太网的帧结构。**

**为了解决以太网交换机自学习是兜圈子问题，IEEE802.1D标准制定了一个生成树协议STP，其要点就是不改变网络的实际拓扑，在逻辑上切断某些链路，从而消除了兜圈子现象。**

**网桥和以太网交换机区别**：

1. 以太网交换机实质上是多端口网桥，通常有十几个端口；而网桥一般只有两个端口；
2. 网桥端口一般连到局域网的网段，而以太网交换机的每个端口一般都直接与主机或集线器相连。
3. 交换机允许多对计算机同时通信，而网桥最多允许每个网段上的一对就按季同时通信
4. 网桥采用存储转发方式转发，而以太网交换机还可以采用直通方式转发，以太网转发速度比网桥快。

### 16. 以太网的工作原理和信道的利用率

**以太网的工作原理**

1. 逻辑上是总线型局域网，物理上是星型局域网，信息以**广播方式**发送

2.采用无连接的工作方式，不编号，不确认

3.采用CSMA/CD，是**半双工通信**（或单工通信）提供的是**不可靠的服务**，差错的纠正由传输层TCP完成。

4.使用曼特斯特编码

**信道利用率**  
  信道的效率，也称信道利用率。信道利用率是对发送方而言的，是指发送方在一个发送周期的时间内，有效的发送数据所需要的时间占整个发送周期的比率。发送方从开始发送数据到收到第一个确认帧位置，称为一个发送周期，所以信道利用率取决于帧的长度。  
  信道利用率=

### 17. 纯ALOHA和时隙ALOHA的结论

**纯ALOHA协议**  
  当网络中的任何一个站点需要发送数据时，可以不进行任何检测就发送数据。如果在一段时间内未收到确认，那么该站点就认为传输过程中发生了冲突。发送站点需要等待一段随机时间后再发送数据，直至发送成功。

**时隙ALOHA协议**  
  把所有各站点在时间上同步起来，并将时间划分为一段段等长的时隙，规定只能在每个时隙开始是才能发送一帧。从而避免了用户发送数据的任意性，减少了数据产生冲突的可能性，提高了信道利用率。在一个时隙内有两个或两个以上的帧到达时，在下一个时隙将产生碰撞。

### 18. CSMA/CD的原理和吞吐量的计算

**CSMA/CD协议**  
  载波侦听多路访问/碰撞检测（Carrier Sense Multiple Access with Collision Detection，CSMA/CD）

  工作流程：先听后发，边听边发（区别于CSMA协议），冲突停发，随机重发  
  如果在传输过程中，适配器检测到来自其他适配器的信号能量，就必须停止传输他的帧，取而代之传输一个48比特的拥塞信号。

  CSMA/CD中的站不可能同时进行发送和接收，因此采用CSMA/CD协议的以太网不可能进行全双工通信，只能进行半双工通信。

  以太网端到端往返时间 2τ 称为争用期（又称冲突窗口或碰撞窗口）。只有经过争用期这段时间还未监测到冲突时，才能确定这次发送不会发生冲突。所以CSMA/CD总线网中的所有数据帧都必须要大于一个最小帧长。所有站点收到帧长小于最小帧长的帧时，就把它当作无效帧立即丢弃。

最小帧长=总线传播时延×数据传输率×2

  以太网规定最短帧长为64B。如果发送数据小于64B，则需在数据字段后加入整数字节的填充字段以保证以太网的MAC帧长度不小于64B。  
  因此，对于10Mbps的以太网，其争用期为512微秒，帧间间隔为9.6微秒；对于100Mbps的以太网，争用期为51.2微秒，帧间间隔为0.96微秒。

  CSMA/CD采用二进制指数退避算法来解决碰撞问题，定义=[重传次数，10]k=min[重传次数，10]，从[0,1,…,2k-1]中随机选取一个 r,重传退避时间就是 2rτ 。**当重传16次仍不能成功时，说明网络太拥挤，认为此帧永远无法正确发出，抛弃此帧并向高层报告出错。（网络层路由TTL也是使用的16作为生存时间）**

  采用二进制指数退避算法可使重传需要推迟的平均时间随重传次数的增大而增大（这也称动态退避），因而能降低发生碰撞的概率，有利于整个系统的稳定。

**吞吐量**

信道吞吐量=信道利用率×发送方的发送速率

例：一个TCP连接使用256kb/s的链路，端到端时延为128ms，吞吐率为120kb/s，问窗口是多少？（忽略确认帧的发送时延）

解：设窗口为N(单位B)

==128×103

解得N=7228B

例2:设TCP使用最大窗口为65535B=64KB，带宽为1Gb/s，若报文段平均往返时间为20ms，则最大吞吐量是多少？

解：因为带宽不受限制，所以发送时延=0.52428ms。平均往返时间20ms，则每秒可发送1/（20.502428×10-3）次=48.723次，最大吞吐量=48.72364KB=25.5Mb/s

**19. VLAN的概念**

  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，而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，指明发送这个帧的计算机属于哪一个VLAN。

一台计算机可以属于多个VLAN，即它可以访问多个VLAN，也可以被多个VLAN访问。

**VLAN的以太网帧格式802.1Q**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6 | 6 | 4 | 2 | 46～1500 | 4 |
| 目的地址 | 源地址 | VLAN标记 | 类型 | 数据 | FCS |

由于VLAN的以太网帧的首部增加了4B，所以最大帧长由原来的1518B（1500B的数据加上18字节的首部）变成了1522B。  
  用以太网交换机划分虚拟局域网，以太网交换机不向虚拟局域网以外的计算机传该虚拟局域网的送广播信息。这样，虚拟局域网限制了接收广播信息的计算机数，使得网络不会因传播过多的广播信息（即所谓的“广播风暴”）而引起性能恶化。因此一个VLAN是一个广播域。  
  当要进行VLAN之间的通信时，需要使用三层设备（或是中继端口），即三层交换机或路由器。

两个虚拟局域网之间的通信必须在第三层(网络层)路由才能实现。因为不同局域网（相当于不同的网段）是不能相互通信了，要通信首先要知道对方的IP地址已经MAC地址，要知道MAC地址要广播一个ARP，同一个广播信号不能在不同的局域网中传播，所以局域网能够抑制“广播风暴”，在只有通过路由选择（第三层）才能进行通信。

### 20. 划分VLAN的方法virtual local area network

  VLAN是Virtual LAN（虚拟局域网）的简写。5种划分：

1. 按交换端口号;属于静态分配
2. 按MAC地址
3. 按第三层协议
4. 使用IP组播
5. 基于策略（实现VLAN最有利）

# 网络层

### 1. 网络的异构性表现在哪些方面

1. 不同类型的网络（广域网、城域网和局域网）
2. 使用不同类型通信协议的网络（Ethernet、Token Ring、ATM等）
3. 不同类型的计算机系统（大型机、小型机、工作站和微型机）
4. 使用不同类型操作系统的计算机（Windows、UNIX、OS/2和Linux等）

### 2. 中继系统的种类

1. 物理层中继系统，即中继器、集线器、转发器

中继器——放大数字信号；放大器放大模拟信号，中继器只能简单再生信号。二层交换机只能对信号进行修复，不是再生

1. 数据链路层中继系统，即网桥或桥接器或交换机
2. 网络层中继系统，即路由器
3. 网桥和路由器的混合物，即桥路器
4. 任何比网络层高的层次上的中继系统，即网关

**用转发器和网桥连接的若干个局域网仍然是一个网络，他们的网络号是相同的**。

### 3. 拥塞控制算法

1. 通信量整形：漏桶算法，令牌桶算法
2. 分组丢弃算法
3. 缓冲区分配算法
4. 定额控制算法

### 4. 距离向量路由算法RIP(只掌握邻居的情况，不知道全网的拓扑结构)

**RIP特点：**

1. **只和相邻路由交换信息，不相邻的路由不交换信息。**
2. **路由器交换的信息时本路由所有的信息**
3. **按固定时间间隔交换信息，如每30s交换一次路由表；**若3分钟还没有收到相邻路由器的更新路由表，则把此相邻路由表记为不可达路由器，即把距离设置为16（16表示不可达）
4. RIP2支持变长子网掩码和CIDR和多播。
5. **路由表中有：网络地址、子网掩码、下一跳地址、距离**

优点：**实现简单、开销小，收敛快**

缺点：1.限制来网络的规模，最大距离为15，16表示不可达；

2.当网络出现故障时，“坏消息传得慢”

  在该算法中，每个路由器维持一张子网中每一个以其他路由器为索引的路由选择表，表中的每一个入口都对应于子网中的一个路由器。此入口包括两个部分，即希望使用的到达目的地输出线路和估计到达目的地所需的时间或距离。所用量度标准可为站点估计的时间延迟、该路由排队的分组估计总数或类似的值

### 5. 链路状态路由算法OSPF最短路径算法(掌握整个网络，知道整个网络的拓扑结构)广播；变化才更新；没有坏消息传得慢问题。40s没有收到邻居的消息，就认为那个邻居不在了。每40min更新数据库链路状态。

**使用Dijkstra算法**

**OSPF open shortest path first协议三要点：**

1. **向本自治系统中所有路由器发送信息，这里使用的是洪泛法**；
2. **发送的信息是与本路由器相邻的所有路由的链路状态**
3. **只有当链路状态发生变化时，路由器才使用可靠的洪泛法向所有路由器发送信息**。
4. **多路径间的负载平衡；如果到达同一个目的网络的多条相同代价，可以将通信量分配给这几条路径。而RIP只能找出到某个网络的一条路径。**
5. 所有OSPF路由器之间交换的分组都具**有鉴别功能**，保证仅在可信赖的路由器之间交换链路状态信息。
6. OSPF支持可变长度的子网划分和无分类编址CIDR
7. OSPF让每个链路状态都带上**32位的序号，序号越大状态越新**。

**OSPF的五种分类**

1. 问候hello分组，用来发现和维持邻站的可达性。
2. 数据库描述分组，向邻站给出自己的链路状态数据库中的所有链路状态项目的摘要信息，
3. 链路状态请求分组LSQ，向对方请求某些链路状态项目的详细信息。
4. 链路状态更新分组LSU：用洪泛法对全网更新链路状态，用该分组将链路状态通知给邻站。
5. 链路状态确认分组LSA：对链路更新分组的确认

通常每隔10s，每两个相邻路由器要交换一次问候分组，以便知道哪些站可达，如果在40s内没有收到邻居发来的分组，路由器就认为哪个邻居不存在了。还规定每隔30min，要刷新一次数据库中的链路状态

  先通过各个结点之间的路由信息交换，每个结点可获得关于整个网络的拓扑信息，得知网络中所有结点之间的链路连接和各条链路的代价（延迟、开销等）；然后将这些拓扑信息抽象成一张带权无向图；最后利用最短路径路由算法计算出到各个目的结点的最短路径。

**边界网关协议BGP-border Gateway protocal**：外部，不同自制系统AS间的；交换整个路由表；变化才更新；是应用层协议，借助TCP传送；BGP4支持CIDR技术，因此BGP的路由表也包括网络前缀、下一跳和目的网络。

|  |  |  |  |
| --- | --- | --- | --- |
| 主要特点 | **RIP** | **OSPF** | **BGP** |
| 网关协议 | 内部 | 内部 | 外部 |
| 路由表内容 | 目的网络，下一跳，距离 | 目的网络，下一跳，距离 | 目的网络，完整路径 |
| 最优通路依据 | 跳数 | 费用、代价 | 多种有关策略 |
| 算法 | 距离-向量协议 | 链路状态路由 | 路径-向量协议 |
| 和谁交换信息 | 只和相邻路由器交换信息  局部性 | 向所有路由器发送信息  全局性 |  |
| 交换信息的内容 | 交换的信息是自己的路由表 | 发送的信息是本路由器相邻的所有链路状态 |  |
| 发送信息的周期 | 定期更新 30s | 变化才更新 | 变化才更新 |
| 传送方式 | (RU)传输层UDP | (OI)IP数据报 | (BT)建立TCP连接 |
| 是否支持CIDR | RIP2支持变长子网掩码和CIDR和多播 | 支持变长子网掩码和CIDR | BGP4支持 |
| 特点 | 简单、效率低、跳数为16不可达，好消息传得快，坏消息传的慢 | 效率高、路由器频繁交换信息，难维持一致性；规模大 |  |

### 6. IP地址的分类及其表示

**IP地址：**  
  网络号+主机号

A类网络地址：

**0**0000001.0.0.0～01111110.0.0.0

1.0.0.0～126.0.0.0

B类网络地址：

**10**000000.00000001.0.0～**10**111111.11111111.0.0

128.1.0.0～191.255.0.0

C类网络地址：

**110**00000.00000000.00000001.0~**110**11111.11111111.11111111.0

192.0.1.0~223.255.255.0

**IP地址有一下重要特点：**

1. **IP地址分等级的地址结构的好处：1，IP地址管理机构分配IP时只分配网络号，剩下的主机号自行分配，这样方便了IP地址的管理；2，路由器仅根据目的主机的网络号来转发分组，这样就大大减少来路由表中的项目数量，从而减少路由表所占的内存以及查找路由表时间。**
2. **用网桥或转发器连接若干个局域网仍为一个网络，因为这些局域网都具有相同的网络号。具有不同网络号的局域网必须使用路由器进行互联。**
3. 路由器总是有两个或两个以上的IP地址。路由器每个接口都有不同网络号的IP地址。
4. **IP地址的源地址和目的地址不会变，但MAC地址的源地址和目的地址会变**

**IP地址的分类：**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **类别** | **起始编码** | **范围** |
| A类地址 | 0 | 网络号7位；主机号24位 | 1.0.0.0～127.255.255.255 |
| B类地址 | 10 | 网络号14位，主机号16位 | 128.0.0.0～191.255.255.255 |
| C类地址 | 110 | 网络号21位；主机号8位 | 192.0.0.0～223.255.255.255 |
| D类地址 | 1110 | 多播地址28位 | 224.0.0.0～239.255.255.255 |
| E类地址 | 11110 | 保留用于试验和将来使用 | 240.0.0.0～247.255.255.255 |

**6种特殊地址**

**1.直接广播地址：主机号全为0，只能做目的地址**

**2.受限广播地址：255.255.255.255作为目的地址，仅局限于本地局域网，属于E类地址。**

**3.这个网络上的主机0.0.0.0：只做源地址，不做目的地址，并且使用255.255.255.255为目的地址**

**4.环回地址127:用来测试**

### 7. IP数据报的结构及其每个域的意义

### 0 4 8 16 19 24 31

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **版本** | **首部长度** | **区分服务** | **总长度** | | | |
| **标识** | | |  | **D**  **F** | **M**  **F** | **片偏移** |
| **生存时间** | | **协议** | **首部校验和** | | | |
| **源IP地址** | | | | | | |
| **目的IP地址** | | | | | | |

1. 版本：占4位；IP的版本，目前广泛使用的版本号为4。
2. 首部长度：占4位；**4B的倍数，因为首部长度为4的倍数，所有数据部分的长度也是4的倍数**。以32位为单位，最大值为60B（15X4B）。最常用的首部长度是20B，此时不使用任何选项（即可选字段）。
3. 总长度：16位；指首部和数据之和的长度，单位为字节，因此数据报的最大长度为216−1=65535B。
4. 标识：16位；它是一个计数器，每产生一个数据报就加1，并赋值给标识字段。并不是“序号”，因为IP是无连接服务。
5. 标志：3位；只有后两位有意义，标志字段的最低位为MF，MF=1表示后面还有分片，MF=0表示最后一个分片。标志字段中间的一位是DF，只有当DF=0时才允许分片。
6. 片偏移：13位；他指出较长的分组在分片后，某片在原分组中的相对位置。8个字节为偏移单位，即每个分片的长度一定是**8B（64位）的整数倍**。
7. 首部校验和：16位；IP数据报的首部校验和只校验分组的首部，而不校验数据部分。
8. 生存时间（TTL）：8位；数据报在网络中可通过路由器数的最大值。路由器在分组转发前，先把TTL减1。若TTL被减为0，则该分组必须丢弃。
9. 协议：8位；指出此分组携带的数据使用何种协议。如**6代表TCP，17代表UDP。**

**常用协议及相应的协议字段**

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

1. 源地址字段：32位；标识发送方的IP地址。
2. 目的地址字段：32位；标识接收方的IP地址。

**补充ARP：**

1. ARP是解决**同一局域网上**的IP地址与硬件地址映射的问题。全世界存在各种各样的网络，**他们使用不同的硬件地址**，要使这些异构网络能够通信必须**进行非常复杂的硬件地址转换工作**，而IP编址把这个复杂问题解决了。

ARP木马原理：利用ARP协议漏洞，把虚假的网关MAC地址发给受害主机，造成局域网大量的ARP信息从而造成网络拥塞。没有破坏网络的连通性。

1. ARP帧结构

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6B | 6B | 2 | 2 | 2 | 1 | 1 | 2 | 6 | 4 | 6 | 4 |
| 以太网目的地址 | 以太网源地址 | 帧类型 | 硬件类型 | 协议类型 | MAC地址长度 | IP地址长度 | 操作类型 | 源MAC地址 | 源IP地址 | 目的MAC地址 | 目的IP地址 |
| 以太网首部 | | | ARP首部 | | | | |  |  |  |  |

### 8. 子网及其掩码

**划分子网的方法：**  
 可以用以下记法来表示：IP地址={<网络号>，<子网号>，<主机号>}

划分子网是从网络的主机号借用若干位作为子网号。

当没有划分子网时，IP地址是两级结构。划分子网后IP地址变成了三级结构；**划分子网只是把IP地址的主机号这部分进行在划分，而不改变IP地址原来的网络号**。

**子网掩码：**  
  子网掩码也是32位，由一串1和0组成，1表示在IP地址中网络号和子网号对应比特，而0表示在IP地址中主机号的对应比特。子网地址=子网掩码+IP地址。A类地址的默认子网掩码是255.0.0.0，B类地址的默认子网掩码是255.255.0.0，C类地址的默认子网掩码是255.255.255.0

子网掩码&子网中的主机IP=子网网络地址；

所有的网络必须使用子网掩码，如果不划分子网，子网掩码使用默认子网掩码。

**划分子网后，路由表必须包含三个内容：目的网络、子网掩码、和下一跳地址；**

**划分子网增加了灵活性，但减少了能够连在网络上的主机总数；**

**CIDR全0和全1的子网号可以使用。**

### 9. CIDR

**CIDR主要特点：**

1. **CIDR消除了传统ABC类地址和子网划分的概念，因而更有效的分配地址空间。**
2. **CIDR把网络前缀都相同的连续的IP地址组成一个“CIDR地址块”，我们只要知道CIDR任何一个地址，就能知道在这个地址块的起始地止和最大地址了**

 CIDR使IP地址从三级编址回到了两级编址。IP地址={<网络前缀>，<主机号>}。

网络前缀不是8倍时，需要进行简单的计算才能得到一些地址信息。

CIDR好处：更加有效的分配IPv4的地址空间。

**路由聚合是将网络前缀缩短，网络前缀越短，其地址块包含的主机地址越多；**

**划分子网是使网络前缀变长。**

**CIDR技术的作用**：把小的网络汇聚成大的超网；将有类别寻址方式替换成更灵活、浪费更少的无类别方案。

**路由聚合的优点**：减少路由器之间的路由选择信息的交换，提供整个互联网的性能。

**划分子网的好处**：减少广播域。划分子网就是把一个大网络分成很多小网络，因为路由器可以隔离广播域，所以就减少了广播域。

**CIDR用二叉线索查找路由表，为了提高二叉线索的查找速度，广泛使用了压缩技术。**

### 10. ICMP差错报告报文的种类 。用ICMP用IP协议封装

  目的站不可到达：无法交付

源站抑制：拥塞丢数据

时间超过：超时，TTL减为0时

参数问题：首部字段有问题

改变路由：重定向

补充：不应发送ICMP差错报文的几种情况：

1. 对ICMP的差错报文不再发送ICMP差错报文
2. 对第一个分片的数据报的所有后续数据报片，都不发送
3. 对具有多播地址的数据报，不发送
4. 对具有特殊地址如127.0.0.0或0.0.0.0数据报，不发送；

**ICMP应用**

1ping使用了ICMP回送请求和回送报答报文，ping是应用层直接使用网络层的例子，它没有通过传输层的TCP或UDP。

2tracer，跟踪一个分组从源点到终点的路径。

ping命令只能测试本机能否跟外部指定主机连接，无法判断故障发生在校园网内还是校园网外。  
tracert (rt是router的简写，该命令意为跟踪路由)命令用于跟踪路由，以查看IP数据包所走路径的连通情况，能查出路径上哪段路由出现了连通故障。  
netstat命令一般用来查看本机各端口的连接情况，如开启了哪个端口、开启的端口是哪个IP主机连接使用的、连接使用何种协议，以确定是否有黑客非法开启端口进行非法活动，其格式为netstat-x，其中x为参数，常用参数是a，显示所有信息。  
arp命令可以查看和修改本地主机上的arp表项，常用于查看arp缓存及解决IP地址解释故障

### 11. OSPF

特点

1.向本自治系统**所有路由器**发送信息，使用的是洪泛法；

2.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；

3.只有当链路发生变化时，路由器才发送用洪泛法发送信息。

4.比RIP相比，OSPF的更新过程收敛的更快

  OSPF(开放最短路径优先协议)支持三种类型的连接和网络：

1. 路由器间的点-点线路
2. 由广播的多路访问网络（大多数LAN）
3. 没有广播的多路访问网络（大多数的分组交换的WAN）

  OSPFv6也是一种内部网关协议（IGP），它是一种基于层次概念的协议。该协议的报头标识字段值为89。

### 12. IP多播的概念和多播地址

  多播是IPv6数据包的3种基本目的地址类型之一，多播是一点对多点的通信。  
  多播地址：D类地址空间是专为IP多播组地址而定义的。每个多播组地址都落在从224.0.0.0-239.255.255.255的空间范围内。

注意：1.组播地址只能用于目的地址，不能用于源地址；相当于主动加入视频会议输入的地址

2.尽最大努力交付，UDP，不可靠传输；

3.组播数据报不产生ICMP差错报文，所有ping多播地址，不会收到响应

4.并非所有的D类地址都是组播地址224.0.0.0-239.255.255.255

当一个主机加入一个多播组时，主机IP地址不用必须修改。因为当主机加入新的多播组时，该主机向多播组地址发送一个IGMP报文，声明自己要加入该组播，一个主机可加入多个组播。

**IGMP internet group management protocol网际组管理协议**

1. **IGMP不知道IP多播的主机有多少个，IGMP协议只知道是否有主机参加或退出了多播组。**
2. **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。**

### 13. 转交地址的分类

**不同址转交地址**：普通的转交地址，

**同址转交地址**：移动站本身可以是外地代理，这样做移动站必须接受发送到转交地址的数据报，好处是移动站可以移动到任何网络，而不必担心外地代理不可用。缺点是移动站需要额外的软件使自己能够有这个功能

1. 外地代理转交地址（被动）：当移动节点进入外部网络时，外部代理会广播一个地址报文，这个报文里包含这个转交地址，移动节点收到后就知道了转交地址。
2. 配置转交地址（主动）：移动节点主动发送一个广播报文来获得转交地址

**移动IP的通信过程**

1. 移动节点在本地网络时，按传统的TCP/IP方式通信；
2. 移动节点漫游到一个外地网络时，仍然使用固定的IP地址进行通信。为了能够收到对方发给它的IP分组，移动节点需要向本地代理注册一个当地的位置地址，这个位置地址就是转交地址。移动IP的转交地址可以是外部代理的地址或动态配置的一个地址。
3. 移动节点通过外部代理发送注册报文给本地代理，这个注册报文包含移动节点的固定地址和转交地址。
4. 本地代理接受来自转交地址的注册后，会发送注册响应报文。并构建一条通向转交地址的隧道，将截获的发给移动节点的IP分组通过隧道送到转交地址处。
5. 在转交地址处解除隧道封装，恢复原始IP分组，最后送到移动节点。
6. 移动节点在外网通过外网的路由器或外部代理向对方发送IP数据报。
7. 当移动节点来到另一个网络时，只需向本地代理更新注册转交地址，就可以继续通信
8. 当移动节点回到本地网络时，移动节点向本地代理注销转交地址，这时移动节点又将使用传统的TCP/IP方式通信。

### 14. 路由器的优缺点

  优点：

1. 更适用于连接大规模的异种网络
2. 可实现复杂的网络拓扑结构，负载共享和有更强的最优路径选择能力
3. 能更好地处理多媒体
4. 有利于提高网络的安全性和保密性
5. 可隔离不需要的通信量
6. 有较好的拥塞控制能力
7. 减少主机负担

|  |  |  |  |
| --- | --- | --- | --- |
|  | 隔离冲突域 | 隔离广播域 | 设备所在层 |
| 中继器、集线器 | × | × | 物理层 |
| 网桥、交换机 | √ | × | 数据链路层 |
| 路由器 | √ | √ | 网络层 |

**缺点：**

1. 不支持非路由协议
2. 安装复杂
3. 价格高

**路由器的结构：路由选择和分组转发**

注意：路由选择和转发是有区别的。

转发：只涉及一个路由，转发表必须包含到目的网络的输出端口和下一跳的MAC地址。转发表用硬件实现的。

路由选择是有多个路由器协同工作的结果。路由表一般仅包含目的网络到下一跳（用IP地址表示），路由表总是用软件实现的。

**但是在讨论路由选择原理的时候，往往不去区分转发表和路由表的区别，而可以笼统的都是使用路由表这一词。**

**14. VPN虚拟专用网和NAT网络地址转换**

专用地址(私有地址)

1.10.0.0.0~10.255.255.255(10.0.0.0/8)

2.172.16.0.0~172.31.255.255(172.16.0.0/12)

3.192.168.0.0~192.168.255.255(192.168.0.0/16)

机构内部计算机通信也是采用TCP/IP协议；

**在互联网中的所有路由器，对目的地址是专用地址的数据报一律不转发。**

**专用的IP地址可以重复，即私有地址可以重复。**

VPN(virtual private network)虚拟专用网：利用公用的互联网作为本机构各专用网之间的通信载体

NAT(network address translation)网络地址转换

# 传输层（为应用进程提供端到端通信）

补充：传输层功能

1.**提供应用进程间端到端的逻辑通信（网络层提供主机间的逻辑通信）**

1. 差错检测
2. 提供无连接或面向连接的服务：面向连接的TCP可靠传输；无连接UDP不可靠传输
3. 分用和复用：分用：从网络层向上交付给不同的应用进程；复用：传输层向下交付给网络层；
4. 对于面向连接的服务还有两个功能：连接管理和流量控制和拥塞控制

### 1. 传输层寻址与端口

  数据链路层按MAC地址寻址，网络层按IP地址来寻址的，而传输层是按端口号来寻址的。  
  端口就是传输层服务访问点。不同的应用进程的报文可以通过不同的端口向下交付给传输层，再往下由传输层统一处理交给网络层，这一过程称为复用。相反，传输层从网络层收到数据统一处理后再根据不同的端口号向上交付给不同的应用进程，这一过程称为分用。从这个意义上讲，端口就是用来标志应用层的进程。  
  端口用一个16 bit 端口号进行标志，共允许有64k个端口号。**端口号只具有本地意义**，即端口号只是为了标志本计算机应用层中的各进程。根据端口号范围可将端口分为三类：

1. 熟知端口(系统端口号)， 0~1023
2. 登记端口必须在IANA登记，1024～49151
3. 客户端端口(短暂端口号)，49152～65535

**常用熟知端口号**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 应用程序 | FTP | TELNET | SMTP | DNS | TFTP | HTTP | SNMP | SNMPtrp | HTTPS |
| 端口号 | 21 | 23 | 25 | 53 | 69 | 80 | 161 | 162 | 443 |

套接字=（主机IP地址：端口号），套接字唯一标识了网络中某台主机上的某个应用进程

### 2. 无连接服务与面向连接服务

**面向连接服务：**  
  基于电话系统模型，用户首先要建立一个连接，然后使用该链接，最后释放链接。

采用TCP时，采用的是全双工可靠的逻辑信道。

**TCP主要特点：**

1. 面向连接，不提供多播或广播服务；
2. 可靠交付，有确认机制；
3. 报文段头部长，传输开销大，有20个字节。
4. 面向字节流

**TCP和IP的比较**

|  |  |
| --- | --- |
| TCP | IP |
| 面向连接 | 无连接 |
| 字节流接口 | IP数据报接口 |
| 有流量控制 | 无流量控制 |
| 有拥塞控制 | 无拥塞控制 |
| 可靠传输 | 不可靠传输 |
| 无丢失 | 可能丢失 |
| 无重复 | 可能重复 |
| 按序交付 | 可能失序 |

**无连接服务：**  
  基于邮政系统模型，每一条报文都携带了完整的目标地址，所以每条报文都可以被系统独立地路由。

**UDP主要特点：**

1. 无连接，数据到达无需确认，支持一对一，一对多，多对一，多对多通信；
2. 首部8字节；TCP首部20字节
3. 不可靠交付；
4. 报文头部短，传输开销小，只有8个字节，时延较短，传输速率比TCP高。
5. 无拥塞控制。适用于实时应用如IP电话、实时视频会议
6. 面向报文

注意：UDP的伪首部仅仅只校验才用得到，不上交也下传。UDP的检验和是把首部和数据部分一起校验，而IP数据报首部校验只校验首部（因为UDP校验已经把数据部分校验了，所以向下传的时候就不再重复校验数据部分了）。UDP数据报指示IP数据报中的数据部分，对路由器是不可见的。

**TCP主要特点：**

1. TCP是面向连接的传输层协议；
2. 每一条TCP连接只能有两个端点；
3. 提供全双工通信，提供可靠传输；
4. 面向字节流.

|  |  |
| --- | --- |
| 应用层协议 | 传输层协议 |
| DNS域名系统 | UDP |
| TFTP简单文件传送协议 | UDP |
| RIP路由信息协议 | UDP |
| DHCP动态配置IP | UDP |
| SNMP简单网络管理协议 | UDP |
| NFS网络文件系统 | UDP |
| IGMP管理多播的 | UDP |
| RTP实时传送协议 | UDP |
| RTCP实时运输控制协议 | UDP |
|  |  |
|  |  |
| SMTP邮件协议 | TCP |
| TELNET远程终端协议 | TCP |
| HTTP | TCP |
| FTP | TCP |

### 3. 传输连接的建立与释放

  建立连接是个复杂的问题，实际上网络上可能会发生丢失、存储和重复分组的情况。  
  释放链接较前者稍简单一点。终止连接有两种方式，即非对称释放和对称释放，非对称释放很突然，可能会丢失数据。更好的一个方法可采用4次握手方法。

### 4. UDP的优点

  用户数据报协议（UDP），无连接协议。  
**UDP优点：**

1. 发送数据之前不需要建立连接，发送数据完后不需要释放连接，因此减少了开销和发送数据之前的时延；
2. UDP不使用拥塞控制，不保证可靠交付，因此主机不需要维持具有许多参数的复杂的连接状态表；
3. UDP用户数据报只有8字节的首部开销，比TCP的20字节的首部要短；
4. 由于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和TCP报文段报头格式

**UDP报文：8B**  
2B 2B 2B 2B

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 源端口 | 目的端口 | 长度：首部+数据部分 | 校验和 | 数据部分 |

伪首部：12B

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 源IP地址 | 目的IP地址 | 0 | 17 | UDP长度 |

**TCP首部：**

**0 16bit 31**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **源端口2B** | | | | | | | | **目的端口2B** |
| **序号4B** | | | | | | | | |
| **确认号4B** | | | | | | | | |
| **数据偏移4** | **保留6** | **U**  **R**  **G** | **A**  **C**  **K** | **P**  **S**  **H** | **R**  **S**  **T** | **S**  **Y**  **N** | **F**  **I**  **N** | **窗口2B** |
| **校验和** | | | | | | | | **紧急指针** |
| **选项（长度可变）** | | | | | | | | **填充** |

1. 序号：报文段的序号，一般是第一个字节的序号
2. 确认号：希望收到的序号值N，表明已经收到前N-1个序号的数据已经正确收到。
3. 数据偏移：首部长度，4B的倍。如(70)16=(0111000)2=710，所以首部长度为7×4=28B。
4. 紧急URG：URG=1时，表明为紧急字段，高速系统此报文段有紧急数据，需要尽快送达，可以插队，发送方把紧急数据放在本报文段的最前面，与紧急指针配合使用，而紧急指针后面的数据就是正常数据。
5. 确认ACK：仅当ACK=1时，确认号才有效，当ACK=0时，确认号无效。TCP规定建立连接后，所有传送的报文段必须把ACK=1。
6. 推送PSH：当两个应用程序进行交互式通信时，有时在一端的应用进程希望在键入一个命令后立即就能收到对方的相应。当PSH=1时，把接受到的报文向上交付给应用进程，不再等到整个缓存满了之后再向上交付。
7. 复位RST：当RST=1时，表明TCP连接中出现严重差错，必须释放连接，然后再重新建立运输连接，RST=1还可以拒绝一个非法报文段或拒绝打开一个连接。
8. 同步SYN：建立连接时用来同步序号。当SYN=1而ACK=0时，表明这是一个连接请求报文段。若对方统一建立连接，则应在响应报文段中使SYN=1而ACK=1
9. 终止FIN：用来释放连接。当FIN=1，表示此报文段的发送方的数据已发送完毕，并要求请求释放连接。
10. 窗口：窗口值是[0,216-1]之间的整数。窗口值告诉对方接收方允许发送的数据量。
11. 紧急指针：在URG=1时才有意义，它指出本报文段中紧急数据的字节数。注意：当窗口为0时也可以发送紧急数据，紧急数据结束后就是普通数据。

### 6. TCP的流量控制：利用滑动窗口实现流量控制

  如果发送方把数据发送得过快，接收方可能会来不及接收，这就会造成数据的丢失。所谓流量控制就是让发送方的发送速率不要太快，要让接收方来得及接收。利用滑动窗口机制实现对发送方的流量控制和可靠传输。

WT+WR≦2n

**TCP窗口单位是字节，不是报文段。**

**TCP规定，接受窗口为0时也必须接受以下几种报文段：零窗口探测报文段；确认报文段；紧急数据报文段。**

**糊涂窗口综合症**

**是流量控制方面的问题，如何解决：让接收方等待一段时间，或等到接受缓存已有一半空闲空间，使接受缓存有足够的空间容纳一个最长的报文段。**

补充：超时重传时间计算：新的RTT=(1-α)×(旧的RTT)+α×(新的RTT样本)

### 7. TCP的拥塞控制：慢开始、拥塞避免、快重传和快恢复四种控制方法

**拥塞：**  
  即对资源的需求超过了可用的资源。若网络中许多资源同时供应不足，网络的性能就要明显变坏，**整个网络的吞吐量随之负荷的增大而下降。判断网络拥塞的依据是出现超时。**

**拥塞控制：**  
  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：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、路由器，以及与降低网络传输性能有关的所有因素**。

当网络吞吐量下降到0时，发生**。拥塞控制是动态的(而不是静态的)。**

**开环控制与闭环控制：**

开环控制：事先将有关发生拥塞的因素考虑周到，根据用户协议限制进入网络的交通，从而阻止拥塞的发生，中途不进行改正

闭环控制：事先不需要预留资源，资源利用率高，实时监控，哪里出问题就去改正问题，主要措施：检测拥塞、报告拥塞和调整措施。

补充：拥塞控制的方法：慢开始，拥塞避免，快重传，快恢复

发送窗口上限值=min{接受窗口，拥塞窗口}

**慢开始**：当主机刚开始发送数据，由于不清楚网络负荷，所以由小到大逐渐增大拥塞窗口值。拥塞窗口cwnd从1，2，4，8，16...

**拥塞避免**：当cwnd增大到快开始门限ssth时，开始使用拥塞避免，以1开始增加

**注意当MSS=2，拥塞窗口增加一个MSS**。当出现网络拥塞（网络超时）时，cwnd变成1，继续慢开始1，2，4，8增长，此时的新的ssth是网络拥塞时窗口的一半，到达新的ssth，再开始拥塞避免。**拥塞避免并非完全能够避免拥塞，只是使网络比较不容易出现拥塞。**

**快重传**：发送方只要连续收到3个重复确认就立即重传对方未收到的报文段

**快恢复**：当收到三个重复确认执行快重传算法，拥塞窗口cwnd变为ssth的一半，不再变成1了，再继续拥塞避免算法，以1增加。

**为什么超时检测和收到三个重复的确认要采用不同策略？**

**因为有时，个别报文段会在网络中丢失，但实际上网络并未发生拥塞。如果发送方没有收到确认，就会产生超时，发送方会误认为网络发生了拥塞，这就导致发送方错误地启动慢开始，把拥塞窗口设置为1，从而降低了传输速率。采用快重传算法可以使发送方尽早知道发生了个别报文段丢失，这样就不会出现超时，发送方就不会误认为出现了网络拥塞，提高整个网络的吞吐量。**

**流量控制与拥塞控制区别：**  
  流量控制指**点对点通信量的控制，是端到端的问题**。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。

拥塞控制是**一个全局性的过程**，涉及所有主机路由器以及与降低网络性能有关的所有因素。

**主动队列管理AQM**(active queue management)：不要等到路由器的队列长度已经达到最大值才不得不丢弃尾部的分组，这样太被动，要采用主动的方式，当队列长度到达某个值时(即网络有了拥塞征兆时)，主动的丢弃到达的分组，以告诉发送发应该放慢发送速率。用**随机早期检测RED**(random early detection)，是用于网络中全局同步现象。

### 8. TCP传送连接的管理

  TCP连接的端口称为套接字（socket）或插口。端口拼接到IP地址即构成套接字。每条TCP连接唯一的被通信端的两个端点（即两个套接字）确定。

**TCP连接的建立**

**三次握手**

1. 客户机首先向服务器发送一个连接请求报文段，该报文段不含应用层数据，SYN=1，ACK=0，客户机随机选择一个起始序号seq=x（连接请求报文不携带数据，但要消耗一个序号）。
2. 服务器如果同意请求，就分配缓存和变量，发回确认报文段，SYN=1，ACK=1，ack=x+1，并且服务器随机产生起始序号seq=y（确认报文不携带数据，但要消耗一个序号）
3. 客户机收到确认报文段后，分配缓存和变量，发回确认报文段，SYN=1，ACK=1，seq=x+1，ack=y+1（该报文段可携带数据，若不携带则不消耗序号）

**注意**：服务器端的资源是在完成第二次握手时分配的，而客户端的资源是在完成第三次握手时分配的，这就使得服务器易于受到SYN洪泛攻击。

  为什么不采用“两次握手”建立连接呢？  
  主要是为了防止发生死锁。例如，假定A给B发送一个连接请求分组，B收到了这个分组，并发送确认帧。按照两次握手协定，此时B认为连接已经建立成功，可以开始发送数据。可是A在接受B的确认帧时，这个确认帧丢失了，A不知道B是否已经准备好，也不知道B发送数据使用的初始序列号，A甚至怀疑B是否收到了自己的连接请求分组，A认为连接还未建立成功，将忽略B发来的任何数据分组，只等待连接确认应该分组，当B发出的分组发生超时后，重复发送同样的分组，就发生了死锁。

**TCP连接的释放**

1. 客户机大算关闭连接时，发送连接释放报文段，并停止发送数据，FIN=1，seq=u，它等于前面发送过的数据的最后一个字节的序号加1（FIN报文段即使不携带数据，也要消耗一个序号）。发送FIN后，发送方不能再发送数据，但对方还可以发送数据。
2. 服务器收到后发回确认，ack=u+1，而这个报文段自己的序号是v，等于他前面已经传送过的数据的最后一个字节的序号加1。此时客户机到服务器方向的连接就关闭了，但服务器若继续发送数据，客户机仍要接收，即服务器到客户机方向的连接并未关闭。
3. 若服务器已经没有要向客户机发送的数据，就发出连接释放报文段，FIN=1。
4. 客户机收到释放报文段后，必须发出确认。在确认报文段中，ACK=1，ack=w+1，seq=u+1。此时TCP连接还未释放，必须经过时间等待计时器设置的时间2MSL后才进入连接关闭状态。

  为什么不采用“三次握手”释放连接，且发送最后一次握手报文后要等待2MSL的时间呢？  
  原因有两个：

1. 保证A发送的最后一个报文段能够到达B。如果A不等待2MSL，若A返回的最后确认报文段丢失，则B不能进入正常关闭状态，而A此时已经关闭，也不可能再重传。
2. 防止出现“已失效的连接请求报文段”。A在发送最后一个确认报文段后，再经过2MSL可保证本连接持续的时间内所产生的所有报文段从网络中消失。造成错误的情形与不采用“两次握手”建立连接的情形相同。

**注意**：服务器结束TCP连接的时间要比客户端早一些，因为客户机最后要等待2MSL后才可进入CLOSED状态。

**总结如下：**

1. 连接建立，分3步：
   1. SYN=1,seq=x **不携带数据，消耗一个序号**
   2. SYN=1,ACK=1,seq=y,ack=x+1 **不携带数据，消耗一个序号**
   3. ACK=1,seq=x+1,ack=y+1 **可以携带数据；若不携带数据则不消耗序号**
2. 释放连接，分4步：
   1. FIN=1,seq=u
   2. ACK=1,seq=v,ack=u+1
   3. FIN=1,ACK=1,seq=w,ack=u+1
   4. ACK=1,seq=u+1,ack=w+1

# 应用层

### 1. C/S结构(客户/服务器模型)的优点

1. 具有灵活的硬件系统构成，同时处理多个远地或本地客户的请求
2. 提高程序的可维护性
3. 利于变更和维护应用技术规范
4. 进行严密的安全管理

P2P模型特点：

1. 繁重的计算机任务可以被分配到其他节点上，提高使用率。
2. 系统可扩展性好。
3. 网络更加健壮，不存在中心节点失效的问题。
4. 平等的对等连接通信。

### 2. DNS的层次结构

**DNS可分三个部分：层次域名空间、域名服务器、解析器**

**层次域名空间：主机名......三级域名 . 二级域名 . 顶级域名.**

**所以最左边的就是主机名。**

**顶级域名分为三大类：**

1. **国家顶级域名：如.cn表示中国，.us表示美国，.uk表示英国等.**
2. **通用顶级域名：ac(科研机构) .com(公司和企业) .net(网络服务机构) .org(非盈利性组织) .edu(教育机构) .gov(政府部门) .mil(军事部门) .int(国际组织)**
3. **基础结构域名：只有一个arpa，反向域名解析。**

  DNS 是一个联机分布式数据库系统，采用客户服务器方式。有点像电脑的目录树结构：在最顶端的是一个“root”，然后其下分为好几个基本类别名称，如：com、org、edu 等；再下面是组织名称，如：ibm、microsoft、intel 等；继而是主机名称，如：www、mail、ftp 等。因为当初 internet 是从美国发展起的，所以当时并没有国域名称，但随着后来 internet 的蓬勃发展，DNS 也加进了诸如 tw、hk、cn 等国域名称。所以一个完整的 dns 名称就好象是这样的：[www.xyz.comr.tw](http://www.xyz.comr.tw/" \t "/Users/hekangjia/Documents\\x/_blank) ，而整个名称对应的就是一个(或多个) IP 位址了

### 3. 域名服务器的类型

1. 本地域名服务器：本地域名服务器不属于层级系统
2. 根域名服务器：它用来管辖顶级域名，它并不直接把待查询的域名转换成IP地址，而是告诉本地域名服务器下一步应该找哪个顶级域名服务器进行查询。
3. 顶级域名服务器：这些域名服务器管理所有二级域名。最后的结果直接告诉你对应的IP地址，也可能告诉下一步应该找谁。
4. 授权域名服务器：负责一个区的域名服务器，当一个授权域名服务器不能给出最后的查询结果，就会告诉发出请求的DNS客户下一步应该找哪个授权域名服务器。

补充：域名解析过程

主机向本地域名服务器查询有两种方式 ：递归查询和迭代查询（更常用）。

1. 递归查询：一步步查询；**主机向本地域名服务器的查询一般都是采用递归查询**
2. 迭代查询：让其他域名服务器告诉本地域名服务器“下一步应该向哪个域名服务器进行查询”。**本地域名服务器向根域名服务器的查询通常采用迭代查询**

### 4. Internet的应用协议:FTP，MIME，HTTP

**1）FTP文件传输协议：属于客户/服务器模式，不是点对点，TCP**

**在进行传输文件时，FTP需要建立两个并行TCP连接，控制连接和数据连接。**

**控制连接：21端口用于发送FTP命令；控制连接在整个会话期间一直保持打开**

**数据连接：20端口用于传输数据；注意：若是主动模式，则是20端口，若是被动模式，将自行决定，一般端口号大于1024。数据传送完数据连接就关闭了**

**补充：**

**FTP(基于TCP)和TFTP(基于UDP简单文件传送协议)，他们都是文件共享协议中的一大类，即复制整个文件，特点是：若要存取一个文件，就必须先获得一个本地的文件副本，若要修改文件，只能对文件副本进行修改，然后在将修改后的文件副本上传到原节点。**

**文件共享协议另一大类是联机访问，即允许多个程序同时对同一个文件进行存取。**和数据库不同之处是用户不需要调用一个特殊的客户进程，而是用户可以用远地文件作为输入输出运行任何应用程序。**操作系统中的文件系统提供对共享文件的透明存取，存取的优点：将原来用于处理本地文件的应用程序用来处理远地文件时，不需要对该应用程序做明显的改动。**

**NFS网络文件系统工作原理：可是本地计算机共享远地资源，目前只是建议标准**

**NFS文件修改：NFS允许应用程序打开一个远地文件，并能在该文件的某个特定位置开始读写数据，NFS可使用户只复制一个大文件中的小的片段，而不需要复制整个大文件，在网络上传送的只是少量的修改数据。**

**FTP工作原理：FTP最主要的功能减少或消除不同操作系统下处理文件的不兼容性。FTP文件修改：因为FTP文件修改只能对副本进行修改，然后将修改后的副本上传到原节点，所以现将远地计算机B的文件传送到计算机A，进行修改，再将修改后的副本传送到计算机B，需要来回的传送，消耗了大量时间。**

**TFTP(trivial)简单文件传送协议:**端口号69，使用UDP数据报，有差错改正措施。TFTP只支持文件传输，不支持交互，没有列目录功能，不能对用户进行身份鉴别。

TFTP优点：

1. 每次传送的数据报文中有512字节的数据，最后一次可不足512字节
2. 数据报文按序编号，从1开始
3. 支持ASC码或二进制传送
4. 可对文件进行读写
5. 使用简单的首部

**TFTP与FTP区别：TFTP没有交互，不进行身份验证。**

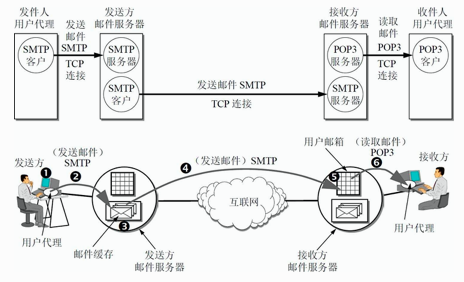
**远程终端协议TELNET：**TCP；能适应许多计算机和操作系统的差异，利用网络虚拟终端NVT，把客户的击键和命令转换成NVT格式，发送给服务器，同理，当服务器返回数据时，服务器把远地系统的格式转换成NVT格式，本地客户再从NVT格式转换到本地系统所需的格式。

**SMTP简单邮件传送协议：C/S；TCP**

**邮件不会在互联网中的某个中间邮件服务器落地。如果SMTP客户还有一些邮件要发送到同一个邮件服务器，可以在原来已建立的TCP连接上重复发送。**

**SMTP三个阶段：1.连接建立：用户代理先建立与发送方SMTP服务器的TCP连接。2.邮件传送：当发件人把邮件内容编辑好后，点击发送，接下来的事会交给发送方邮件服务器来完成，发送放SMTP服务器通过与接收方的SMTP服务器建立TCP连接，利用SMTP协议进行传输邮件。3.释放连接：邮件发送完毕后，SMTP释放TCP连接。**

注意：这里只有POP，没有SMTP



**POP3邮件读取协议：C/S；TCP**

POP3服务器用来接收邮件。POP3有一个特点，当读取了邮件，POP3服务器会把该邮件删除。

注意：SMTP只用来发送邮件，接收邮件是POP3.

**IMAP网际报文存取协议：C/S；TCP**

IMAP最大的好处在不同的地方可以使用不同的计算机随时上网处理邮件。IMAP允许只读邮件中的部分内容。缺点是如果没把邮件复制到本地，则邮件一直会存放在IMAP服务器上，想要查阅必须上网。

注意：不要把POP3和SMTP协议弄混，当发件人向发送方邮件服务器发邮件和发送方邮件服务器向接收方邮件服务器发邮件，都是用的SMTP协议。而POP3则是用户从接收方邮件服务器上读取邮件所使用的协议

**MIME通用互联网邮件扩充**

MIME（Multipurpose Internet Mail Extensions，多用途Internet邮件扩展）。MIME被用在电子邮件系统中，也应用到HTTP中。MIME增加了邮件主体的结构，定义了传送非ASC码的编码规则，比如原来的SMTP不能传送中文或是图片，有了MIME就使得邮件内容的种类多样。

**MIME作用：MIME使内容类型多样化，增加了邮件的灵活性能够不仅能够传送文本，还能传送图像音频及视频等。**

MIME有两种将非ASCII码转换为ASCII码的编码方式：quoted-printable编码和base64编码。

**ASCII 0(48)；A(65)；a(97)；=(61)；**

1.quoted-printable编码：**针对少量的非**ASCII**码**，用一个等号“=”十六进制

例如：汉字“系统”二字的二进制编码是11001111 10110101 11001101 10110011（这四个字节都不是ASCII码，因为超过了127），换成十六进制为CFB5CDB3，用quoted-printable编码表示为=CF=B5=CD=B3，这12个字符都是可以用ASCII码打印的等号“=”的二进制代码为00111101，即十六进制为3D，因此等号“=”的quoted-printable编码为“=3D”

quoted-printable编码例子：

quoted-printable： 01001100 10011101 00111001

十进制： 76 157 121

十六进制 4 C 9 D 3 9

字符“=9D”

十进制 61 57 68

ASCII编码 01001100 00111101 00111001 01000100 00111001

其中字符=的ASCII编码为61 ；字符9的ASCII编码为57；字符D的ASCII编码为68

01001101 00100001 01111001 其开销为5/3-1=0.667

2.base64编码：对于任意二进制文件都可用，分为4个6位组。0～63

A表示0，Z为25，a为26，z为51，0为52，61为9，+为62，/为63，

ASCII码：0为48，9为57，A表示65，Z为90，a为97，z为122，例如

24位二进制： 01001001 00110001 01111001

划分为4组6位: 010010 010011 000101 111001

化为十进制 18 19 5 65

对应的base64编码 S(83) T(84) F(70) 5(53)

ASCII码 01010011 01010100 01000110 00110101

大写A：Bin(二进制)0100 0001、baiOct(八进制)0101、Dec(十进制)65、Hex(十六进制)0x41 例如：41H为41为16进制 ，其开销为1-24/32=0.25

1. **HTTP超文本传送协议：TCP，无连接；端口80**

**HTTP是面向事务的应用层协议，它是万维网能够可靠交换文件声音、图像等多媒体文件的基础。HTTP本身是无连接的，HTTP是面向文本的**。虽然使用了TCP连接，但是双方在HTTP交换时，不需要建立HTTP连接。

过程：当浏览器要访问WWW服务器时，首先要对WWW服务器进行域名解析，获得了IP地址后，浏览器通过TCP向服务器发送连接建立请求。每个服务器上都有服务进程，不断的监听TCP的端口80，当监听到连接请求后便于浏览器建立连接。TCP连接建立之后，浏览器会向服务器发送要求获取某一WEB页面的HTTP请求，服务器收到HTTP请求后，将构建请求web页面的必须信息，并通过HTTP响应返回给浏览器。浏览器在将信息进行解释，然后将web页面显示给用户，最后TCP连接释放

  HTTP是一种为了将位于全球各个地方的Web服务器中的内容发送给不特定多数用户而制订的协议。也就是说，可以把HTTP看作是旨在向不特定多数的用户“发放”文件的协议。

**非持续连接**：每请求一个文档都要进行TCP连接和HTTP页面请求两倍RTT开销，HTTP1.0就是非持续连接

**持续连接**：进行TCP连接和HTTP页面请求之后不会释放TCP，此连接不局限于同一个网页，只要这个文档在同一个服务器上就一直保持连接。目前的浏览器默认设置HTTP1.1，也可以取消。

**持续连接下还有两种连接方式：非流水线方式和流水线方式。**

**HTTP报文结构：**

GET /dir/index.htm HTTP/1.1 请求读取此连接

Host：[www.xyz.edu.cn](http://www.xyz.edu.cn) 主机域名

Connection：close/keepalive 非持续连接/持续连接

Cookie：12345 表示之前访问过

### 5. Web页面文档的分类

1. 静态文档：内容不会改变；优点：简单
2. 动态文档：由应用程序动态创建。内容不断变化；优点：报道最新信息
3. 活动文档：程序事先被编译成二进制代码存放在服务器端，当请求活动文档时，服务器返回活动文档程序副本给浏览器，该程序副本在浏览器端运行，对于服务器活动文档的内容是不变的。

### 6. 生成动态文档的方法

1. CGI通用网关接口（common gateway interface）程序：用来是万维网服务器将浏览器发来的数据传送给CGI程序，然后万维网服务器能够解释这个应用程序的输出，并向浏览器返回HTML文档。
2. 内嵌的PHP：超文本预处理器，是一种脚本语言
3. JSP：用于实现java web应用程序的用户界面，功能：访问数据库记录用户选择信息，在不同网页中传送控制信息和共享信息
4. ASP：是一种生成动态交互性页面强有力的工具，动态的编辑改变和添加网页的任何内容

### 7. 生成活动文档的方法

1. 用java技术创建活动文档
2. 用javascript技术创建活动文档

### 8. URL的格式：统一资源定位符<协议>://<主机>:<端口>/<路径>

  URL由三部分组成：资源类型、存放资源的主机域名、资源文件名。  
  URL的一般语法格式为(带方括号[]的为可选项)：  
  protocol :// hostname[:port] / path / [;parameters][?query]#fragment or file  
其中，

1. protocol（协议）：指定使用的传输协议（各种Internet应用协议），在最左边
2. hostname（主机名）：是指存放资源的服务器的域名系统 (DNS) 主机名或 IP 地址。
3. :port（端口号）：整数，可选，省略时使用方案的默认端口，各种传输协议都有默认的端口号，如http的默认端口为80。如果输入时省略，则使用默认端口号。有时候出于安全或其他考虑，可以在服务器上对端口进行重定义，即采用非标准端口 号，此时URL中就不能省略端口号这一项。
4. path（路径）：由零或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址。
5. ;parameters（参数）：这是用于指定特殊参数的可选项。
6. ?query(查询)：可选，用于给动态网页（如使用CGI、ISAPI、PHP/JSP/ASP/ASP.NET等技术制作的网页）传递参数，可有多个参数，用“&”符号隔开，每个参数的名和值用“=”符号隔开。
7. fragment（信息片断）：字符串，用于指定网络资源中的片断。例如一个网页中有多个名词解释，可使用fragment直接定位到某一名词解释。
8. file是资源文件名

例如：http://www.tsinghua.edu.cn/public/newthu/newthu\_cnt/faculties/index.html

协议 主机域名 路径名 文件名

### 9. 网络管理系统逻辑模型

  通常一个网络管理系统在逻辑上由被管对象、管理进程和管理协议组成。

1.被管对象：可以是主机、路由、打印机、集线器、网桥、调制解调器等。

2.管理站/管理器：由网络管理员操纵

3.管理协议：简单网络管理协议SNMP(simple network management protocol)

### 10. 网络管理的主要功能

### 网络管理的原理：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”对原有对象的影响必须尽量小些。

1. 配置管理：识别管理网络的拓扑结构、动态维护数据库等
2. 性能管理：确保网络提供可靠、连续的通信能力，到达网络资源最优化
3. 故障管理：找到故障发生位置，将故障与其他部分分离，修复或替换重新配置
4. 计费管理：统计用户使用什么信道，传输多少数据，访问什么信息等
5. 安全管理：确保网络资源不被非法使用，防止网络资源遭到攻击和破坏

### 11. 被管对象的特性

1. 命名：所有被管对象必须处在对象命名树上。
2. 类。表明被管对象拥有的属于哪个对象类。
3. 属性。被管对象拥有的特性参量。
4. 管理操作。可对被管对象施加的操作。
5. 行为。被管对象对管理操作所做出的反应。
6. 通报。被管对象可能主动发出的报告类信息。

### 12. SNMP的基本元素：UDP，CS

1. SNMP本身：负责读取和改变各代理中的对象名及其状态数值。
2. SMI(structure of management information)管理信息结构：定义命名对象和定义对象类型的通用规则和编码规则。为了确保网络管理数据的语法和语义无二义性。比如：int
3. MIB(management information base)管理信息库：对变量进行说明，定义变量名和类型整型等。只有MIB中的对象才能被SNMP管理

**总之，SMI建立规则，MIB对变量进行说明，SNMP完成网管动作。**

### 13. SNMPv3的安全模式

1. 基于用户的安全模式（USM）：提供身份验证和数据保密服务
2. 基于视图的访问控制模式（VACM）本地处理模块完成访问控制功能

与SNMPv1和2相比，SNMPv3增加了三个安全机制：身份验证、加密和访问控制。

# 网络安全

### 1. 网络面临的4种威胁:截获、中断、篡改、伪造

**被动攻击：** 是指攻击者从网络上窃取他人的通信内容，称为截获，了解正在通信的协议实体的地址和身份，又称为**流量分析**。被动攻击有时候比主动攻击更可怕。  
**主动攻击：** 中断、篡改、伪造

补充：

主动攻击：

1. 恶意程序：病毒、木马、流氓软件等。
2. 拒绝服务：攻击者向某个服务器不断发送大量分组，是服务器无法提供正常服务，导致瘫痪。

针对攻击采取的措施

主动攻击能够采取措施加以防范，但被动攻击很难检测出来；对于被动攻击可采取数据加密技术；对于主动攻击，需将加密技术与适当的鉴别技术相结合。

### 2. 替代加密和置换加密

**替代加密**：明文中的字符被替换成另一个字符。如凯撒密码

明文：abcd efgh ijkl mnop qrst uvwx yz

密文：zsex drcf tgyb

置换加密：将字符按一定的规则移动，但不改变它

### 3. 秘密密钥加密算法：DES（明文位数，密钥位数，分组密码）

**明文位数**  
  加密前对整个明文进行分组，每个分组位64位长的二进制数据。然后对每个64位二进制

**密钥位数**  
  然后对每一个64位二进制数据进行加密处理，产生一组64位密文数据。最后将各组密文串接起来，密钥占有64位，实际长度为**56位**，外加8位用于奇偶校验。

**对称加密密码体制(DES)保密性仅取决于对密钥的保密，算法是公开的**

**补充：公钥加密密码体制和对称加密密码体制(DES)**

**公钥加密密码体制**：使用不同的加密密钥和解密密钥，加密密钥是公开的，解密密钥是保密的，算法是公开的，需要数字签名。

**对称加密密码体制**：使用相同的加密密钥和解密密钥，加密解密密钥都是保密的，算法的公开的。

**公钥加密密码体制和对称加密密码体制区别：在使用信道方面有很大的不同。**

在使用对称密钥时，由于双方使用同样的密钥，因此通信信道上可以进行**一对一双向保密通信**，每一方即可用此密钥加密明文，并发送给对方，也可以接受密文，用同一密钥解密，这种保密通信仅限于持有此密钥的双方(如再有第三方就不保密了)。它的密钥都是保密的，但是算法是公开的。

在使用公钥密钥时，在信道上可以**多对一单向保密通信**，例如可以有很多人持有公钥，并用此公钥对自己的明文加密发送给对方，只有持有对应私钥的人才能对收到的多个密文进行一一解密，由于**公开密钥加密密钥只能加密不能解密**，所以反方向保密通信是不行的，因此是多对一单向保密通行。它的密钥分为公钥和私钥，公钥是公开的，私钥是保密的。

**任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量，并不是简单的取决于加密体制。公钥密码体制并没有让传统密码体制弃用，因为目前的公钥密码体制的开销较大，**暂时不会被放弃。

### 4. 公开密钥算法的特点

  公钥密码体制使用不同的加密密钥与解密密钥。

  在公钥密码体制中，加密密钥PK是向公众公开的，而解密密钥SK则是需要保密的。加密算法E和解密算法D也都是公开的。

  ※使用公开密钥时，在通信信道上可以是多对一的单向保密通信。例如，可以有很多人同时持有**B**的公钥，并各自用此公钥对自己的报文进行加密后发给对方，只有对方才能用其私钥对收到的多个密文进行解密，**由于公开密钥只能加密不能解密**，这对密钥进行反方向保密通信是不行的。

使用对称密钥时，在通信信道上可以是**一对一的双向保密通信**。

### 5. 公开密钥加密算法：RSA

**公开密钥加密算法**RSA体制基于数论中的**大数分解问题的体制**

“常见的对称加密算法包括:DES、3DES、RC-5、IDEA。常见的非对称加密算法包括:RSA、ECC。

### 6. 数字签名

**功能**

1. 报文鉴别(核实签名)：接收者能够核实发送者对报文的签名，其他人无法伪造对报文签名。
2. 报文的完整性：接收者确信所受到的数据和发送者发送的完全一样而没有被篡改过
3. 不可否认：发送者时候不能抵赖对报文的签名

采用公钥算法要比采用对称密钥算法更容易实现。发送方用私钥经过D运算得到的密文发给对方，对方为了核实签名，用发送方的公钥进行E运算，还原出明文。注意：任何人使用发送发的公钥进行E运算后都可以得出发送方的明文，因此数字签名的通信方式并未为了保密，而是为了进行签名和核实签名，即确认此明文的确是发送方发的。

**注意：加密解密是先公钥加密进行E运算，然后用私钥D运算解密。**

**数字签名是先密钥签名进行D运算，然后用公钥E运算进行核实签名；**

**他俩是相反的过程！**

1. **鉴别：验证通信的对方的确是自己所要通信的对象，而不是其他冒充者，并且所传送的报文是完整的，没有被人篡改果。**

鉴别分为两种：报文鉴别(鉴别收到的报文是报文的发送者发送，而不是他人篡改和伪造)和实体鉴别(仅仅鉴别发送报文的实体，实体可以是一个人，一个服务器或客户)。

报文鉴别和实体鉴别区别：报文鉴别是对每一个报文都鉴别；

实体鉴别是全部持续时间，只需验证一次。

1. **防火墙**

防火墙是一种访问控制技术，是一个特殊编程路由器，把防火墙里面的称为可信的网络，外面称为不可信网络。

防火墙技术分为两类：

1. 分组过滤路由器具有分组过滤功能，它根据过滤规则对进出内部网络的分组执行转发或丢弃。过滤规则是基于分组的网络层或运输层首部的信息，例如可以将分组过滤器中所有目的端口号为23的入分组全部阻拦，这样就有效控制访问了。
2. 应用网关。所有进出网络的应用程序报文必须通过应用网关，应用网关可以在应用层打开报文，查看报文是否合法，如果不合法就丢弃。

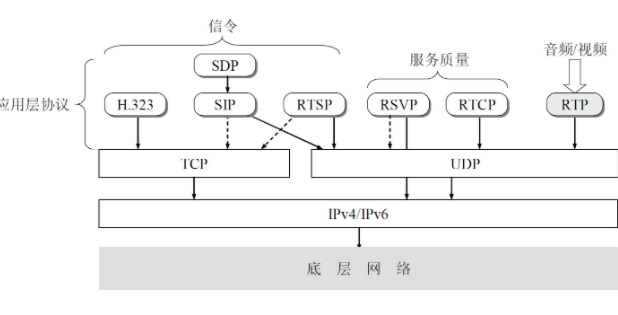
关于防火墙，以下哪种说法是错误的  
A．防火墙能隐藏内部IP地址  
B．防火墙能控制进出内网的信息流向和信息包  
C．防火墙能提供VPN功能  
D．防火墙能阻止来自内部的威胁

防火墙也有自身的限制，这些缺陷包括：防火墙无法阻止绕过防火墙的攻击、防火墙无法阻止来自内部的威胁、防火墙无法防止病毒感染程序或文件的传输。

# 视频、音频与无线网络

**IP电话所需要的几种协议**

### 第一种协议是信令（在互联网上找到被叫用户），第二种是直接传送音频/视频数据，如RTP，第三种是提高服务质量的，如RTCP。

****

### 1. RTP、RTCP、Qos等的概念

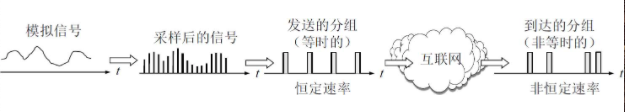
**RTP实时运输协议real-time transport protocol：端口号5004**  
  **为实时应用提供端到端的运输，但不提供任何服务质量的保证**。  
  基于UDP协议。  
  RTP分组只包含RTP数据，而控制是由另一个配套使用的RTCP协议提供的。  
  RTP在端口号1025到65535之间选择一个未使用的偶数UDP端口号，而RTCP则使用下一个奇数端口号。5004和5005分别为RTP和RTCP的默认端口号。

**RTCP(RTP控制协议)实时运输控制协议**  
  与RTP配合使用的协议，两者不可分割。基于UDP传送，但不对音频/视频封装。  
  主要功能是：服务质量的监视与反馈、媒体间的同步(如RTP传送的声音和图像的配合)以及多播组中成员的标志。

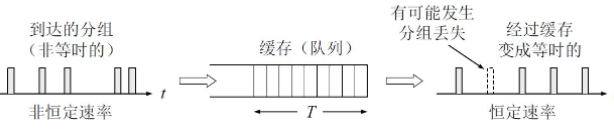
注意区分RTSP，RTSP功能让视频可以暂停播放和快进快退等功能。

**QoS**  
  服务质量（Quality of Service）：**是服务性能的总效果，此效果决定了一个用户对服务的满意程度**。指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，用来解决网络延迟和阻塞等问题。

### 2. 时延、时延抖动等的处理

当视频进行传输时时模拟信号，经过采样和数模转换变成数字信号，然后封装成分组进行传送，这时的时间间隔时恒定的即等时，经过互联网后，这些分组到达的时间会变不一样也就是非等时。如何解决呢？

**可以在接收端设置一个适当大小的缓存**，**通过缓冲区缓存后再以恒定速率读出，就变成了等时的分组，很大程度上消除了时延的抖动，但增加了时延。T就是播放时延**

  
  对于实时数据传送，使用UDP协议而不使用TCP，因为使用TCP如果出现丢失会进行重传，这样时延大大增加，对于传送实时数据时，**我们宁愿丢失少的分组，也不要太晚达到分组**，允许丢失少量分组来保证时延。

**对分组进行序号和时间戳**，接收端就知道应该在什么时间开始播放缓存中的分组来，这样可减少分组的丢失率。时间戳可以消除时延抖动，时间戳还可以使视频中的声音和图像同步。

### 3. WLan、WPan、WMan、WLL的概念

**WLan：**无线局域网（Wireless Local Area Network）

便携站和移动站意思不相同，便携站是位置固定，但是**移动站不仅能移动而且在移动的过程中进行通信**。

1. **无线局域网的组成**

无线局域网可分为两大类：固定基础设施和无固定基础设施

(1)固定基础设施

802.11是无线以太网的标准，使用星型拓扑，中心接入点AP每个AP必须分配一个不超过32字节的服务集标识符和通信信道，在MAC层使用CSMA/CA，又称为WiFI。

一个基本服务区BS和无限移动通信的蜂窝小区相似，直径不超过100米.

(2)无固定基础设施

又称为自主网络，是由一些平等状态的移动站之间相互通信组成的临时网络。这些移动站具有路由器功能，自组网络一般不和外界其他网络相连接。

802.11无线局域网MAC帧结构**。帧有三种类型：控制帧、数据帧、管理帧**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2B | 2 | 6 | 6 | 6direct | 2 | 6source | 0~2312 | 4 |
| 去往AP | 帧控制 | 生存周期 | AP地址 | 源地址 | 目的地址 | 序号控制 | ———— | 数据部分 | FCS |
| 来自AP |  |  | 目的地址 | AP地址 | 源地址 |  |  |  |  |

**WPAN 802.15，2.4GHz的ISM频段**  
  无线个人区域网（Wireless Personal Area Network）就是在个人工作地方把属于个人使用的电子设备用无线技术连接起来自组网络，不需要使用接入点AP（Access Point），整个网络范围约为10m。蓝牙就是WPan。注意：无线区域网和个人区域网不完全等同，因为PAN不一定都是使用无线连接。

**WMAN 802.16**  
  无线城域网（Wireless Metropolitan Area Network）802.16是无线城域网的标准，WMAN可提供最后一英里的宽带无线接入。802.16可覆盖一个城市的部分区域，通信距离变化很大，远的可达50英里

### 4. 无线局域网的DCF和PCF

  802.11的MAC层的低层是**分布协调功能（DCF）**，DCF**使用一个竞争算法**来提供对所有通信的访问，普通异步通信直接使用DCF。**PCF（点协调功能）**是集中的MAC算法，该算法用来**提供无竞争**的服务。  
  **DCF：DCF采用争用服务，而是**DCF子层使用简单的CSMA算法，让各个站的争用信道来获取发送权。DCF向上提供争用服务，**802.11规定所有实现都必须有DCF功能**。如果一个站点有一个MAC帧要发送，它先监听介质，如果介质空闲，站点可以发送，否则站点必须等待，直到现在的传输完毕，才能进行传输。  
  **PCF：PCF采用无争用服务，**是在DCF之外实现的一个**可供选择的访问方式**，其操作包括集中轮询主管的轮询。对于时间敏感业务就使用PCF，如分组话音。

### 5. CSMA/CA协议的原理：ACK确认帧；预约信道：使用RTS/CTS帧

对于无线局域网为什么不使用CSMA/CD **A B C**

这是因为：“碰撞检测”要求一个站在发送数据的同时，还要不断检测信道，但由于无线局域网传输条件特殊，在802.11适配器上收到的信号强度有时候非常弱，如果在无线局域网实现碰撞检测，在硬件上花费很大。更重要的是，即使无线局域网可以碰撞检测，仍然无法避免碰撞，比如隐蔽站和暴露站问题，所以无线局域网不需要进行碰撞检测。

1.隐蔽站问题

由于A和C距离较远，彼此听不见对方，检测不到碰撞。

1. 暴露站问题

检测到信道忙，其实不忙  **A B C D**

  载波侦听多路访问/碰撞避免（Carrier Sense Multiple Access with Collision Avoidance，CSMA/CA），主要用于无线网，不需要进行碰撞检测。

**原理**：发送数据前先检测信道，若信道空闲，则等待一段时间DIFS(分布协调功能帧间隔)后就可以发送。为什么要等待DIFS间隔呢？因为要考虑到可能有其他高优先级的帧要发送。当源站发送一个数据帧后，目的站若正确接收，则经过SIFS(最短帧间隔)后，目的站会向源站发送**确认帧ACK**，所有802.11采用的是停止等待协议，是一种可靠传输协议。但802.3有线局域网是不可靠传输，它的可靠传输有高层负责

  CSMA/CA协议的基本思想是在发送数据时先广播告知其他结点，让其他结点在某段时间内不要发送数据，以避免出现碰撞。**当信道从忙专为空间状态时，为了避免碰撞，所有站都采用随机退避算法：第k次退避2k+2中随机选，最大是256(第六次退避)。802.11局域网使用的是CSMA/CA，采用停止等待协议，是可靠传输**。因为无线信道的通信质量不如有线信道，必须等到收到对方的确认帧后才能继续发送下一帧，有**确认机制**。

CSMA/CA算法归纳：

1. 若站点有数据发送，检测到信道空闲，则等待时间DIFS后，就发送数据；
2. 若信道忙，站点执行CSMA/CA退避算法。一旦检测到信道忙，就冻结退避计时器。只要信道空闲就开始倒计时。
3. 当退避计时器减到0时，就开始发送数据并等待确认；
4. 源站收到确认帧，则证明目的站已经收到了。如果要发送第二帧，就开始步骤2.若规定时间内没有收到确认帧，就必须重传此帧，再次使用CSMA/CA协议争用接入信道，若经过若干次重传失败还是没有收到，则丢弃。

**只有这个情况不使用退避算法：检测到信道空闲时，发送第一帧数据时，不用退避**。

**信道预约：RTS/CTS帧**

**请求发送RTS(request to send)：**在A向B发送数据之前，先发送一个短的控制RTS，它包括源地址，目的地址和这次通信所需的时间，发送RTS之前也要先检测信道，然后在等待DIFS后才能发送。

**允许发送CTS(clear to send)：**若B收到A的RTS帧，则等待SIFS后，向A发送一个允许发送CTS帧。A收到CTS后，再等待SIFS后，开始发送数据帧，B收到数据帧后，再等待SIFS后，发送ACK确认帧。过程如下图：**NAV网络分配量**

**DIFS SIFS SIFS SIFS**

数据帧

RTS

**A**

ACK

**B**

CTS

A在RTS帧中填写所需的持续时间

A的NAV

B在RTS帧中填写所需的持续时间

B的NAV

# 注意：这里的NAV都是RTS和CTS发送完才开始计算

# 下一代因特网

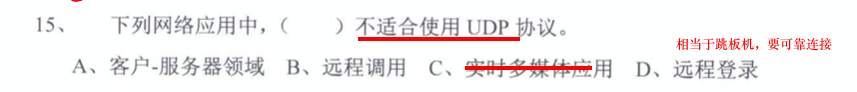
### 1. IPv6的特点

1. 更大的地址空间，IPv6地址从IPv4的32位扩大到128位；4B-->16B，使地址空间扩大到了296倍
2. 减少路由选择表的长度
3. 简化协议，使路由器处理分组更迅速
4. 提供比当前IP更好的安全性（鉴别和保密）
5. 增加对服务类型的注意，特别是实时数据
6. 通过定义范围来帮助多播的实现
7. 让主机可以不改变其地址即可漫游
8. 协议未来还可以扩充
9. 允许新旧协议共同存在一些时间
10. 拓展的地址层次结构：地址多了，所以可以划分更多的层次；
11. 灵活的首部格式：IPv6将IPv4的可选字段移出首部，变成拓展首部，提高路由处理效率；
12. 改进的选项：IPv6首部长度是固定的，所以不需要首部长度字段；
13. 支持即插即用(即自动配置)：IPv6不需要DHCP协议；
14. 支持资源预分配：IPv6支持实时视像等保证一定的带宽和时延的应用。
15. IPv6首部长度必须是8B的倍数，首部基本长度40B；IPv4是4的倍数；
16. IPv6只能在主机分片，而IPv4可在路由和主机分片；重组在目的主机

**IPv6基本首部40B**

**0 4 12 16 24 31**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **通行量类** | **流标号** | | |
| **有效载荷长度** | | | **下一个首部** | **跳数限制** |
| **源地址**  **(128bit 16B)** | | | | |
| **目的地址**  **(128bit 16B)** | | | | |

**版本：**指明协议的版本，IPv6该字段为6

**通行量类：**区分不同的IPv6数据报的类别或优先级

**流标号：**IPv6的一个新机制是支持资源预分配，允许虚有其把每个数据报于一个给定的资源分配相联系。“流”比如是实时音频或视频传输，这个流经过的路径上的路由器都保证指明的服务质量。属于同一个流的数据报具有相同的流标号。

**有效载荷长度：**指明IPv6数据报除基本首部以外的字节数。该字节最大值64KB

**下一个首部**：它相当于IPv4的协议字段或可选字段

**跳数限制：**用来防止数据报在网络中无限期的存在，源点在每个数据报发出时设定一个跳数限制(最大值为255跳)。每经过一个路由器就减1，当减为0时，丢弃该数据报。

**数据报途中经过路由器都不处理这些拓展首部，这样就大大提高了路由器的处理效率。**

**IPv6的地址表示**：

104.230. 140.100. 255.255. 255.255. 0.0. 17.128. 150.10. 255.255

68E6 : 8C64 : FFFF : FFFF : 0: 1180: 960A: FFFF

FE80:0:0:0:02AA:00FF:FE9A:2CA0 后三位是MAC地址

0010 AA 00 其中1要变0 ,所以MAC地址高位是0000 AA

所以mac地址为00：AA：00:9A：2C：A0

### 2. P2P技术的特点

1. 非中心化
2. 可扩展性
3. 健壮性
4. 高性价比
5. 隐私保护
6. 负载均衡

P2P模型特点：

1.繁重的计算机任务可以被分配到其他节点上，提高使用率。

2.系统可扩展性好。

3.网络更加健壮，不存在中心节点失效的问题。

4.平等的对等连接通信。

**目前P2P工作方式下的文件共享在互联网流量中已占据最大份额，比万维网所占的比例大很多。**

**当对等方的数量很大时，采用P2P方式下载大文件，比传统CS模式快很多。**

**P2P应用中，广泛使用索引和查找技术是分布式散列表DHT。**

### 3. 标记交换原理

**补充：MPLS的由来：**

在传统IP网络中，分组每到达一个路由器就必须查找路由表，并按照“最长前缀匹配”的原则找到下一跳IP地址，当网络很大时(路由表很大)，查找有大量项目的路由器要花费很多时间，这样会引起分组丢失、传输时延增大和服务质量下降。因此我们引入了MPLS。

**MPLS特点：MPLS是面向连接的，就像虚电路一样**

1.支持面向连接的服务质量；2支持流量工程，平衡网络负载；3有效地支持虚拟专用网VPN。

标记交换就是根据分组中的“标记”检索交换机内部的转发信息库，使用转发消息库给定的出口信息完成该分组的转发。

在MPLS域的入口处，给每一个IP数据报打上固定长度的“标记”，然后对打上标记的IP数据报，**根据标记在链路层用硬件进行转发**，这就使得转发时不用查找转发表，使转发速度加快。

**MPLS的工作原理：**

**当一个IP数据报进入MPLS域时，MPLS入口节点会给数据报打上标记(实际是插入一个MPLS首部)，并按照转发表（不再上升到第三层网络层查找转发表，而是根据标记在第二层链路层用硬件进行转发）发给下一个LSR标记交换路由器；注意一个标记仅在两个标记交换路由器LSR才有意义，每经过一个LSR路由器换一个标记。**

**转发等价类EFC**

**传统路由选择协议选择最短路径，这会导致这段最短路径负载过重，使用EFC可使网络负载均衡，这种做法叫做流量工程TE或通信量工程。**

### 4. MPLS的封装：面向连接

由于IPv4数据报首部没有多余的位置存在MPLS标记，这就需要一种封装技术：在把IP数据报封装成以太网MAC帧之前，在以太网帧首部和IP数据报首部之间插入一个4字节的MPLS首部。MPLS首部就处在数据链路层和网络层之间。把加上MPLS首部的IP数据报封装成以太网帧，当以太网的类型字段为8847时是单播，8848是多播，这样接收方可以用帧类型来判断这个帧是否携带了MPLS标记还是普通的IP数据报。

MPLS首部格式

|  |  |  |  |
| --- | --- | --- | --- |
| 20bit | 3bit | 1 | 8 |
| 标记值 | 试验 | S栈 | 生存时间TTL |

以太网帧格式

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 6B | 6 | 2 | 4 | 20 | 20 | 1500 | 4 |
| 目的 | 源地址 | 类型 | MPLS首部 | IP首部 | TCP首部 | 数据部分 | FCS |

  MPLS （多协议标记转换，MultiProtocol Lable Switching）独立于第二和第三层协议，诸如ATM 和IP。它提供了一种方式，将IP地址映射为简单的具有固定长度的标签，用于不同的包转发和包交换技术。它是现有路由和交换协议的接口，如IP、ATM、帧中继、资源预留协议（RSVP）、开放最短路径优先（OSPF）等等。  
  在MPLS 中，数据传输发生在标签交换路径（LSP）上。LSP 是每一个沿着从源端到终端的路径上的结点的标签序列。现今使用着一些标签分发协议，如标签分发协议（LDP）、RSVP 或者建于路由协议之上的一些协议，如边界网关协议（BGP）及OSPF。因为固定长度标签被插入每一个包或信元的开始处，并且可被硬件用来在两个链接间快速交换包，所以使数据的快速交换成为可能。MPLS 主要设计来解决网路问题，通用MPLS封装包括标记栈、TTL和CoS(业务等级)等。

### 5. 标记分配的方式

1. 上游分配
2. 下游分配
3. 按需下游分配

### 6. 与以路由器作为核心网络平台的技术相比，MPLS的主要优点

1. 转发处理简单
2. 提供显式路由功能
3. 能够进行业务量规划
4. 提供QoS服务质量保证
5. 入口一次完成业务流分类
6. 提供多种分类细度
7. 用一种转发方式实现各种业务的转发（包括单播、组播和有特定质量要求的单播等）

### 7. IntServ综合服务的局限，IntServ可对单个会话提高服务质量的保证

1. **状态信息的数量与流的数目成正比**，流越多需要进行资源预留的开销越大，不具有扩展性；
2. 对路由器的要求高，所有的路由器必须实现资源预留协议RSVP、接纳控制、MF分类和分组调度；
3. 该服务不适合于短生存期的数据流
4. 许多应用需要某种形式的QoS,但是无法使用IntServ模型来表达QoS请求
5. 必要的策略控制和价格机制尚处于发展阶段，无法付诸应用
6. **IntServ体系结构复杂**，所有路由器必须装有RSVP，接纳控制和调度器等。
7. 综合服务IntServ所定义的**服务质量等级数量太少，不够灵活**

由于综合服务IntServ和预留资源协议RSVP都较复杂，所以提出了新策略**区分服务DiffServ，简写成DS**

### 8. DiffServ的体系结构

1. DS区域与DS区：一个DS域内在一个管理实体的控制下实现相同的区分服务策略。
2. 区分服务表记域与区分服务表记DSCP：不同字段对应不同等级的服务质量
3. 边界结点的传输分类与调节机制：**把所有复杂性放在DS域的边界结点，是DS域内部路由其工作尽可能简单**
4. 每跳行为PHB、PHB组与PHB组簇：**每跳行为只涉及本路由器转发这一跳**的行为(首先转发或是最后丢弃这个分组)，**而下一个路由器怎么处理与本路由器无关**。

**每跳行为PHB**

PHB分为两种：迅速转发PHB(EF PHB)和确保转发PHB(AF PHB)。

迅速转发PHB(EF PHB)：指明离开一个路由器的通信量的数据率**必须大于或等于**某一值，因此EF用来构造通过DS域的一个低丢失率、低时延、低时延抖动、确保带宽的端到端服务(即不排队或很少排队)对应EF的区分服务码点DSCP值为101110.

确保转发PHB(AF PHB)：DSCP把通信量分为不同等级和丢弃优先级。

**DS总共有8bit，DS不同字段对应不同等级的服务质量。前6bit是区分服务码点DSCP，后面两位目前不使用**

### 9. DiffServ的技术特点

1. 层次化结构
2. 总体集中控制策略
3. 利用面向对象的模块化思想与封装思想，增强了灵活性与通用性
4. 不影响路由
5. diffserv提供聚合功能。相同DS值按照同优先级转发，**区分服务不需要使用RSVP信令。**

### 10. 搜索引擎

全文搜索和分类目录搜索

全文搜索：需要关键词，由软件进行查询，数据库的容量非常大，准确度不是很高。例如谷歌、微软必应、百度、北大天网

分类目录搜索：有主题划分，针对性强一点，比如娱乐 有雅虎、新浪、搜狐、网易

垂直搜索引擎：购物，旅游，汽车，求职，房产，交友等。

补充：

1. 关于TCP/IP协议中，IP层只提供无连接服务；但若是说网络层和OSI中就提供面向连接（虚电路）和无连接服务（IP数据报）。
2. X.25是网络层的面向连接、虚电路的服务，HDLC帧格式，IP是无连接服务.
3. 帧中继是X.25简化版，都是点对点，可变长帧，面向连接虚电路
4. 公用分组交换网使用的是X.25
5. 信元长度是53B。首部是5B。
6. 信道利用率取决于帧的长度
7. 帧间隔取决于帧的类型，高优先级间隔短。
8. 当计算机给另一台计算机发送电子邮件，描述了数据封装步骤：数据、段、数据包、帧、比特。
9. 局域网是一个种广播技术发展起来的，广域网是基于交换技术发展起来的。
10. 在缺省配置的情况下，交换机的所有端口属于同一VLAN。连接在不同交换机上的、属于同一VLAN的数据帧必须通过Trunk链路传输
11. 当一个IP分组进行直接交付时，要求发送方和目的站具有相同的子网地址。
12. 目前广域网采用网状结构。
13. 目前城域网采用环状结构。
14. 目前局域网采用星型结构。
15. 网桥是即插即用设备。
16. 数据链路层和传输层都有差错控制，有什么区别？

对于差错控制：数据链路层只保证了点到点之间的无错传输，经过了网络层，要进行拆包和重新封装及其他加工处理，其间可能会发生偏差，网络层的检验和只校验了首部部分，还要经过传输层进行数据部分校验，所以传输层的差错控制保证了端到端之间的无错传输。

1. 模拟信道就传输模拟信号——频带；基带是数字信号。
2. 假设通信信道带宽为1Gb/s，端到端时延为10ms，TCP传送窗口为65535字节，最大吞吐量是多少？线路利用率是多少？

解：一个窗口的发送时延=65535\*8/1000000000=0.52428ms

一个窗口的总时延=10\*2+0.52428=20.52428ms

1s内可以发送1/20.52428ms个窗口=48.72个窗口

吞吐量是1s传送多少数据=48.72\*65535\*8=25544379b/s

利用率=吞吐量\*带宽=25544379\*1000000000=2.55%

19.被路由协议是是IP协议，OSPF是路由协议

20.路由协议是建立路由表的协议；被路由协议是使用路由表的协议。

21.对于同一目的，路由协议RIP在路由表中只能保存一条最短的路由

22.对于同一目的，路由协议OSPF在路由表中可以保存多条相同代价成本的路由。

23.葡萄酒策略适应文件传输。旧的分组比新分组好，

24.牛奶策略适应流媒体应用。新的分组比旧的分组好，适合实时传输。

# 12截屏2020-11-28下午5.17.46

解析：（1）到源路由器就丢弃了，跳数1跳，概率p

到目标路由器就丢弃了，跳数2跳，概率(1-p)p

成功到达目标主机，跳数3跳，概率(1-p)(1-p)；

利用加权平均，平均跳数=1×p+2(1-p)p+3(1-p)(1-p)=p2-3p+3；

（2）一次成功，必须要经过3跳，即一次成功的概率A=(1-p)(1-p)；

二次成功，=(1-A)A

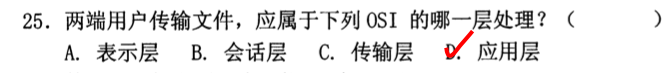
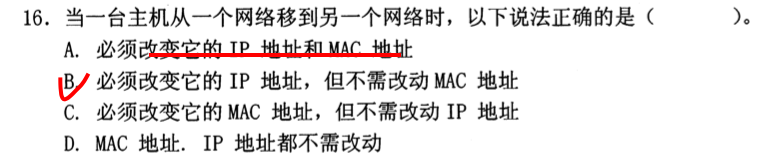
三次成功，=(1-A)(1-A)A

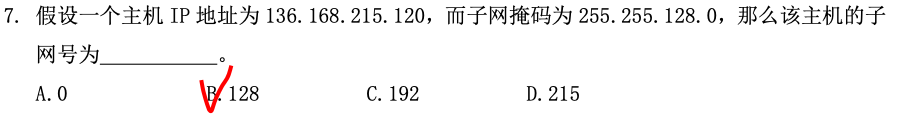
利用加权平均：平均次数=1×A+2(1-A)A+3(1-A)(1-A)A=1/(1-p)2

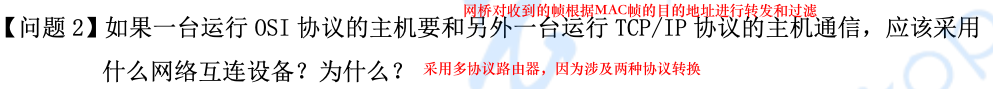
（3）平均跳数=平均次数×平均跳数=(p2-3p+3)/(1-p)2

# 13

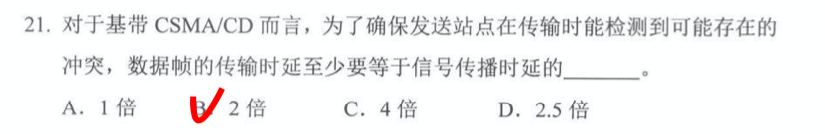
# 截屏2020-11-29下午5.13.33

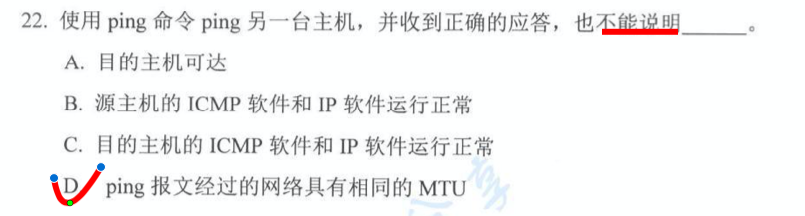


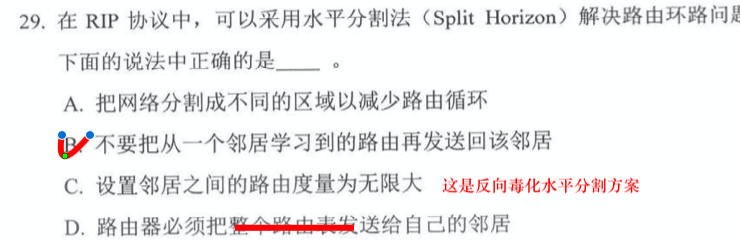


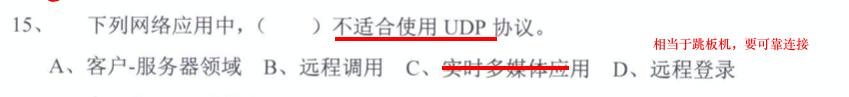


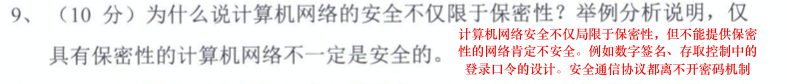
# 截屏2020-12-03下午3.53.39

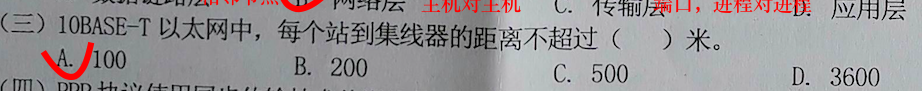


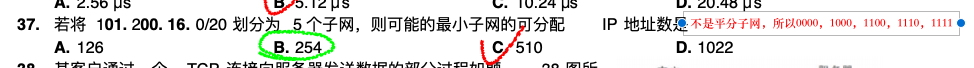




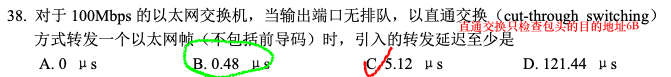


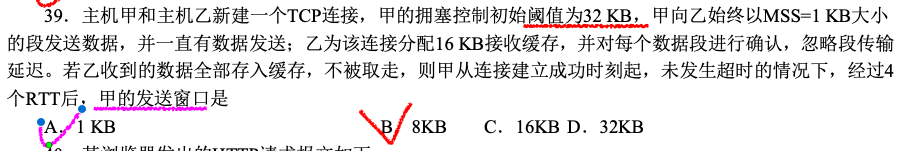


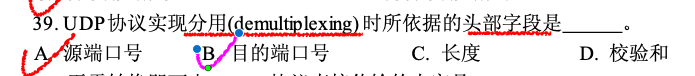




# 





****

# 英译

1. ISP：Internet Service Provider 因特网服务提供者
2. LCP：Link Control Protocol
3. ICP：Internet Content Provider 因特网内容提供者
4. NCP：Network Control Protocol 网络控制协议
5. URL：uniform resource locator 统一资源定位符
6. URI：uniform resource identifier 统一资源标识符
7. SPF：short path first 最短路径算法
8. LSR：link state request 链路状态请求
9. LSU：link state update 链路状态更新
10. LSA：link state acknowledge 链路状态确认
11. ROM：read only memory 只读存储器
12. RAM：random access memory 随机存储内存
13. VPN：virtual private network 虚拟专用网
14. ICMP:internet control message protocol 网际控制报文协议
15. IGMP：internet group management protocol 网际组管理协议
16. QoS：quality of service 服务质量
17. SNMP：simple network management protocol 简单网络管理协议
18. SMTP：simple mail transfer protocol 简单邮件传送协议
19. ADSL：asymmetric digital subscriber line 非对称数字用户线
20. ARP：address resolution protocol 地址解析协议
21. HTTP：hyper text transfer protocol 超文本传送协议
22. DNS：domain name system域名解析系统
23. IMIE：multipurpose internet mail extensions通用互联网邮件扩充
24. POP3：post office protocol 邮局协议版本3
25. IMAP：internet mail access protocol 网际报文存取协议
26. FDM：frequency division multiplexing 频分复用
27. TDM：time division multiplexing 时分复用
28. STDM：statistic time division multiplexing 统计时分复用
29. WDM：wavelength division multiplexing 波分复用
30. DWDM：dense wavelength division multiplexing 密集波分复用
31. CDMA：code division multiple access 码分多址
32. SONET：synchronous optical network 同步光纤网
33. SDH：synchronous digital hierarchy 同步数字系列
34. STM-1：synchronous transfer module-1 第一级同步传输模块
35. OC-48：optical carrier-48 第48级光载波
36. LLC：logical link control 逻辑链路控制
37. MAC：medium access control 媒体接入控制
38. ISP：internet service provider 因特网服务商
39. WAN：wide area network 广域网
40. MAN：metropolitan area network城域网

补充：