计算机网络

零、概述

协议名							
ISO/OSI	物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
TCP/IP	网络接口层	——	网络互联层	传输层	应用层	——	——
五层协议	物理层	数据链路层	网络层	传输层	应用层	——	——

各层作用：【大概考一层】

物理层：完成比特和能量间的转换，处理物理传输介质相关接口；

数据链路层：介质访问控制子层（MAC）和逻辑链路控制子层（LLC）；

网络层：主机间通信、路由寻径；

传输层：进程间端到端的通信，提供传输可靠性，流量控制和拥塞控制；

应用层：提供通用应用程序，完成用户信息或软件转换信息的交互。

一、物理层

1.1 传输介质

介质分类：光、电气、无线电波。【可能让举例】

引导型四种介质：

非屏蔽双绞线、屏蔽双绞线（稍贵一点）和同轴电缆。

同轴电缆抗干扰性最强，常用于有干扰的短距离传输。双绞线则最常用。

光纤：高带宽、抗干扰、**贵**。分为多模光纤（有反射衰减）和单模光纤（衰减小，贵）。只有全双工。

非引导型：

红外线、激光、无线电波、卫星。

1.2 局域通信

传输模式分为串行（同步、异步、等时）和并行。

异步通信：

单工：单方向通信。

半双工：双向，但通道唯一，故同一时刻只能单向。

全双工：双向，多条通道，故可任意双向。

端序：

大端序：高位置数据存在低地址。小端序：与大端序相反。

Eg：数据[12345678]，若以字节大端序位小端序存储，则12为最高字节，34其后。

12存在低地址0000，以位小端序存储，故实际为21。

```
0003:87
0002:65
0001:43
0000:21
```

DCE和DTE设备：

DCE：数据通信设备，用来连接DTE和数据通信网络的设备；

DTE：数据终端设备，用于发送和接受数据的设备；

异步通信标准-RS232：【大概率考】

采用全双工。

机械特性：D型插头，三根线-发送、接受、地。

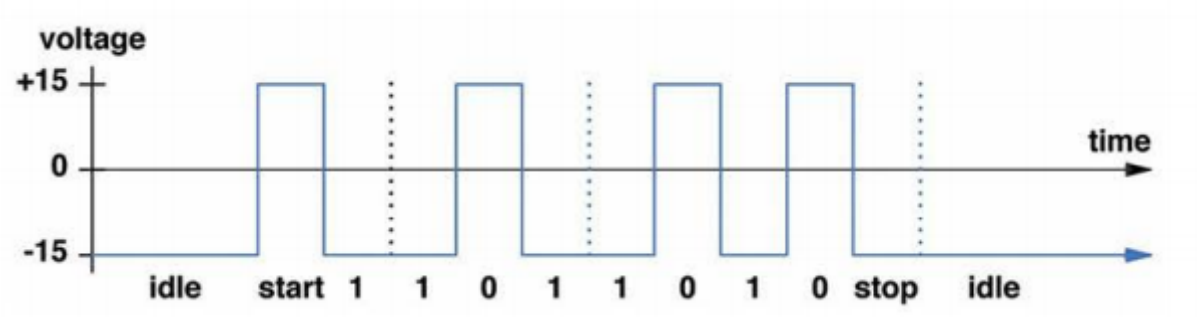
电气特征：电压范围-15V~+15V；[-15V~-3V]表示1，[+3V~+15V]表示0。

帧格式：字节大端序位小端序，即数据单元内数据需要倒过来看。

起始位[1bit]-数据单元[8bit，最高位=0]-停止位[>=1bit]；

空闲期（idle）在起始位前，停止位后，一般包含停止位，故至少1bit。

Eg：传输"["(ASCII=91)



若发送方和接收方使用停止位位数不同，数据传输正确，但会减缓传输速率。

波特率：每秒传输位数。bps。

奈氏定理：理论最大数据速率——$D = 2Blog_2K$，B=带宽，K=信号可能取值（二进制情况下K=2）。故采样频率大于信号带宽2倍即可完全采样。

香农定理：

信噪比（信号功率和噪声功率的比）$SNR = 10log_{10}S/N(dB)$，S/N=100时，信噪比为20分贝。

实际最大传输速率：$C = Blog_2(1 + S/N)$。

1.3 远程通信

调制：用基带信号控制载波信号的参量变化，将信息荷载其上形成已调信号以在信道内传输。包括调幅、调频、调相。

解调：将已调信号恢复为基带信号的过程，为调制逆过程。包括解调幅、解调频、解调相。

复用：多个信源信息流组合在一条介质上传输。

频分复用FDM：用户在同一时间占用不同频率带宽。

时分复用TDM：用户在不同的时间占用同样的频带宽度。将时间分为若干TDM帧，分开使用。TDM信号也叫等时信号。

TDM分为**同步时分复用**（普通的时分）和**统计时分复用**[异步时分复用]（没有数据时跳过缓存）。

这两种复分技术比较成熟，但不够灵活；时分更有利于数字信号传输。

波分复用WDM：光的频分复用。

基带和宽带：

基带：原始电信号所固有频带。基带信号：将数字1、0用电压表示。

宽带：同时传输多个信号的通信系统。宽带信号：基带信号调制后的频分复用模拟信号。

二、数据链路层

2.1 差错控制

奇偶校验码：【这俩考一个】

数据和校验位共有奇数个1或偶数个1（奇校验或偶校验）。

Eg：数据[01011011]，共5个1，故even[偶]=1，odd[奇]=0。

奇偶校验码可检测错误（50%），但不能纠正错误。

Internet校验和：

每16位计算总和，若结果大于16位，重复计算，最后取反。

Eg：[F3,04,E7,23,E5,E6]=F304+E723+E5E6=2C00D->C00F->3FF0。

CRC：

不考计算。无法发现“同余”错误。

2.2 局域编址

三种交换：

分组交换：以分组为单位，**统计时分复用**。信道利用率高。

电路交换：独立信道，实时性高。交换的是电路。

报文交换：交换报文。

网卡作用：处理地址识别、CRC计算、帧识别、发送接受帧。减少CPU负荷。【可能考】

以太网MAC地址构成：

用于表示网络设备位置。地址48位，形式为：姓+名。

[姓]高24位由IEEE向厂家分配，[名]低24位由厂家自行分配。

第1个字节最低位=0[单播]，=1[多播或广播]，倒数第二低位=0[全局网址]，=1[局域网址]。

单播：一对一发送；多播：一对多特定发送；广播：一对全体，48位全为1。

网卡处理分组：【可能考】

①检测CRC，提取目标地址D；②如果网卡为混杂模式，接受；

③如果D=本地地址，接受；④如果D=广播地址，接受；

⑤如果D=多播地址，接受；⑥否则，丢弃分组。

以太网帧格式：【大概率考】

一般帧格式是头部+荷载，下为以太网帧格式。

目的地址[6B]-源地址[6B]-类型[2B]-数据[46~1500B]-CRC32[4B]。

数据少于46B，要填补到46B，满足加上头部64B的要求。超过1500就分片。

2.3 局域机制

网络拓扑四大结构：

【感觉这玩意不考，看看特点就行】

①网状拓扑：点对点连接；

优点：独立安装、独立访问、安全稳定；

缺点：线多成本高；

常用于远距离。

②星型拓扑：一组计算机通过集线器来传输信息，各节点与中心节点为点对点；

优点：容易增加节点，单节点异常不影响其他节点，容易实现网络监控；

缺点：中心节点故障引起网络瘫痪；

常用于近距离。

③环型结构：各节点为封闭环。相邻节点为点对点，非相邻要经过其他节点。

优点：结构简单易安装，节省资源；

缺点：容量有限，难增加新节点，单节点异常影响其他节点；

常用于远距离。

④总线型拓扑：所有节点连到一条长电缆。同一时间只能有一台计算机传信号。

优点：安装简单，成本低，单节点异常不影响其他节点；

缺点：介质故障引起网络瘫痪，安全性低，监控难，也难增加新节点；

以太网介质访问控制策略(CSMA/CD)：【大概率考】

适用于半双工的传统以太网。

①载波侦听[发送前]：站点发送前，监视电缆上是否有其他站点在发送。阻止最明显冲突。

②冲突检测[冲突时]：站点发送过程中，监视电缆的信号是否与本站信号相同，不同则终止发送。

③二进制指数退避[冲突后]：第n次冲突，延迟时间为$0-2^{n-1}d$随机。

其他类型网络：

【感觉也不考】

Local Talk：成本低、安装简单；Token Ring：单点故障会影响；

FDDI：单点故障能恢复，成本高；ATM：性能好，没冲突，成本高；

WLAN速度对比：知道WIFI快蓝牙贼慢就行。

2.4 局域设备

粗缆：总线型，连接网卡和收发器的电缆为AUI。

细缆：总线型，直接连接到使用BNC的计算机背面，成本比粗缆低；

双绞线：星型，使用集线器，计算机和集线器间为RJ-45双绞线；

冲突域和广播域：

冲突域：如果一CSMA/CD网络上两台计算机在同时通信时会冲突，则它们属于同一冲突域。

广播域：可以收到同样广播消息的节点集合。

四种用于扩展以太网的设备：【估计会考某个的功能和某几个的区别，注意作用域】

中继器：

工作在物理层。不理解帧格式，也无物理地址，不区分有效帧和其他信号。

适用于完全相同的网络互连。

功能：对数据信号重新发送或转发，来扩大网络传输距离。

集线器：

工作在物理层。

优点：使属于不同冲突域的计算机能跨碰撞域通信，扩大了局域网覆盖范围。

缺点：冲突域增加，但吞吐量未提高；若不同冲突域使用以太网技术不同，则不能相连。

网桥：

工作在数据链路层，其内的网卡始终处于混杂模式。

网桥接受到帧后，在地址表内寻找：

①如果目的地址和源地址在同一LAN段，则扔掉此帧；

②如果目的地址和源地址不在同一LAN段，则转发此帧，转发前要执行CSMA/CD；

③找不到，则发送到除本端口外的其他端口；

//广播风暴：当广播过多时产生网络拥堵。

//分布生成树：相互连接的网桥网络的一个生成树子集，以避免转发帧在网络内形成环。

网桥的地址表由自学习算法建立而成。

交换机：

工作在数据链路层。本质是多接口[全双工]的网桥。

//最大优点：独占传输媒体的带宽。

网桥和交换机都可以隔离冲突域，但这四种设备都不能隔离广播域。

2.5 远程技术

大多数互联网用户遵循非对称模式：接受数据比发送数据多。

上行：用户传输数据到ISP（互联网服务提供商）。

下行：ISP传输数据给用户。

ADSL：采用频分复用。上行大概800kb，下行大概10Mb。

【本节的其他东西太杂了，感觉不是重点，干脆没记录】

2.6 广域路由

分组交换机：

功能：存储与转发。

存储：把分组存储在存储器里；

转发：解析目的地址，只基于交换机ID[下面的站点号]，发送到对应端口；

寻址方案：站点号[标识分组交换机的唯一编号]+主机号[标识计算机]。

转发表[路由表]：列出所有交换机并**都**给出对应下一跳，要求为最短路径。

转发到下一跳的过程就称为**路由**。

默认路由：其实就是把下一跳相同的条目合并为单条目[to reach *]。只允许有一个默认路由。

路由表为每个交换机自己计算。

三、网络层

3.1 网际协议

IPv4：

全球唯一32位数字，网络号[全球协调]+主机号[局域网内协调]。

每8位作为无符号十进制值，用点分隔。Eg：192.5.48.3。

有类地址：【考】

A类：前缀0，0.0.0.0~，网络位8，主机位24，子网掩码255.0.0.0；

B类：前缀10，128.0.0.0~，网络位16，主机位16，子网掩码255.255.0.0；

C类：前缀110，192.0.0.0~，网络位24，主机位8，子网掩码255.255.255.0；

D类：多播地址，224.0.0.0~；

E类：保留地址，240.0.0.0~；

特殊IP地址：

主机号全0网络地址；主机号全1直接广播地址；

地址全1有限广播地址；地址全0本地地址；

127.0.0.1~127.255.255.254：环路地址，用于测试，不经过网卡。

CIDR表示法：ddd.ddd.ddd.ddd/m，d=网络号，m=掩码内1个数。【考】

划分子网：IP地址变为网络号+子网号+主机号，子网号借主机号的位数。【考啊】

子网掩码：路由器交换信息时必须提供该信息给其他路由器，路由表也得给出子网掩码。该信息用于找到IP地址中的子网划分。

多穴主机：有多个IP地址，每个网络连接1个地址，可提高可靠性。

IP报文头格式（共计160bit）：【可能扯到一些】

版本[4bit] 报头长度[4bit] 服务类型[8bit]

报文总长度[16bit] 标识[16bit] 分片标识[3bit]

片偏移[13bit] TTL[8bit] 协议类型[8bit]

报头校验和[16bit] 源IP地址[32bit] 目的IP地址[32bit]

封装：把IP报文塞进帧的载荷里，加入帧头帧尾，传输后再丢弃这些。

MTU：数据链路层支持的最大传输字节数。

分片：把大片分成小片，满足MTU。尽量分大片。除最后一片，每片字节数为8整数倍。注意原片和分片开头都有20B的IP头。分片到目标端才重组，过程不重组。【铁考啊】

3.2 支撑协议

ICMP：

目的：提高IP数据报交付成功机会。

机制：主机或路由器报告差错情况和提供异常报告。ICMP报文是封装在IP数据报内的。

分为差错报告报文和询问报文。

ping：把包含ICMP回送请求消息的IP数据报发送到指定目的地等回送。为应用层直接使用ICMP。

APR（地址解析协议）：建立IP地址和物理地址的映射。【APR还有一些细节看PPT去】

【剩下差不多看看就行】

3.3 路由协议

静态路由（非自适应）：简单、开销小、不能及时适应网络状态变化；

动态路由（自适应）：复杂、开销大，能适应网络状态变化；

自治系统：单一技术管理下的一组路由器，对其他自治系统表现出一种单一和一致的路由策略选择；

内部网关协议（IGP）：在自治系统内部使用的路由选择协议。

①RIP：每个路由器维护自己到其他目的网络的距离，仅和相邻路由器交换自己的路由表。

RIP距离（跳数）：路由器到直接连接网络距离为1。

优点：实现简单开销小；

缺点：限制网络规模（15）、出现故障要较长时间传送、网络规模增加开销增加；【同学说会考，我觉得不会】

②OSPF：向所有路由器发送信息（洪泛法）；发送的是本路由器相邻的所有路由器链路状态；只有链路状态发生改变才发送；

OSPF将自治系统分为更小的区域。每个区域有32位的标识符。区域不要超过200个。

洪泛法仅限于区域内，减少了通信量；区域内部只知道本区域；主干区域为0.0.0.0，连接下层区域；

OSPF直接使用IP数据报，而且很短；没有坏消息传的慢的缺点；

【不过上俩的区别特点还是得看看】

外部网关协议（EGP）：自治系统边界网关使用的路由选择协议，从一自治系统到另一自治系统。

BGP：不是找最佳路由而是找能到达且不绕圈的路由；

每个AS要选一个路由器作为BGP发言人，BGP发言人要建立TCP连接交换可达性信息；

四、传输层

4.1 可靠传输

端口：

端口号（16bit）：0~65536。用于标识本机的不同进程。

熟知端口号：0~1023；登记端口号：1024~49151；客户端口号：49152~65535；

UDP：【考特点和TCP的区别吧】

不可靠但高速的传输；

特点：无连接（发送数据前不用建立连接）、尽力交付（可能出错可能拥塞）、可多对多、轻量级。

应用场景：丢包损失小，应用层可控制丢包的场景。

TCP：【大考点】

可靠的传输；

特点：面向连接、点对点、流接口、完整可靠、全双工。

报文段的首部格式[20B=160bit]：

源端口号[16bit]；目标端口号[16bit]；

报文段序号[32bit]；确认序列号[32bit]；

报头长度[4bit]；保留位[4bit]；标识符[8bit]；

滑动窗口缓冲区[16bit]；校验和[16bit]；紧急指针[16bit]；

流接口：

以字节为单位封装在报文段内传输。

将字节写入发送缓存->加上TCP首部变成报文段->发送->从接受缓存读取然后去掉首部。

收到的报文段不一定按顺序，最后要按报文段的首部序号排序连接。

虚连接：

非真正的物理连接。不关心应用发的消息长度，而是根据窗口值和拥塞程度来决定报文段长度。

停止-等待：

发送、停止、等待确认，超过一定时间没收到确认，则重传。

简单但信道利用率低。可用流水线[即连续自动重传请求]提高效率。

连续自动重传请求的窗口机制：

逐一确认：窗口内分组连续发送，无需等待，收到一个确认就窗口滑动。

累积确认：收到几个分组才发送确认[收到的最后一个分组]。TCP要求接收方必须有这个功能。

窗口前沿不能收缩。发送窗口和接受窗口不一定一样大。

发送和接受缓存：

发送：应用程序要发的数据和已发还没收到确认的数据；

接受：已按序到达但还没被应用程序读走的数据和不按序到达的数据；

流量控制：就是滑动窗口的机制。注意窗口单位一直是字节。

拥塞控制：

拥塞窗口（cwnd）：发送方维持的状态变量。

①慢开始：初始cwnd=1，发送方每收到一个对新报文段的确认，cwnd+1。（指数增长）

②拥塞避免：cwnd=门限值时开始，将拥塞窗口变为线性增长。一旦拥塞门限值变为cwnd的一半，cwnd=1，重新开始。

③快重传：每收到一个失序报文段就立刻发出重复确认。发送方收到三个重复确认就开始重传。

④快恢复：发送方收到三个重复确认时，门限值减半，但cwnd不变。

发送方窗口=MIN（拥塞窗口，接收方窗口）

⑤随机早期检测：设置最小门限和最大门限，分组到达时，计算平均队列长度。

最小门限内的数据排队发送，最小门限~最大门限内的数据概率丢弃，最大门限外的数据直接丢弃。

连接建立和解除：【绝对会考】

A客户端B服务器端

三次握手：

①A发送请求报文段，SYN（首部同步位）=1，seq=x；

②B收到后，若同意则发回确认报文段，SYN=1，ACK=1，seq=y，ack=x+1；

③A收到后，再返回确认，ACK=1，seq=x+1，ack=y+1；

四次挥手：双方都可以主动。

①假设A先。A发送解除报文段：FIN=1，seq=u；

②B发出确认，ACK=1，seq=v，ack=u+1；此时B通知应用程序，A->B的连接解除；

③B再发，FIN=1，ACK=1，seq=w，ack=u+1；

④A收到，确认：ACK=1，seq=u+1，ack=w+1；A等待两个最长报文寿命后，B->A也解除；

五、应用层

5.1 C/S模式

客户端：主动打开、主动结束；

服务器端：被动打开、响应请求；

服务器和用户（硬件）与服务器端和客户端（软件）的区别：硬件上可以运行多个软件，有的是服务器软件和客户软件，有的不是；

Socket结构：：由IP地址+端口号。

API函数：

socket：创建一个绑定到特定传输服务提供者的插口；

bind：将本地地址关联到socket上；

connect：建立到一个给定套接字的连接；

listen：将套接字置于侦听传入连接的状态；

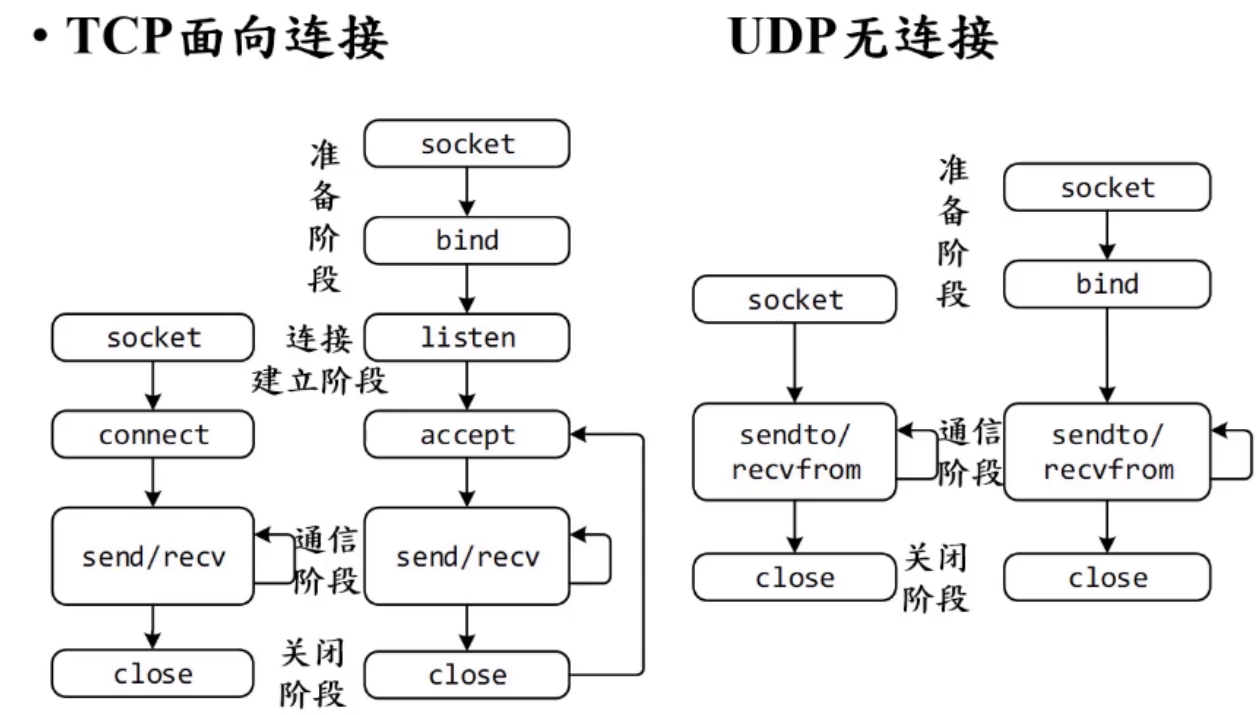
accept：允许套接字上的传入连接尝试；

send/sentto：把数据发送到已连接的套接字；

recv/recvfrom：从连接套接字接受数据；

closesocket：关闭插口；

【下图也绝对会考吧】



半相关：用（协议，本地地址，本地端口号）标志一个进程；

全相关：用（协议，本地地址，本地端口号，远程地址，远程端口号）标志一个进程；

5.2 域名系统

域名系统（DNS）：把可读符号映射到计算机地址。

域名：计算机名.组织名.顶级域名。

域名服务器：

根域名服务器-顶级域名服务器-权限域名服务器-本地域名服务器。

域名解析过程：

递归查询：主机向本地域名服务器查询，查不到本地域名服务器就作为客户往上查询；

迭代查询：本地域名服务器向根域名服务器的查询，根服务器给出IP地址或对应服务器；