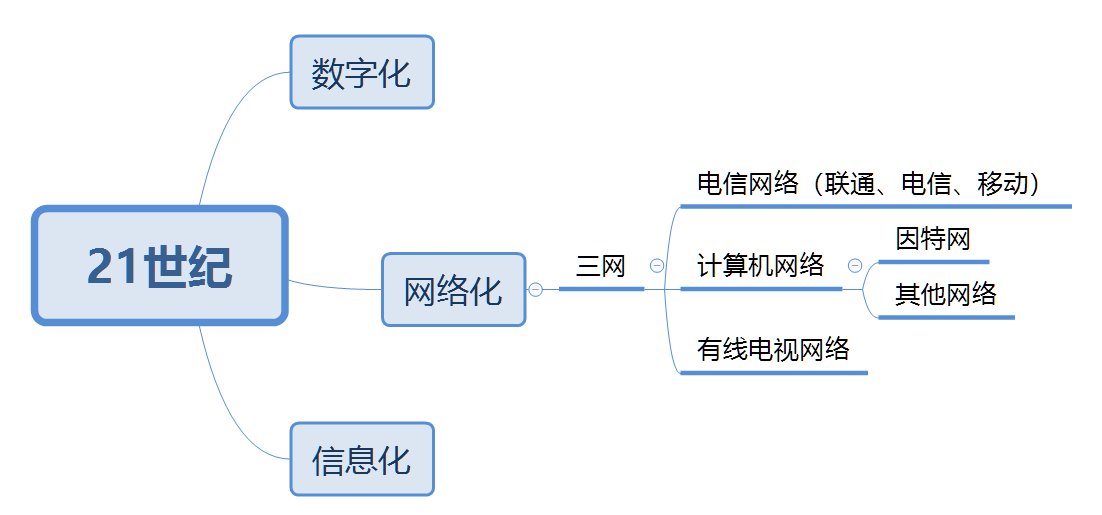
**计算机网络**

## 一、计算机网络概述



1. 计算机网络功能：连通性、共享性（信息共享、软硬件共享）
2. 因特网概述：

网络：许多计算机通过交换机连接在一起。

互联网（internet）：许多网络通过漏油器连接在一起。

因特网（Internet）：全球最大的一个互联网。

1. 因特网发展的三个阶段：

a. ARPANET向互联网发展（1983年 TCP/IP）

b. 三级结构的因特网（1985年 校园网-地区网-主干网）

c. 多层次ISP（Internet服务提供商）结构的因特网

地址分配是由因特网管理机构统一分配

1. 因特网的组成：

因特网 = 边缘部分 + 核心部分 = 资源子网 + 通信子网

a. 边缘部分：

主机间的通信：CS方式（Client Server）[客户端服务器方式]

P2P方式（Peer-to-Peer）[对等方式]

b. 核心部分：

数据交换方式：电路交换（电话）、报文交换、分组交换（计算机）

* 电路交换

电路交换适合于数据量很大的实时性传输。核心路由器之间可以使用电路交换。

* 分组交换

优点：高效、灵活、迅速、可靠

缺点：有时延、开销大

1. 计算机网络按拓扑结构可分为总线型、环型、星型（现多为星型）、树型、网状
2. 计算机性能指标

a. 速率（bit rate）：连接在计算机上的主机在数字信道上传送数据位数的速率。（b/s）

b. 带宽：数据通信领域中，数字信道所传输的最高数据率。（b/s）

c. 吞吐量：单位时间内通过某个网络的数据量。

d. 时延：发送时延、传播时延、处理时延、排队时延

处理时延：网路结点存储转发处理时间

排队时延：网络结点缓存队列排队时间

e. 时延带宽积 = 传播时延 × 带宽

f. 往返时间（RTT：Round-Trip Time）：从发送数据开始，到发送方收到接收方确认的时间。

g. 利用率：信道利用率、网络利用率

* 信道利用率

信道利用率与时延的关系：（利用率高时延也高）

其中，表示网络空闲时的时延，D表示网络当前时延，U表示信道利用率

* 网络利用率：信道利用率的加权平均值。

1. 计算机网络的体系结构

* 几个概念

ISO：国际标准化组织

OSI：互联网法律上的国际标准

ICP/IP Suit：因特网事实上的国际标准

* OSI七层模型

Application：能够产生网络流量，能够和用户交互的应用程序。

Presentation：加密，压缩，ASCII码/二进制码

Session：服务和客户端建立的会话 【可以用来查看木马（netstat -n）】

Transport：可靠传输（建立会话），不可靠传输（不建立会话），流量控制

Network：IP地址偏址，选择最佳路径

Data Link：数据如何封装，添加物理层地址（MAC地址）

Physical：电压，接口标准

* 网络排错：从底层到高层逐一排查
* 网络安全
  + 数据链路层安全：ADSL宽带、无线AP密码
  + 应用层安全：SQL注入漏洞，上传漏洞（php上传）
* TCP/IP四层模型：Application、Transport、Internet、Network Access（网络接口层）

1. 开放系统信息交换概念

实体（entity）：交换信息的硬件或软件进程。

协议（protocol）：控制两个对等实体通信的规则。

服务（service）：下层向上层提供服务，上层需要使用下层提供的服务来实现本层的功能。

服务访问点（SAP）：相邻两层实体间交换信息的地方。

1. 课本五层协议对应的数据单元

应用层：传输数据单元PDU

传输层：传输层报文

网络层：IP数据报（IP分组）

数据链路层：数据帧

物理层：比特流

## 二、物理层

1. 基本概念：
2. 物理层：解决如何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。
3. 数据：运送消息的实体。（消息一般都有实际意义，而数据指的是无意义的数据。）
4. 信号：数据的电气或电磁的表现。（模拟信号/数字信号）
5. 码元：在使用时间域的波形表示数字信号时，代表不同离散数值的基本波形就称为码元。在数字通信中常常使用时间间隔相同的符号来表示一个二进制数字，这样的时间间隔内的信号称为二进制码元。而这个时间间隔被称为码元长度。1码元可以携带nbit的信息量。
6. 信道：表示向一个方向传送信息的媒体。平常的通信线路一般包含一条发送信息的信道和一条接收信息的信道。
7. 单向通信（单工通信）：只能有一个方向的通信而没有反方向的交互。【广播电信号】
8. 双向交替通信（半双工通信）：通信的双方都可以发送或接收信息，但不能双方同时发送或接收信息。
9. 双向同时通信（全双工通信）：通信的双方可以同时发送和接收信息。
10. 基带信号（基本频带信号）：来自信源的信号，没有经过任何处理。
11. 带通信号：把基带信号经过载波调制后，把信号的频率范围搬移到较高的频段以便在信道中传输。
12. 几种基本的调制方法：调幅(AM)、调频(FM)、调相(PM)
13. 常用编码：

单极性不归零码：只使用一个电压值，用高电压表示1，没电压表示0。

双极性不归零码：用正电平和负电平分别表示1和0，正负幅值相等。

单极性归零码、双极性归零码

曼彻斯特编码、差分曼彻斯特编码（抗干扰能力强于曼彻斯特编码）：带有时钟频率

1. 信道的极限容量：有失真、但可识别
2. 奈氏准则：给出了在假定的理想条件下，为了避免码间串扰，码元的传输速率的上限值。

理想低通信道的最高码元传输速率=2WBaud

W是理想低通信道的带宽，单位为Hz；

Baud为波特，是码元传输速率的单位。

【波特与Bit区别：波特是在调制解调器中用到的概念，bit是信息量。

若一个码元含3个bit信息量，则1波特=3Bit/s】

1. 香农公式

信噪比：香农用信息论的理论推导出了带宽受限且有高斯白噪声干扰的信道的**极限、无差错**的信息传输速率。

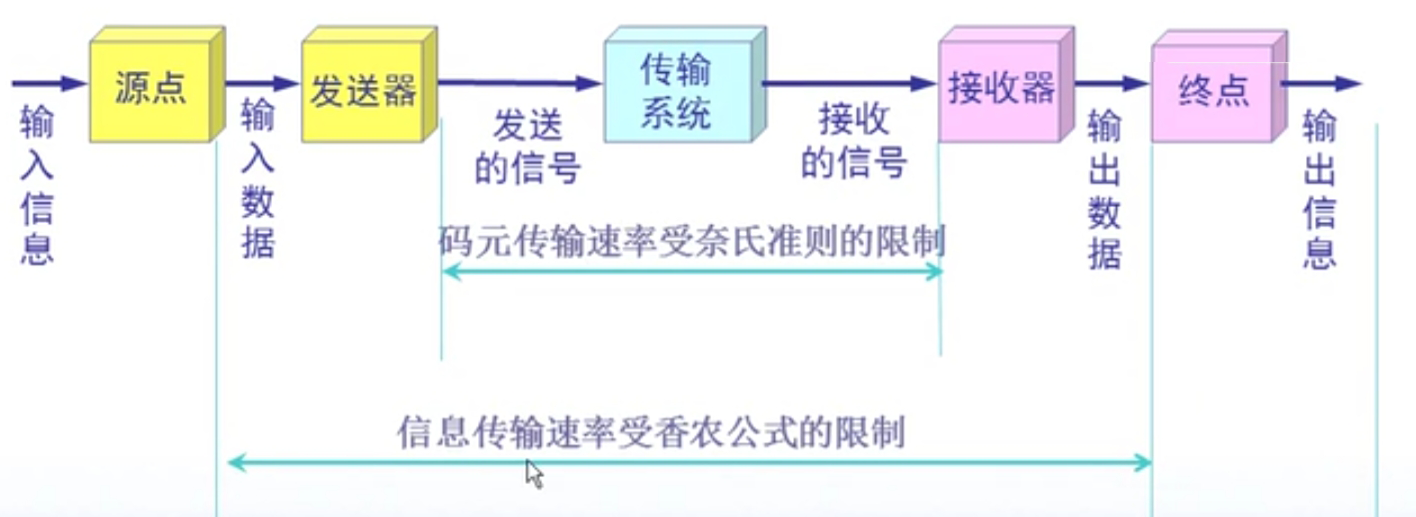
信道的极限信息传输速率C可表达为 b/s。

W为信道的带宽（以Hz为单位）；

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。

说明：只要信道传输速率低于信道的极限信息传输速率，就一定可以找到某种办法来实现无差错的传输。即如果传输速率足够慢，对方一定是可以听到声音的、

**

1. 物理层下面的传输媒体

* 导向传输媒体：双绞线（屏蔽和非屏蔽）、同轴电缆、光纤（单模、多模）
* 非导向传输媒体：无线电（短板主要是靠大气电离层的反射，通信质量较差；微波主要是直线传播，需要接收站）

【集线器：已被交换机代替，在网络中只起信号放大和重发的作用，本身是一个冲突域（半双工通信、会把信息传递给所有连接到集线器的PC端，由对方PC判定是否需要，不安全）。】

1. 信道复用技术

* 频分复用FDM：用户在分配到一定的频带后，在通信过程中自始至终都占用这个频带。
* 时分复用TDM：将时间划分为一段段等长的时分复用帧，每一个时分复用的用户在每一个TDM帧中占用固定序号的时隙，每一个用户所占用的时隙是周期性的出现。
* 统计时分复用STDM：加标记传输。
* 波分复用WDM：波分复用就是光的频分复用。（利用光解调器）
* 码分复用CDM：

码分多址CDMA：各用户使用经过特殊挑选的不同码型，因此彼此不会造成干扰。

每一个比特时间划分为m个短的间隔，称为码片。

同一码片规格化内积：

一个码片向量和该码片反码的向量的规格化内积值是-1。

规定码分方式时，一个码和其他的码必须正交。

1. 数字传输系统

脉码调制PCM体制最初是为了在电话局之间的中继线上传送多路电话。

PCM有两个互不兼容的国际标准，北美的简称Tl，欧洲的简称为El。我国使用的是El标准。El速率是2.048Mb/s，Tl的速率是1.544Mb/s。

1. 宽带接入技术

ADSL：用数字信号对现有的模拟电话用户线进行频分复用。（电话线）

光纤同轴混合网HFC（有线电视线）

光纤到户：FTTx

### 三、数据链路层

1. 基本概念
2. 数据链路层使用的信道主要有以下两种类型：点对点信道、广播信道。
3. 链路：一条点到点的物理线路段，中间没有任何其他部分。
4. 数据链路：除了物理线路，还有通信协议控制数据的传输（网卡），构成了数据链路。
5. 数据链路层解决的三个基本问题：

封装成帧【其中：IP数据报也称为最大传输单元MTU，不能超过1500字节。】

透明传输：用字节填充解决透明传输问题。（如：转移字符）

差错控制

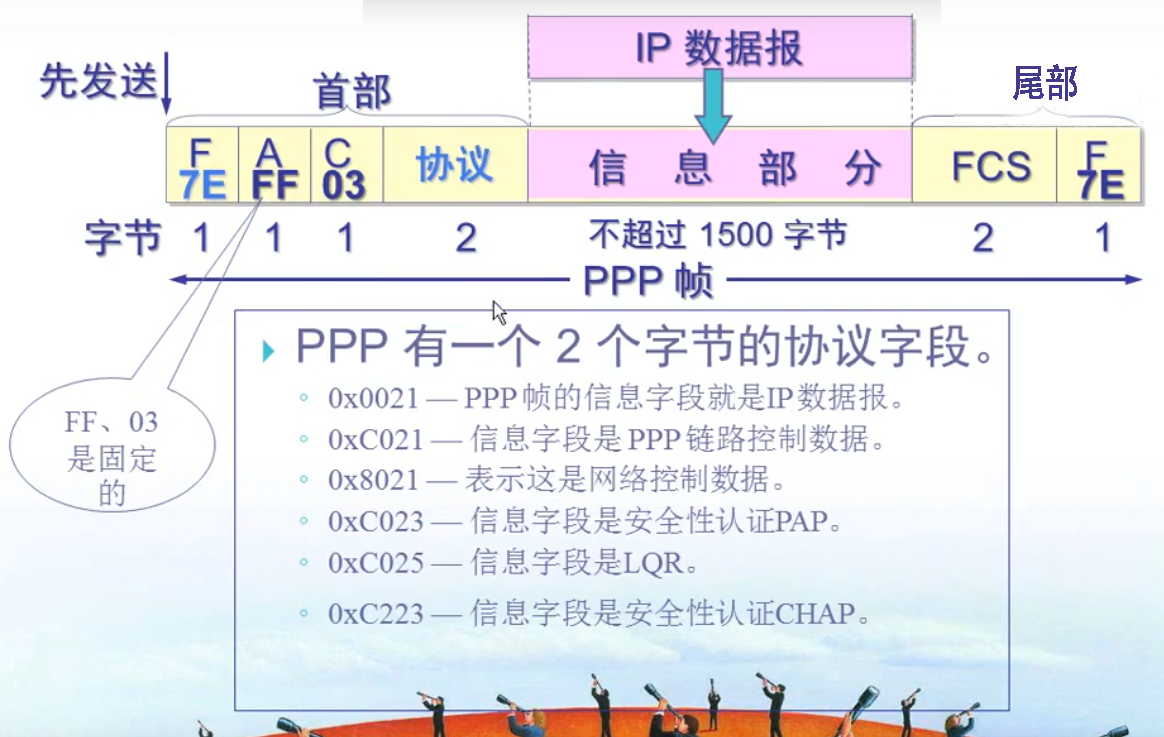
* 误码率(BER)：在一段时间内，传输错误的比特占所传输比特总数的比率。
* 循环冗余检验（CRC）：检验数据在传输过程中是否有错误，不是百分之百的可靠。（做抑或运算）

余数称为帧检验序列（FCS）

1. 点到点信道：

PPP协议

* 特点：有身份认证的功能、支持多种网络层协议、支持多种类型链路、可检测连接状态、网路层地址协商、支持数据压缩协商
* PPP协议内部分为三个层：高级数据链路控制协议（HDLC）、链路控制协议（LCP）【负责身份验证】、网络控制协议（NCP）
* 帧格式：



* PPP协议差错控制：如果传输的是字节的话，采用字节填充；如果传输比特流，采用零比特填充法

1. 使用广播信道的数据链路层（CSMA/CD协议）

局域网的拓扑：**星形网**、环形网、总线网、树形网

局域网共享通信媒体：静态划分信道（频分复用。。。）、动态媒体接入控制（随机接入、受控接入[目前以不被采用]）

* 以太网：载波监听多点接入/碰撞检测，使用CSMA/CD协议

1. 多点接入：表示许多计算机以多点接入的方式连接在一根总线上。
2. 载波监听：指每一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送数据，如果有，则暂时不要发送数据，以免发生碰撞。
3. 碰撞检测：发现冲突时间最长为2倍的单程时间【】，故一般以太网不能超过100米。
4. CSMA/CD协议特点：半双工通信
5. 争用期：最先发送数据帧的站，在发送数据帧后最多经过时间就可以知道发送数据帧是否遭受到了碰撞，我们将以太网端到端往返时间称为争用期。通常，取为争用期的长度。【对于10Mb/s以太网，在争用期可发送512bit，即64字节，即以太网在发送数据时，若前64字节未发生冲突，则后续的数据就不会发生冲突】
6. 以太网最短有效帧：64字节，若发送字节原本少于64字节，则会补零。故凡长度小于64字节的帧都是由于冲突而异常中止的无效帧。
7. 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）一个随机时间后才能再发送数据。

a. 确定基本退避时间：

b. 定义参数k，k = Min[重复次数, 10]

c. 从整数集合中随机地选取出一个数，记为r。重传所需的时延就是r倍的基本退避时间。

d. 当重传达16次仍不能成功时即丢弃该帧，并向高层报告。

1. 以太网
2. 为了使数据链路层能更好地适应多种局域网标准，802委员会将局域网的数据链路层拆分成了两个子层：逻辑链路控制LLC子层、媒体接入控制MAC子层【目前的局域网只有MAC协议了】
3. 以太网提供的服务是不可靠的交付，当接收到有差错的数据帧时就丢弃此帧，差错的纠正由高层来决定。
4. 以太网的信道利用率：

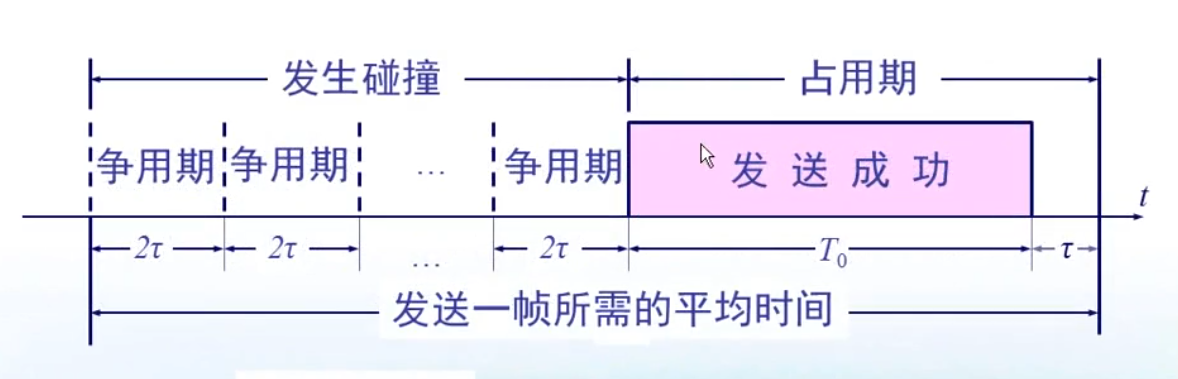
帧长为L（bit），数据发送速率为C（b/s），因而帧的发送时间为 。

参数：，a越小越好，即

当数据率一定时，以太网的连线长度受到限制，否则的数值会过大；

以太网的帧长不能太短，否则的值会太小，使a值太大。

理想情况下发送数据不发生碰撞，极限信道利用率为

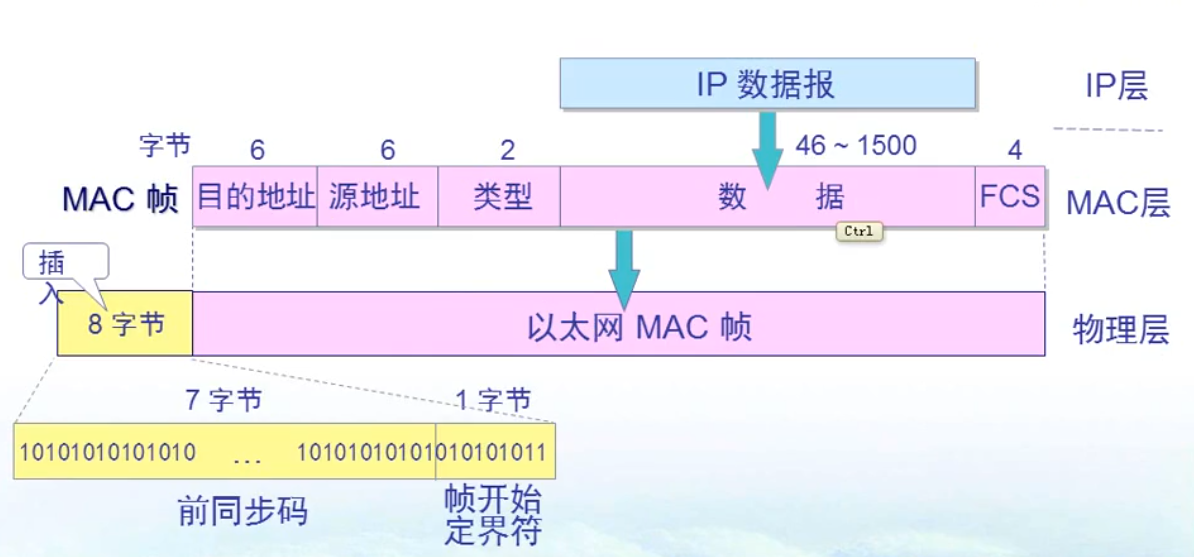


1. MAC地址，又称硬件地址或者物理地址，网卡的MAC地址由48位二进制组成，前24位是厂家信息，后24位由厂家指定。

查看MAC地址指令：ipconfig /all

网卡能收到的数据帧：单播帧、广播帧、多播帧

MAC帧格式：【以太网采用曼彻斯特编码，没有帧结束字符，电压消失时认为帧结束】



1. 扩展以太网

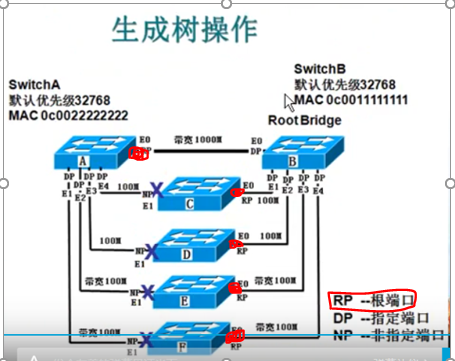
* 在物理层上扩展：使用光纤和一对光纤调制解调器连接到集线器以延长传输距离。
* 在数据链路层上扩展：使用网桥（会自学习MAC地址表）
* 网桥隔绝了冲突，但在一定程度上会增加延迟，因为其有储存转发的功能。

透明网桥：局域网上的站点并不知道所发送的帧经过了哪几个网桥，因为网桥对于各站点来说是不可见的。

网桥MAC地址表里若没有当前MAC地址，网桥会把数据帧转到所有的站点处，并记录此MAC地址。

透明网桥使用了生成树避免成环算法：

先选一个交换机做为根，然后其他交换机都选择一个离根近的端口作为根端口，对于所有线来说，选择离根交换机近（带宽高）的端口为指定端口，其他端口为阻断端口。



* 交换机：效率高，比较安全。

【扩展：远程重启计算机：shutdown -m [\\192.168.80.130](file:///\\192.168.80.130) -r】

1. 虚拟局域网VLAN

干道链路：可以走多个vlan的数据（统计时分复用）

组建局域网三层模型：接入层交换机、汇聚层交换机、核心层交换机

|  |
| --- |
| // 配置交换机安全  Switch(config)#interface fastEthernet 0/1  // 设置接PC  Switch(config-if)#switchport mode access  // 启用安全  Switch(config-if)#switchport port-security  // 违反安全关掉端口  Switch(config-if)#switchport port-security violation shutdown  // 绑定现在的mac地址  Switch(config-if)#switchport port-security mac-address sticky |

### 四、网络层

1. 网络层向运输层提供的两种服务：

虚电路服务：发送逻辑线路由管理员确定。（已被淘汰）

数据报服务：逻辑线路由路由器自主选择，数据报中包含起始地址和终止地址。

|  |  |  |
| --- | --- | --- |
| **对比** | **虚电路服务** | **数据报服务** |
| 思路 | 可靠通信由网络来保证 | 可靠通信由用户主机来保证 |
| 连接的建立 | 需提前指定 | 不需要指定 |
| 终点地址 | 仅在连接建立阶段使用，每个分组使用短的虚电信号 | 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 |
| 当结点出现故障时 | 所有通过出故障的结点的虚电路均不能工作 | 故障出现的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 | 到达终点时不一定按发送顺序 |
| 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 |

1. 网际协议IP
2. 网络互连的设备：中间设备又称中间系统或中继系统

物理层中继系统：转发器（集线器）

数据链路层中继系统：网桥或交换机

网络层的中继系统：路由器

网络层以上的中继系统：网关【非平时所说的网关，平时所说的网关一般指路由器的接口（网关一般都使用本网段的第一个地址或者最后一个地址）】

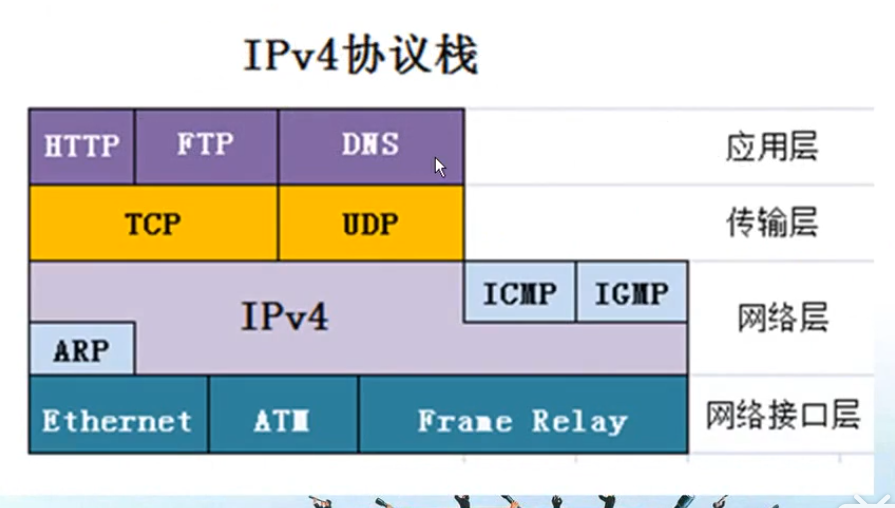
1. 虚拟互连网：不关心具体网络设备，只通过IP地址进行访问，不关注具体网络异构细节。
2. 网络层的协议：

IP协议

地址解析协议ARP、逆地址解析协议RARP：负责解析对方网卡的MAC地址

网际控制报文协议ICMP：报告网络故障

网际组管理协议IGMP



1. IP层次结构：

* 层次化IP地址将32位的IP地址分为网络ID和主机ID。
* IP地址的分类：

A类：1 ~ 127（可用地址：1 ~ 126，127为计算机本地环回地址）

B类：128 ~ 191

C类：192 ~ 223



* 特殊的几个地址

127.0.0.1 本地环回地址

169.254.0.0 拨号失败时，windows自动分配的一个临时使用地址

保留的私网地址：

10.0.0.0

172.16.0.0 --- 172.31.0.0

192.168.0.0 --- 192.168.255.0

1. 子网掩码：又叫网络掩码，告诉计算机网络部分和主机部分。同一**网络部分**的计算机可直接ping通，非同一**网络部分**的计算机通信需要经过网关。

【扩展：跟踪路径ping：pathping】

1. 子网划分：划分时主机部分不能全为1或者0

点到点的通信子网掩码为255.255.255.252

1. 变长子网划分：4 8 16 32 64 128 192 224 240 248 252 254
2. 超网：让两个子网的计算机划分在一个网段。（合并网段时，小的是偶数就可合并。比如：192.168.118.0和 192.168.119.0）
3. IP地址决定了数据包最终的地址，MAC地址决定了数据包下一跳给哪个设备。
4. 协议

* ARP协议：通过广播将IP地址解析为MAC地址。

查看保存的IP对应的MAC地址：**arp -a**

修改IP对应的MAC地址：**arp -s 192.168.0.1 80-89-17-b5-73-c0**

* RARP协议：将物理地址请求为IP地址

1. IP数据报(包)：一个IP数据报由首部和数据两部分组成。首部的前一部分是固定长度，共20字节，是所有IP数据报必备的；在首部的固定部分后面是一些可选字段，其长度是可变的。

版本：指明数据报是IPV4或者IPV6

区分服务（QoS）：给数据报一个标记告诉网络实时性要求高低

标识：占16位，数据报计数器

标志：告诉数据报是否分片，与片偏移一起使用。

生存时间（TTL）：每经过一个路由器，TTL减一。

根据TTL，可粗略断定对方操作系统：

TTL = 128 windows

TTL = 64 linux

指定TTLping包：**ping 192.168.80.1 -i 5**

协议：协议号，指明上层协议是什么（ICMP、TCP、UDP等）

首部校验和：供对方检验首部是否正确

可变部分：选项字段，用来支持排错、测量以及安全等措施。（1字节~40个字节）



1. IP转发分组的流程（数据路由）：路由器在不同网段转发数据报。

网咯畅通的条件：能去能回

沿途的路由器必须知道到目标网络下一跳给哪个接口。

1. Windows上的默认路由和网关相同：**route print**

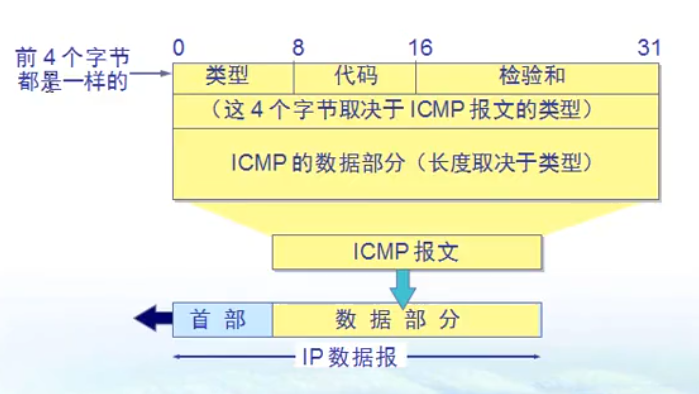
Windows上添加默认路由：**route add 0.0.0.0 mask 0.0.0.0 10.7.86.1**

计算机上最好只有一个网关。

负载均衡：

1. ICMP协议：为了提高IP数据报交付成功的机会，在网际层使用了网际控制报文协议ICMP，ICMP允许主机或者路由器报告差错情况和提供有关异常情况的报告。

ICMP不是高层协议，而是IP层协议。ICMP报文作为IP层数据报的数据，加上数据报的首部，组成IP数据报发送出去。

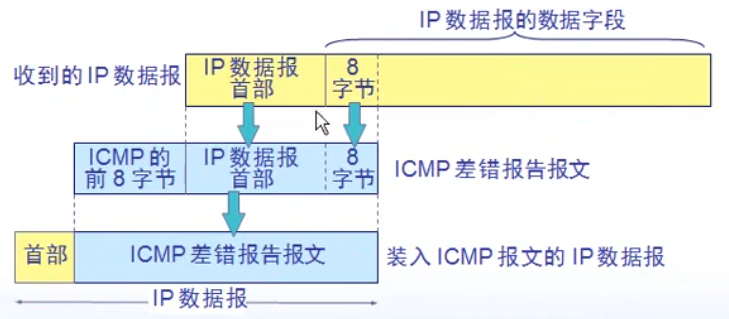


类型：共有两种，为ICMP差错报文和ICMP询问报文。

差错报文有五种：终点不可达、源点抑制、时间超过、参数问题、改变路由（重定向）

询问报文：回送请求和回答报文、时间戳请求和回答报文

差错报告报文的数据字段内容：



1. IGMP组(多)播管理协议：管理组播成员
2. 动态路由协议

* RIP协议：周期性广播[30s]（将自己知道的网段广播给其他路由器）

选择最佳路径时只看跳数（最大跳数为16跳时认为不可达）。

* 内部网关协议OSPF(Open Shortest Path First,开放式最短路径优先协议)

开放式的、度量值使用的是带宽、支持多区域（只支持二级区域）、触发式更新

内部有三个表：邻居表（发送hello包）

链路状态表：将邻居表交换得到

路由表：通过最短路径算法计算带宽形成路由表

不会形成环路。

支持负载均衡、不用UDP而是直接用IP数据报传送、支持可变长子网划分和无分类编址CIDR。

|  |
| --- |
| Router>en  Router#conf t  Router(config)#router ospf 1  Router(config-router)#network 172.16.0.0 0.0.255.255 area 0  Router(config-router)#network 192.168.0.0 0.0.0.3(反转子网掩码) area 0 |

* 外部网关协议BGP

不同自治系统的路由器之间交换路由信息的协议。每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”。该协议只是力求寻找一条能够到达目的网络且比较好的路由，而并非一条最佳路由。

BGP协议交换路由信息量不是很多。

BGP发言人数不多，路由选择相对简单。

BGP协议支持CIDR。

BGP建立时，交换整个路由表，之后只交换部分。

1. VPN：虚拟专用网

隧道技术。

1. 网络地址转换NAT：使内网可以访问到外网

NET的端口映射：使外网可以访问到内网

端口地址转换PAT

## 五、传输层

1. 传输层两个协议应用场景：

* TCP：可靠传输、需要分段、有流量控制功能、编号、丢包后要求重传、要建立会话

例如：QQ传文件、访问网站

* UDP：不可靠传输、一个数据包就能完成数据通信、不建立会话

例如：QQ聊天、多播

1. 传输层和应用层间的关系

http = TCP + 80

https = TCP + 443

ftp = TCP + 21

SMTP = TCP + 25

POP3 = TCP + 110

RDP = TCP + 3389

共享文件夹 = TCP + 445

SQL = TCP + 1433

Telnet = TCP + 23

DNS = UDP + 53 or TCP +53

1. 应用层协议和服务之间的关系：

对外服务运行后在TCP或者UDP某个端口侦听客户端请求。

查看计算机侦听的服务：**netstate -na**

测试远程计算机打开的端口：**telnet 10.7.1.53 21**【需要安装telnet客户端】

**端口代表的是服务**

1. windows防火墙的作用：屏蔽掉外来的请求，可以指定只开某些端口。

防火墙屏蔽不了木马程序(服务)。

ipsec严格控制网络流量

1. TCP协议
2. TCP是面向连接的传输层协议、每个TCP连接只能有两个端点、全双工通信、面向字节流
3. TCP连接的端点叫做套接字socket（IP+端口）。
4. 可靠传输

* 自动重传请求ARQ：停止等待协议（确认丢失、确认迟到、超时重传）

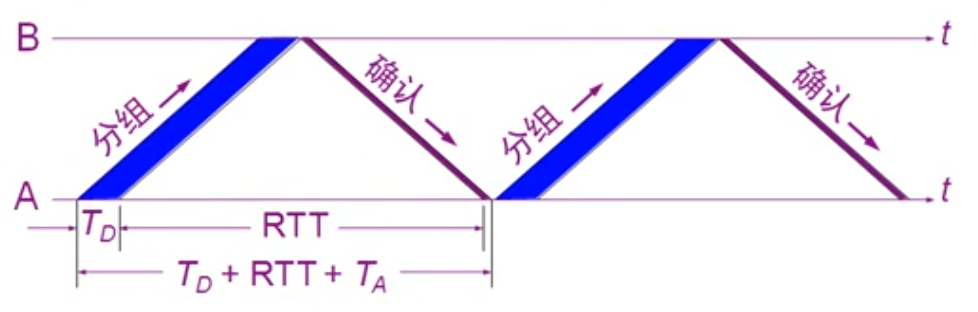
缺点：信道利用率太低

信道利用率：

：发数据包的时间

：传输时间

：等待延迟时间

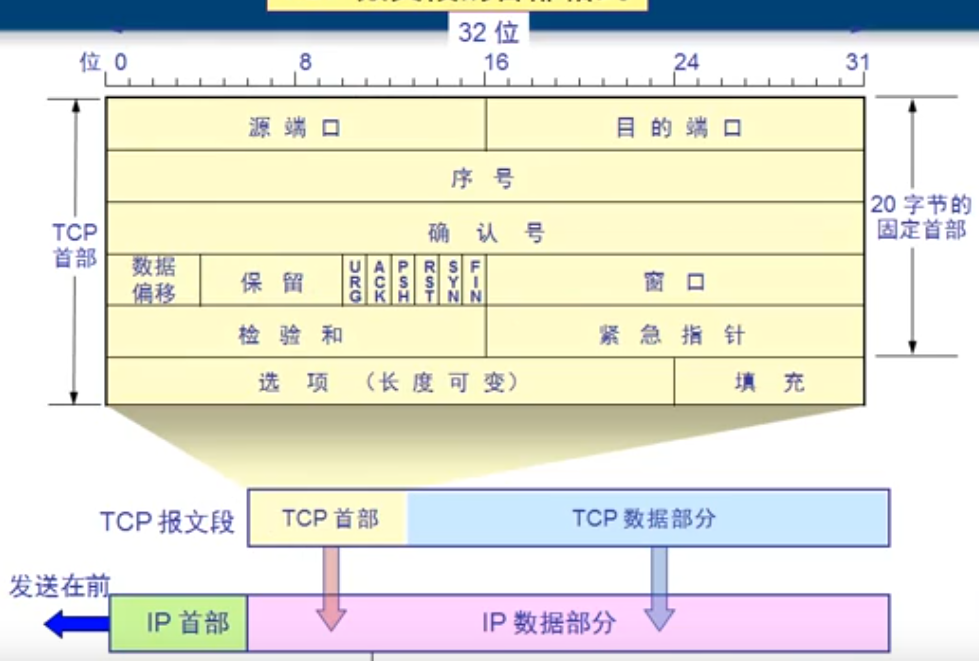


* 流水线传输：发送方连续发送多个分组，不必发完一个分组就停下来等待对方确认。

连续ARQ传输：滑动窗口技术

也可使用累积确认

1. TCP报文段的首部格式



一般数据报没有可变部分。但一些数据报需要做相应的协商，故有可变部分。一些数据报只有固定部分和可变部分，没有数据部分。

序号：当前数据报第一个字节在整个数据报中的序号

确认号：需要的下一个数据报的第一个字节

数据偏移：表示TCP从哪个位置开始是TCP数据部分。（其中，一个1代表4个字节。故首部最多60个字节，可选部分最多40个字节）

保留：无用

URG：1的话告诉计算机优先级比较高，不排队

ACK：0的话确认号无效，1的话确认号有效

SYN：同步时，建立会话请求和同意建议会话请求时是1（SYN攻击：拟造一个假的源地址一直发起建立会话请求；Land攻击原地址和目标地址都为自己一直建立会话）

【发起会话时：序号为0，确认号为0，ACK为0，SYN为1；

同意会话时：序号为0，确认号为1，ACK为1，SYN为1】

PSH：为1代表接收端在器缓存时，先取此数据报

RST：为1代表TCP会话出现了严重的错误，必须重新建立连接。

FIN：为1代表释放连接。

窗口：接收和发送缓存大小(wnd)【扩展：抓包时，MSS表示所能处理的数据报最大的字节】

检验和：检验范围为首部和数据，TCP报文前加12字节的伪首部

紧急指针：只有在URG为1时，表示数据部分中需要紧急处理部分的终止位置

选项：可有可无，规定最大数据报为多大，是否支持选择性确认，时间戳等等。

选项不够4个字节会填充凑够字节

1. TCP可靠传输：以字节为单位的**滑动窗口技术**

SACK：选择性确认，告诉计算机中间有部分数据报丢失，选择性进行重传

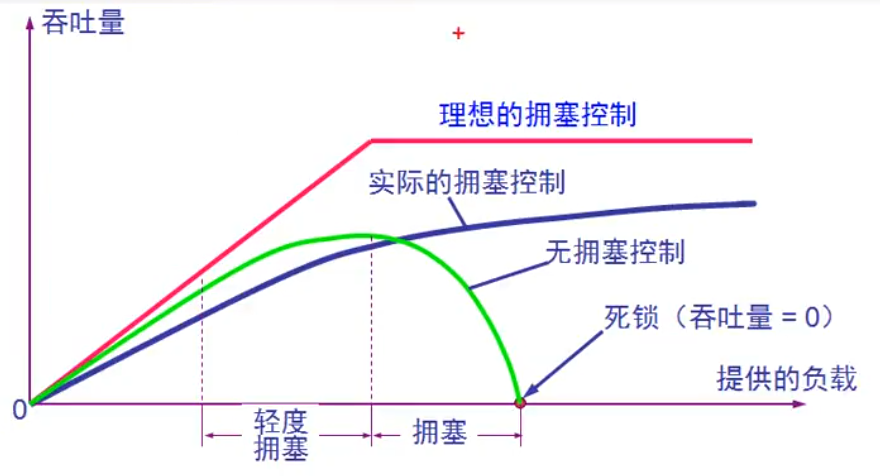
超时重传时间的选择：TCP每发送一个报文段，就对这个报文段设置一次计时器。只要计时器设置的重传时间到但还没有收到确认，就要重传这一报文段。

超时重传时间应略大于上面得出的加权平均往返时间。【RFC2988推荐的值为1/8】

1. 流量控制：接收端通过改变接收窗口大小来通知发送端。
2. TCP拥塞控制：

出现资源拥塞的条件：对资源需求的总和 > 可用资源

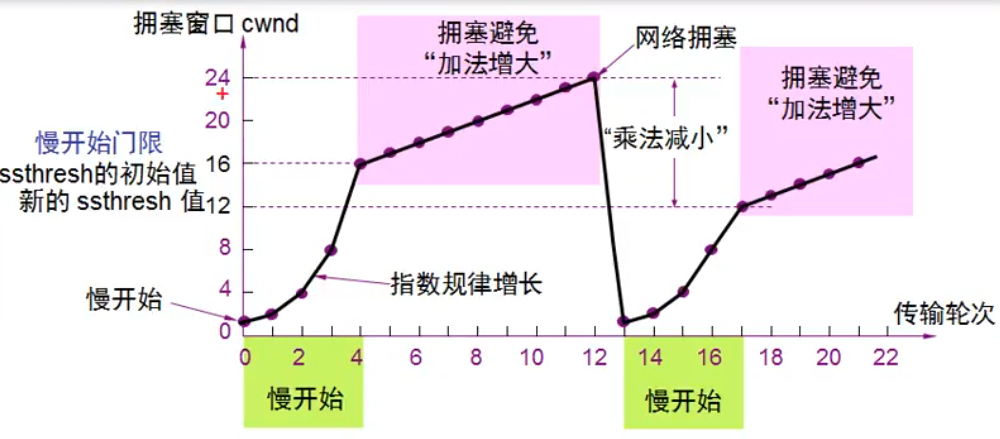
拥塞控制所起到的作用：



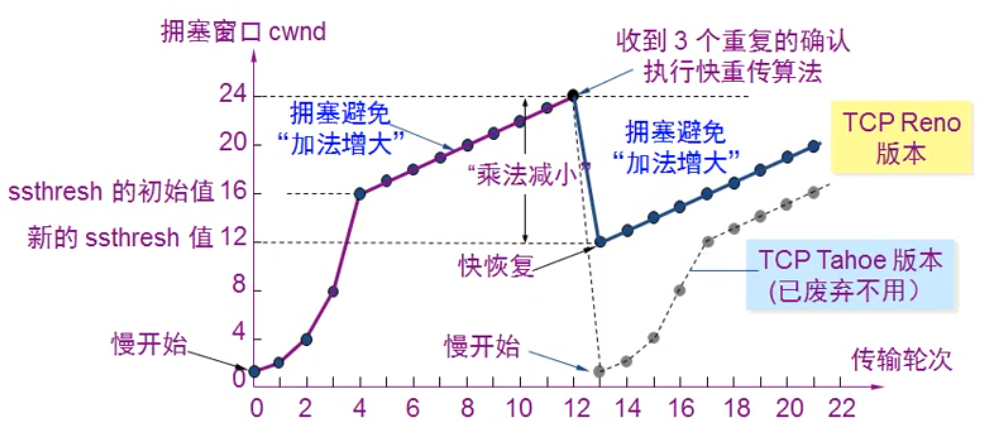
实现：发送方维持拥塞窗口cwnd。（慢开始算法）

发送方控制拥塞窗口的原则是：

* + - 只要网络没有出现拥塞，拥塞窗口就再增大一些，以便把更多的分组发送出去。
    - 只要网络出现拥塞，拥塞窗口就减小一些，以减少注入到网络中的分组数。

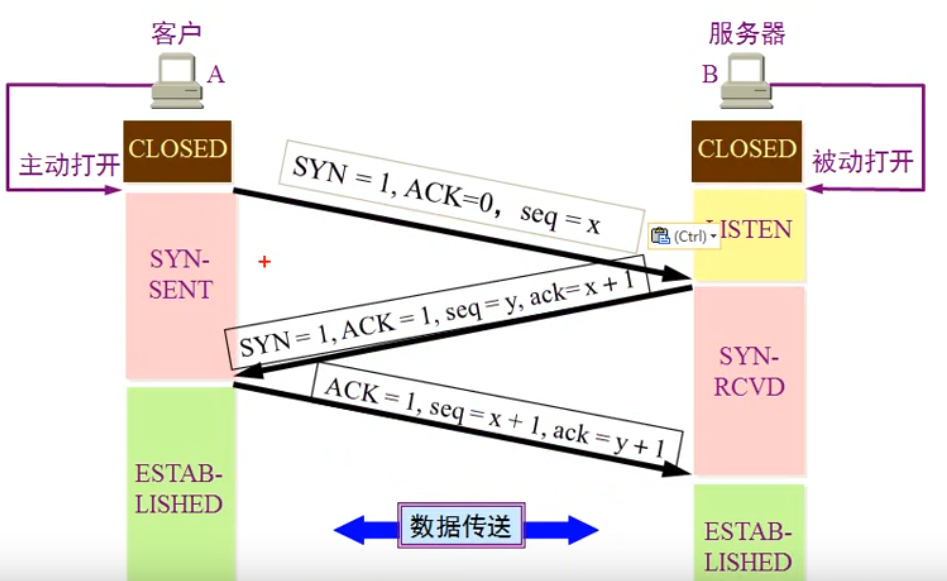


快重传算法、快恢复算法：



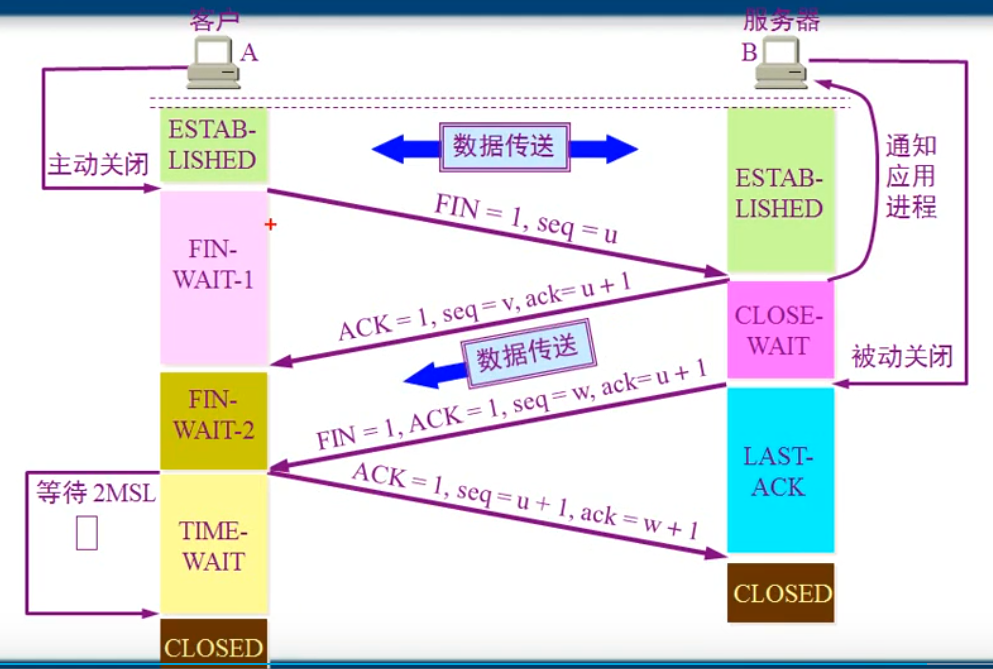
故，发送窗口的上限值 = Min(接受窗口，拥塞窗口)

1. TCP的传输连接管理
2. 传输连接有三个阶段：连接建立、数据传输、连接释放
3. 用三次握手建立TCP连接



第三次握手作用：避免因为路由器路径选择不同而出现延时，以导致B计算机资源浪费，A计算机发出的第三个确认，B计算机认为刚才的确认是有效的。若没有接到第三次确认，B计算机便释放会话。

1. TCP的连接释放



2MSL：4分钟，为了防止最后一个同意包丢失的情况。

## 六、应用层

1. 域名系统DNS

负责将域名解析为IP地址。

域名：

顶级域名：com edu net cn org gov

二级域名、三级域名

DNS服务器：222.222.222.222 电信公司服务器

8.8.8.8 谷歌公司服务器

检查域名解析是否正常：**nslookup，然后可输入需要解析的域名，输入quit来退出**

域名解析的过程：分布式查询，缓存功能

安装DNS服务器：

为了解析内网自己的域名，降低到internet的域名解析流量，域环境

1. 动态主机配置协议DHCP

* DHCP客户端请求IP地址的过程：

DHCP客户端发广播请求IP地址，广播目标IP地址是255.255.255.255，目标MAC地址为FF-FF-FF-FF-FF-FF，DHCP服务器（可能有多个）收到请求后，会从地址池里随机取一个地址进行分配，后客户端进行确认是使用哪个地址，后DHCP把子网掩码网关等再给计算机。

* DHCP服务器必须是静态地址。

释放地址：ipconfig /release

重新获取地址：ipconfig /renew

* 跨网段地址分配，需要在路由器上配置

|  |
| --- |
| ip helper-address 192.168.0.100【服务器的静态IP地址】 |

1. 文件传输协议FTP

TCP控制连接：上传、下载、删除、复制等命令（21端口用来建立控制连接）

TCP数据连接：主动模式、被动模式

主动模式：ftp客户端告诉ftp服务器使用什么端口侦听，ftp服务器和ftp客户端该端口建立连接，ftp服务器源端口为20

被动模式：建立控制连接后，ftp服务器打开一个新窗口，告诉ftp客户端使用该端口来请求，ftp服务器被动等待客户端连接。

FTP服务端如果有防火墙，需要在防火墙上开21和20端口，使用**主动模式**进行数据连接。

1. 远程终端协议telnet

【net user administrator password：更改用户密码

net user han password：添加用户

shutdown -r -t 0：关机】

还可以测试远程某个端口是否打开。telnet 192.168.80.117 80

1. 远程桌面协议RDP

将用户添加到远程桌面组 Remote Desktop Users组便可以进行远程连接了

本地硬盘映射

1. 超文本传输协议HTTP

使用Web代理服务器访问网站：节省内网访问internet的带宽；绕过防火墙；避免跟踪

1. 电子邮件（SMTP，POP3，IMAP）：中继，发送到中继和接收邮件时需要身份验证。

安装POP3和SMTP服务及DNS服务。

在DNS服务上创建域91xueit.com和51cto.com

创建主机记录：mail 192.168.80.100

创建邮件交换记录，MX记录

在POP3服务上创建域名 创建邮箱

在SMTP服务器上创建远程域名\*.com，允许发送邮件到远程。

配置outlookExpress指明收件的服务器和发件的服务器，使用POP3协议收邮件。

### 七、网络安全

1. 计算机安全：数据存储安全、应用程序安全、操作系统安全、网络传输安全、物理安全
2. 计算机网络上的通信面临的威胁：截获、中断、篡改、伪造

截获为被动攻击，其他三种都是主动攻击。

分布式攻击DDos。