###################计算机网络#################

注：网关：帮助两个不能直接互通的网络，进行数据转发

网关实质上是一个网络通向其他网络的[IP地址](https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80)

VLAN(Virtual LAN)翻译成中文是“虚拟局域网”。VlAN所指的LAN特指使用路由器分割网络—也就是广播域

MAC地址（media access control address）,直译为存取控制位址，也称局域网地址，它是一个用来确认网络设备位置的位址，在OSI模型中,第三层网络层负责IP地址第二层数据链路层则负责MAC位址。MAC地址用于在网络中唯一标示一个网卡。

网卡在这里面就充当了一个解码器的作用,将电信号重新转换文文字图像等就是网卡的责任。网卡的其他功能还有监控上传及下载流量,控制网速稳定的作用,它就相当于电脑的港口,所有信息上传到网络之前都要先到网卡这里走一遭

一、

* 网络：由节点和连线构成的图
* 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。
* internet和Internet的区别：

两者的区别嘛！！简单，开头字母前者小写后者大写！！

这只是一方面啦。

* 以小写字母“i”开头的internet：

是指互连网 ，是一个通用名词，它泛指由多个计算机网络互连而成的（计算机）网络。

不一定要采取TCP/IP协议，通信协议（即通信规则）可以是任意的。

* 以大写字母“I”开头的Internet：

指因特网或互联网 ，是一个专有名词，它指当前全球最大的、开放的、由众多网络相互连接而成的特定的计算机网络，它采用TCP/IP协议作为通信的规则，并且前身为ARPAnet。

补充：

* 互联网和计算机网络的联系是什么？

可以这么说：互联网是计算机网络的一种。

互联网是目前技术最为成功、应用最为广泛的计算机网络。

计算机网络按照覆盖范围分的话，包括局广域网、城域网、局域网，互联网是广域网的一种，互联网计算机网络的子集。 互联网可以认为是世界范围内的一个大广域网。

互联网和因特网的关系：

* 互联网包含因特网，因特网包含万维网，凡是能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台机器，不论用何种技术使其彼此通信，也叫互联网。
* 因特网是互联网的一种。它是由上千万台设备组成的互联网。虽然因特网使用TCP/IP协议，但使用TCP/IP协议的网络并不一定是因特网，一个局域网也可以使用TCP/IP协议。

（1）计算机网络是互连的，自治的计算机集合。

互连—互联互通 通信链路

自治—无主从关系

（2）计算机网络的功能

1）数据通信

2）资源共享

3）分布式处理

4）提高可靠性

5）负载均衡

（3）计算机网络的组成

1）组成部分 硬件、软件、协议

C/S方式

P2P方式

边缘部分 用户直接使用

2）工作方式

核心部分 为边缘部服务

通信子网 实现数据通信

3）功能组成

资源子网 实现资源共享/数据处理

应用层

资源子网 表示层

实现资源共享功能的设备和软件的集合

会话层

网络层：路由器

通信子网 数据链路层：交换机，网桥

各种传输介质、通信设备、相应的网络协议组成

物理层：集线器，中继器

4）计算机网络的分类

分布范围：广域网、域域网、局域网、个人局域网

使用者：公用网、专用网

交换技术：电路交换、报文交换、分组交换

拓扑结构：总线型、星型、环型、网状型

传输技术：广播式、点对点

（5）分层结构

1）实体：第n层的活动元素称为n层实体。同一层的实体称为对等实体

2）协议：为进行网络中对等实体数据交换而建立的规则、标准或约定称为网络协议。(水平)

语法：规定传输数据的格式

语义：规定所要完成的功能

同步：规定各种操作的顺序

3）、接口：上层使用下层服务的入口

4）、服务：下层为相邻上层提供的功能调用（垂直）

SDU 服务数据单元：为完成用户要求的功能而应传送的数据

PCI 协议控制信息：控制协议操作的信息

PDU 协议数据单元：对等层次之间传送的数据单位

PCI + SDU = PDU

（6） ISO/OSI参考模型

为了解决计算机网络复杂的大问题 分层结构（按功能）

* **应用层**：用户与网络的界面，所有能和用户交互产生网络流量的程序

典型应用层服务：文件传输（FTP）电子邮件（SMTP）万维网（HTTP）

* **表示层**：用于处理在两个通信系统中交换信息的表示方式

功能一：数据格式变换 （翻译官）

功能二：数据加密解密

功能三：数据压缩和恢复

* **会话层**：向表示层实体/用户进程提供建立连接并在连接上有序地传输数据。这是会话，也是建立同步

功能一：建立、管理、终止会话

功能二：使用校验点可使会话在通信失效时从校验点/同步点继续恢复通信，实现数据同步

* 传输层：负责主机中两个进程的通信，即端到端的通信。传输单位是报文段或用户数据报

功能一：可靠传输、不可靠传输

功能二：差错控制

功能三：流量控制

复用：多个应用层可同时使用下面运输层的服务

分用：运输层把收到的信息分别交付上面的应用层中相应的进程

功能四：复用分用

协议：TCP UDP

* 网络层：主要任务是把分组从源端传到目的端，为分组交换网上的不同主机提供通信服务。网络层传输单位是数据报。

功能一：路由选择 最佳路径

功能二：流量控制

功能三：差错控制

功能四：拥塞控制

协议 ip

* 数据链路层：主要任务是把网络层传下来的数据报组装成帧，数据链路层/链路层的传输单位是帧

功能一：成帧（定义帧的开始和结束）

功能二：差错控制 帧错+位错

功能三：流量控制

功能四：访问（接入控制） 控制对信道的访问

主要协议SDLC HDLC PPP STP

* 物理层：主要任务是在物理媒体上实现比特流的透明传输

物理层传输单位是比特

透明传输：不管所传送的数据是什么样的比特组合，都应当能够在链路上传送

功能一：定义接口特性

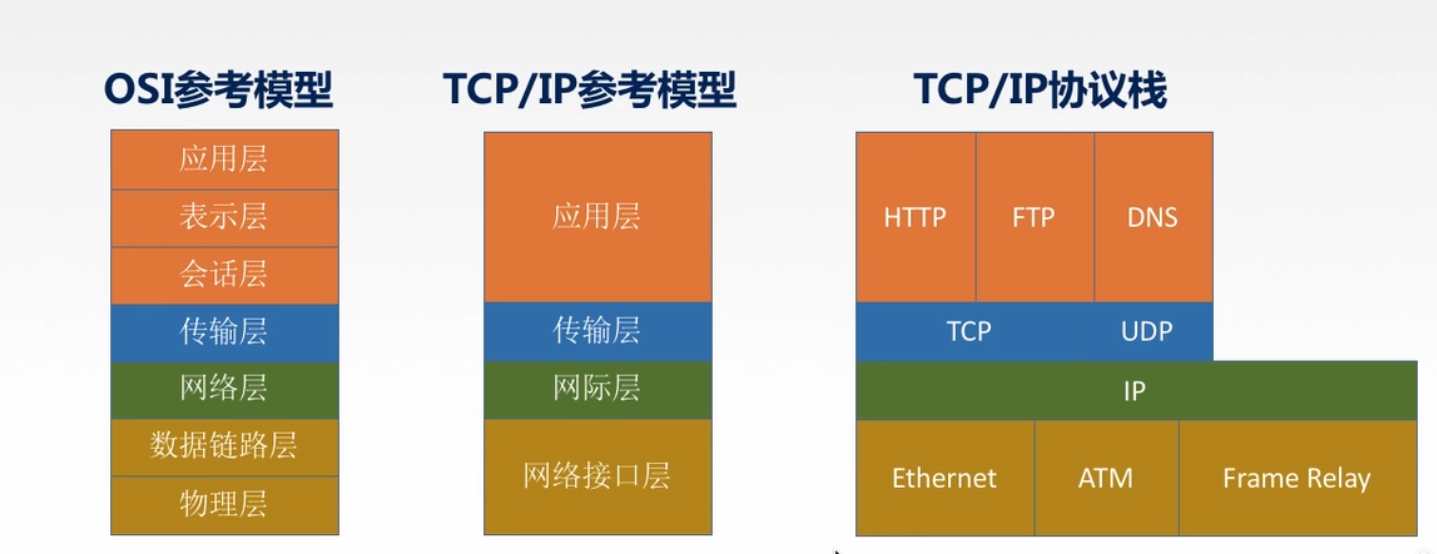
功能二：定义传输模式 单工、半双工、全双工

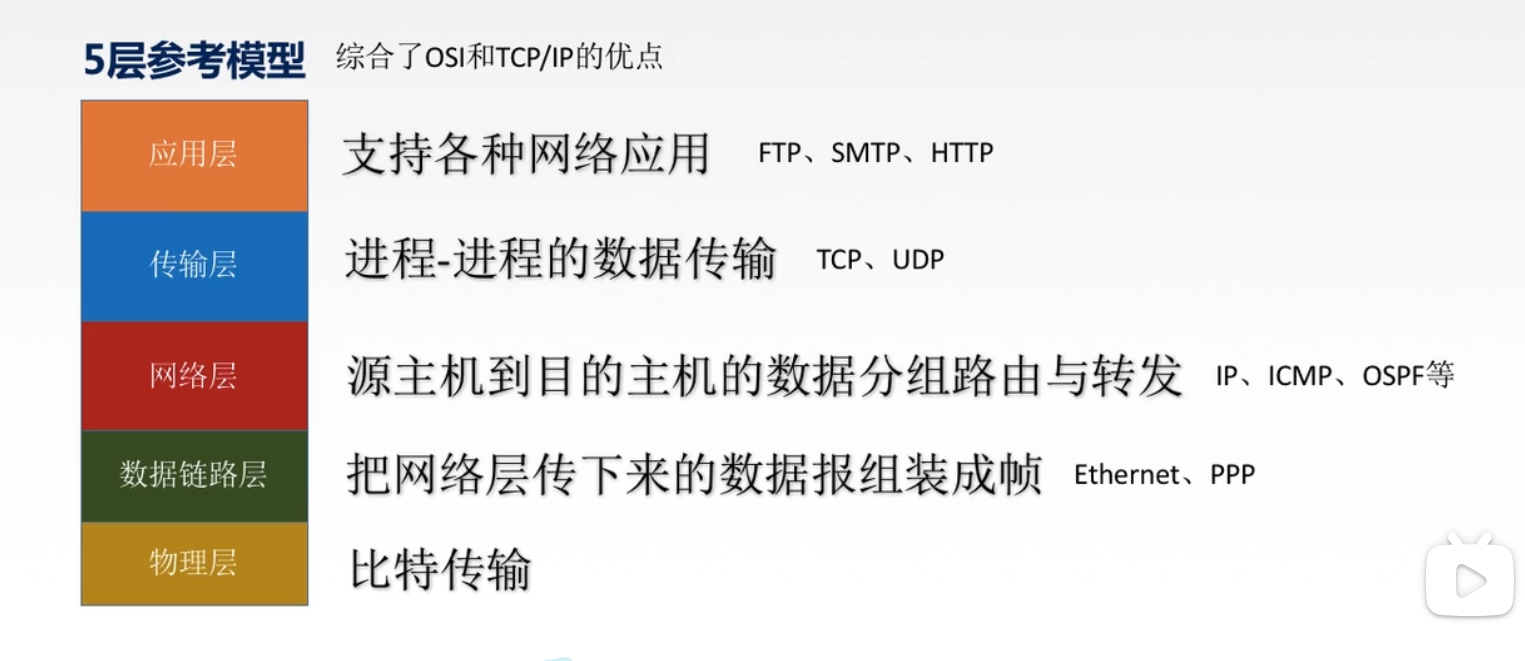
功能三：定义传输速率

功能四：比特同步

功能五：比特编码

（6）TCP/IP参考模型





1. 物理层

三种通信方式

1. 单双工通信 只有一个方向的通信而没有反方向的交互，仅需一条信道
2. 半双工通信 通信的双方都可以发送或接收信息，但任何一方都不能同时发送和接收，需要两条信道
3. 全双工通信 通信双方可以同时发送和接受信息，也需要两条信道

TCP服务

* 可靠的，按顺序地传送数据
* 流量控制
* 拥塞控制

电路交换：独享资源不共享，如果呼叫没有数据发送被分配的资源就会浪费。

电路交换不适合计算机之间的通信：连接时间长计算机之间通信有突发性

网络核心

分组交换：以分组为单位存储—转发

网络带宽资源不在分为一个个片传输时使用全部带宽

主机之间传输的数据被分为一个个分组

资源共享，按需使用

转发之前节点必须收到整个分组，延迟比线路要大，排队时延

电路交换网络 FDM TDM

通信网络

分组交换网络： 虚电路网络： 有连接

数据报网络： 无连接 分组的目标地址决定了下一跳 类似问路 ，在不同的阶段中路由改变

数据链路层：在物理层的服务之上，以相邻两点之间，传输以帧位单位的数据 （点到点的传输）

网络层：在链路层提供的相邻两点之间的传输基础之上，传输以分组为单位端到端的数据传输 （端到端的传输：转发路由）

传输层：区分进程，把网络层提供的不可靠变成可靠

各层次的协议数据单元

* 应用层：报文(message)
* 传输层：报文段(segment)：TCP报文段，UDP数据报
* 网络层：分组packet(如果无连接方式：数据报)
* 数据链路层：帧(frame)
* 物理层：位(bit)

1. 应用层协议原理

进程为了接受报文，必须有一个标识

* 主机：唯一的32位地址
* 所采用的传输层协议：TCP or UDP
* 端口号

传输层提供的服务需要穿过层间的信息

* 层间接口的信息必须要携带的信息
* 要传输的报文：（对于本层来说：SDU）
* 谁传的：对方的应用进程的标识 ip+tcp(udp) 端口
* 传给谁：对方的应用进程的标识 对方的ip+tcp(udp) 端口

传输层实体（tcp udp实体）根据这些信息进行tcp报文段（udp数据报）的封装

对于使用面向连接服务(TCP)的应用而言，套接字是四元组的一个具有本地意义的标识

* 4元组：（源ip、源port、目标ip、目标port）

UDP socket:本地IP 本端口

但是传输报文时，必须需要提供对方的IP port

接受报文时，传输层需要上传对方的ip port

Internet传输层提供的服务

TCP服务：

可靠的传输服务（不丢、不乱，不错） 流量控制 拥塞控制 面向连接

UDP服务：

不可靠传输，无连接，没有流量控制，拥塞控制

TCP UDP都没有加密 明文通过互联网传输

可以通过SSL进行加密

http:超文本传输协议web的应用层协议

客户/服务器模式

使用tcp

http是无状态的：服务器并不维护客户的任何信息

使用cookies 使http是有状态的

**传输层**

复用

从多个套接字接收来自多个进程的报文，根据套接字对应的ip地址和端口号等信息对报文端用头部加以封装（该头部信息用于以后解复用）

解复用

根据报文段的头部信息中的ip地址和端口号将接收到的报文段发给正确的套接字（和对应的应用进程）

udp (user datagram protocol)

* 尽力而为的服务，报文段可能：丢失，送到应用程序的报文乱序
* 无连接：UDP发送端和接收端之间没有握手
* 每个UDP报文段都被独立的处理

tcp

* 点对点：一个发送方，一个接收方
* 可靠的、按顺序的字节流
* 管道化（流水线）tcp拥塞控制和流量控制设置窗口大小
* 发送和接收缓存
* 全双工数据：在统一连接中数据流双向流动，MSS:最大报文段大小
* 面向连接：在数据交换之前，通过握手（交换控制报文）初始化发送方、接收方的状态变量
* 流量控制：发送方不会淹没接收方

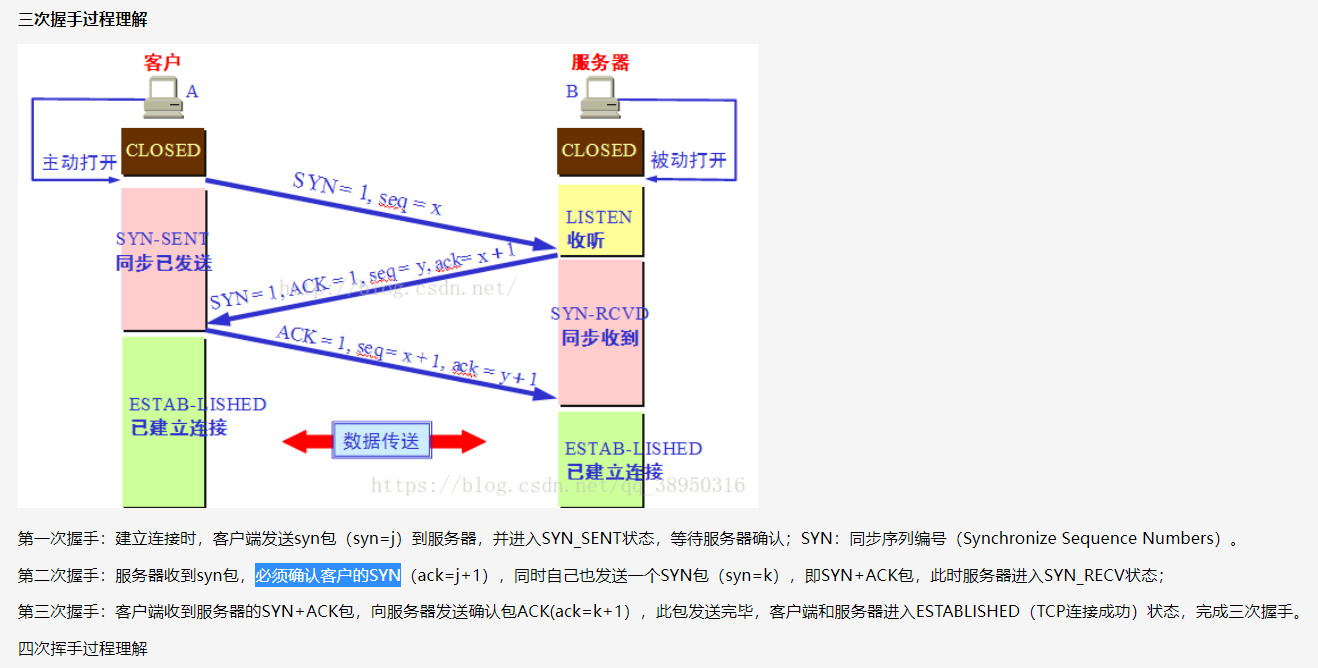
**三次握手**

序列号seq：占四个字节，用来标记数据段的顺序

确认号ack：占四个字节，期待收到对方下一个报文段的第一个数据字节的序号

确认ACK: 占一位，仅当ACK=1时，确认号字段才有效

终止FIN: 用来释放一个连接。FIN=1表示：此报文段的发送方的数据已经发送完毕，并要求释放连接

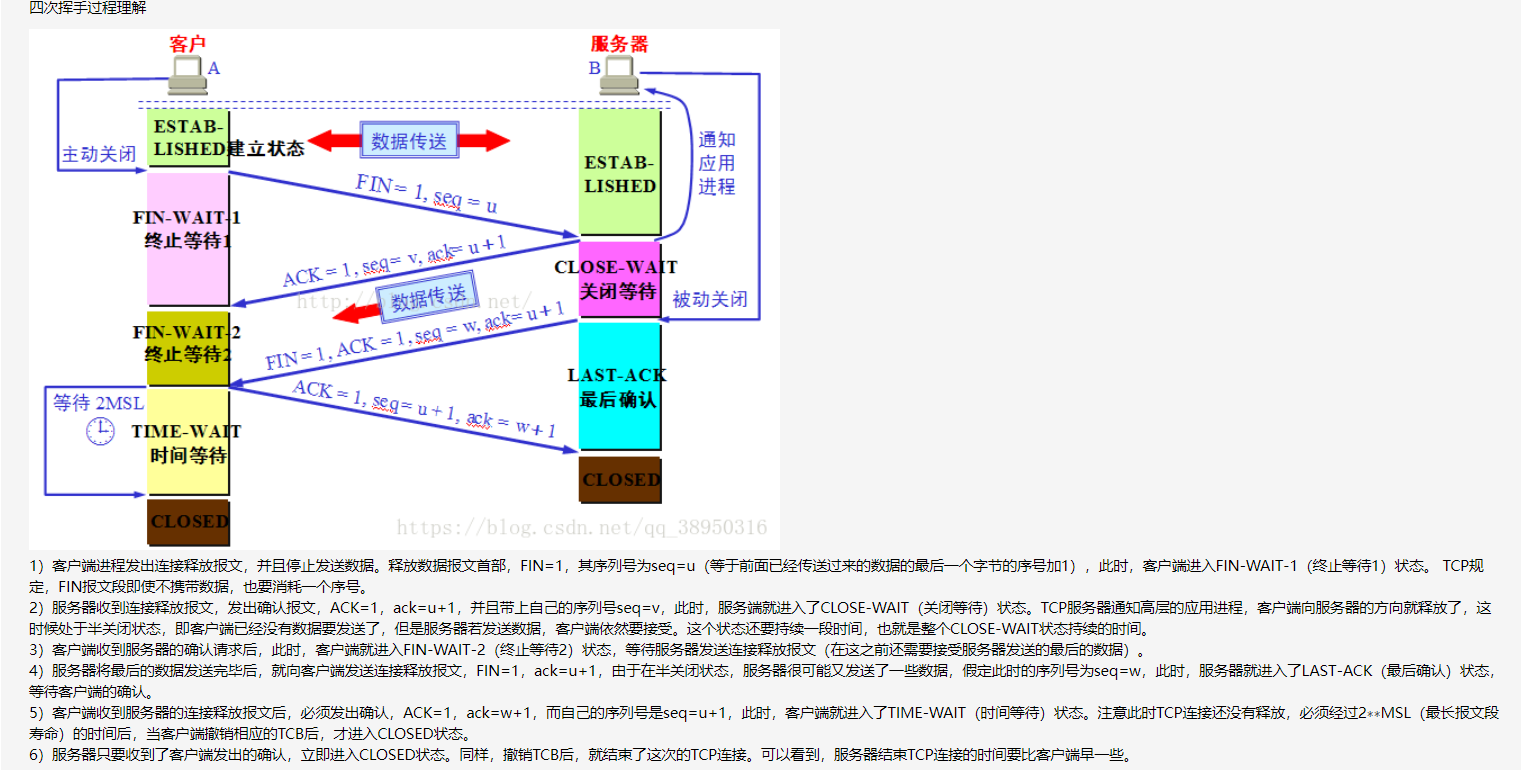


第一次握手：向服务器发送请求建立连接，等待服务器确认

第二次握手：服务器收到请求，然后发送给客户端确认收到请求

第三次握手：客户端收到服务器的响应，然后向服务器发送表示我已收到。然后TCP连接成功，完成三次握手

**四次挥手**



常见面试题

问题1：为什么连接是时候是三次握手，关闭的时候是四次挥手

因为当Server端收到Client端的SYN连接请求报文后，可以直接发送SYN+ACK报文。其中ACK报文是用来应答的，SYN报文是用来同步的，但是关闭连接时，当Server端收到FIN报文时，因为还有数据要处理，所以只能先回复ACK报文，告诉Client,你发的FIN报文我收到了。只有等待我把Server端所有 的报文都发送完了。才能发送FIN报文，因此不能一起发送，故需要四次握手

【问题2】为什么TIME\_WAIT状态需要经过2MSL(最大报文段生存时间)才能返回到CLOSE状态？

答：虽然按道理，四个报文都发送完毕，我们可以直接进入CLOSE状态了，但是我们必须假象网络是不可靠的，有可能最后一个ACK丢失。所以TIME\_WAIT状态就是用来重发可能丢失的ACK报文。在Client发送出最后的ACK回复，但该ACK可能丢失。Server如果没有收到ACK，将不断重复发送FIN片段。所以Client不能立即关闭，它必须确认Server接收到了该ACK。Client会在发送出ACK之后进入到TIME\_WAIT状态。Client会设置一个计时器，等待2MSL的时间。如果在该时间内再次收到FIN，那么Client会重发ACK并再次等待2MSL。所谓的2MSL是两倍的MSL(Maximum Segment Lifetime)。MSL指一个片段在网络中最大的存活时间，2MSL就是一个发送和一个回复所需的最大时间。如果直到2MSL，Client都没有再次收到FIN，那么Client推断ACK已经被成功接收，则结束TCP连接

问题3：为什么不能两次握手进行连接

三次握手完成两个重要的功能，既要双方做好发送数据的准备工作

也要允许双方就初始序列号进行协商，这个序列号在握手过程中被发送给和确认

PS：失效的连接请求：若客户端向服务端发送的连接请求丢失，客户端等待应答超时后就会再次发送连接请求，此时，上一个连接请求就是『失效的』。

若建立连接只需两次握手，客户端并没有太大的变化，仍然需要获得服务端的应答后才进入ESTABLISHED状态，而服务端在收到连接请求后就进入ESTABLISHED状态。此时如果网络拥塞，客户端发送的连接请求迟迟到不了服务端，客户端便超时重发请求，如果服务端正确接收并确认应答，双方便开始通信，通信结束后释放连接。此时，如果那个失效的连接请求抵达了服务端，由于只有两次握手，服务端收到请求就会进入ESTABLISHED状态，等待发送数据或主动发送数据。但此时的客户端早已进入CLOSED状态，服务端将会一直等待下去，这样浪费服务端连接资源。

**网络层：**

**网络层协议IP是TCP/IP体系中两个组重要的协议之一**

与IP协议配套使用的还有三个协议：

地址解析协议ARP

网际控制报文协议ICMP

网际组管理协议IGMP

* 转发：将分组从路由器的输入接口转发到合适的输出接口
* 路由：使用路由算法来决定分组从发送主机到目标接收主机的路径
* 路由选择算法
* 路由选择协议
* 数据平面

本地。每个路由功能

决定从路由器输入端口到的分组如何转发到输出端口

转发功能：

传统方式：基于目标地址+转发表

SDN方式：基于多个字段+流表

* 控制平面
  + 网络范围内的逻辑
  + 决定数据报如何在路由器之间路由，决定数据报从源到目标主机之间的端到端的路径
  + 2个控制平面方法：
    - 传统的路由算法：在路由器中被实现
    - software-defined networking(SDN)在远程的服务中实现

路由结构概况：

高层面通用的路由器体系结构

路由：运行路由选择算法/协议（RIP,OSPF,BGP）生成路由表

转发：从输入到输出链路交换数据报-根据路由表进行分组转发

子网：

一个子网内的节点他们的IP地址的高位部分相同，这些节点构成的网络的一部分叫做子网

无需路由器介入，子网内个各主机可以在物理上相互直接到达

DHCP:DHCP服务器生成DHCP ACK 包含客户端的ip地址，第一跳路由器的ip地址和DNS域名服务器的IP地址

子网掩码：子网掩码可以分离IP地址中的网络地址和主机地址，为什么要分离，因为两台主机通信，首先要判断是否处于同一网段，即网络地址是否相同。如果相同，那么可以把数据包直接发送到目标主机，否则就需要路由网关将数据包转发送达目的地

可以这么简单的理解：A主机要与B主机通信，A和B各自的IP地址与A主机的子网掩码进行And与运算，看得出的结果：

1、结果如果相同，则说明这两台主机是处于同一个网段，这样A可以通过ARP广播发现B的MAC地址，B也可以发现A的MAC地址来实现正常通信。

2、如果结果不同，ARP广播会在本地网关终结，这时候A会把发给B的数据包先发给本地网关，网关再根据B主机的IP地址来查询路由表，再将数据包继续传递转发，最终送达到目的地B。

计算机的网关（Gateway）就是到其他网段的出口，也就是路由器接口IP地址。路由器接口使用的IP地址可以是本网段中任何一个地址，不过通常使用该网段的第一个可用的地址或最后一个可用的地址，这是为了尽可能避免和本网段中的主机地址冲突。

n为1到32的数字，表示子网掩码中网络号的长度，通过n的个数确定子网的主机数=2^(32-n)-2（-2的原因：主机位全为0时表示本网络的网络地址，主机位全为1时表示本网络的广播地址，这是两个特殊地址

**数据链路层：**

**帧：链路层的协议数据单元，封装网络层数据报，核心包含了目标地址，源地址**

**数据链路层再物理层提供的服务基础上向网络层提供服务，其最基本的服务是将源自网络层来的数据可靠的传输到相邻节点的目标机网络层。其主要作用是加强物理层传输原始比特流的功能，将物理层提供的可能出错的的物理连接改造成为逻辑上无差错的数据链路，使之对网络层表现位一条无差错的链路。**

1. 数据链路层主要使用两种信道

* 点对点信道使用一对一的点对点通信方式。主要使用ppp协议
* 广播信道：这种信道使用一对多的广播通信方式，因此过程比较复杂。广播信道上连接是主机很多，因此必须使用专用的共享信道协议来协调这些主机的数据发送。主要使用MAC协议

数据链路层中的MAC子层主要功能。这里所说的“寻址”与“IP地址寻址”是完全不一样的，因为此处所寻找地址是计算机网卡的MAC地址，也称“物理地址”、“硬件地址”，而不是IP地址。在以太网中，采用媒体访问控制（Media Access Control, MAC）地址进行寻址，MAC地址被烧入每个以太网网卡中。这在多点连接的情况下非常必需，因为在这种多点连接的网络通信中，必须保证每一帧都能准确地送到正确的地址，接收方也应当知道发送方是哪一个站。

**数据链路层提供给网络层的服务**

**三种一般服务：**

1. **无确认的无连接服务**

使用场合：错误率很低，或者对数据的完整性要求不高的情况下如语音通话

1. **有确认的无连接服务**

* 无需事先建立连接，但源主机发送的每一帧都要单独确认。若每一帧在指定时间间隔没有收到目标主机发来的确认，则源主机需要重新发送该帧
* 使用场合：不可靠的信道 如无线系统

1. **有确认的有连接服务**

* 需事先建立连接，每一帧都被编号，数据链路层确保发出的每个帧都会被真正的接收到，并保证只接收一次，且按顺序接收。相当于位网络层提供了可靠的比特流传输服务
* 使用场合：长距离且不可靠的信道如卫星信道

数据包在这些节点之间的传递都是由 ARP（Address Resolution Protocol：地址解析协议）负责将IP地址映射到 MAC地址上来完成的。

**三个基本问题：**

* **封装成帧**

数据链路层的发送方应当让接收方的数据链路层知道，所发送的帧是从什么地方开始到什么地方结束

* 透明传输

数据链路层传送的比特组合是不受限制的

* 差错控制

数据链路层必须要有差错检测功能

**差错控制**

**位错：比特位出错**

**差错**

**帧错：丢失，重复，失序**

奇偶校验码

检错编码

循环冗余码CRC

纠错编码 海明码

**流量控制方法：**

**停止等待协议：**每发送一个帧就停止发送，等对方的确认，在收到确认后再发送下一个帧

后退N帧协议（GBN）

**滑动窗口协议**

选择重传协议 （SR）

滑动窗口解决：流量控制，可靠传输（发送方自动重传）

* 在多路访问链路（广播链路）中多个站点同时发送数据，则会产生冲突。这种问题是点到点链路没有的，因此，需要重新考虑数据链路层的功能设计
* OSI把这种访问共享介质的功能划分为数据链路层的一个子层，就是介质访问控制子层（Media Access Control）. 其功能是控制和协调所有站点对共享介质的访问，以避免或减少冲突
* 因为MAC子层不提供可靠的数据传输，所以在MAC子层之上又定义了一个子层，逻辑链路控制子层（Logic link control）,用来为上层协议提供服务
* 以太网：以太网属于数据链路层，是为了实现局域网通信而设计的一种技术，它规定了包括物理层的连线，电子信号和介子访问层的内容，是目前应用最普遍的局域网技术

频分多路复用FDM

时分多路复用TDM

波分多路复用WDM

码分多路复用CDM

静态划分信道

介质访问控制

ALOHA协议

CSMA协议

CSMA/CD协议

CSMA/CA协议

Medium Access Control

动态分配信道

以太网的MAC层协议：

发送帧的方法——CSMA/CD协议：(Carrier Sense MultipleAccess With Collision Detection)

1. 发送数据帧之前先监听信道。如果**信道空闲，立即发送。如果信道忙，则持续监听**，直到信道空闲，立即发送。
2. 边发送边检测冲突。如果发送完毕都没有检测到冲突，则发送成功。
3. 如果检测到冲突，则停止发送，并发送32位干扰位（jamming signal）以加强冲突信号。采用二进制指数退避算法随机延迟一段时间后，转1。

三种CSMA协议：

1. 1-persistent CSMA： 信道空，立即发送；信道忙，持续监听。（以太网）
2. non-persistent CSMA： 信道空，发送；信道忙，随机延迟一段时间
3. p-persistent CSMA:信道空，立即以概率p发送，以概率1-p延迟一个时间槽；信道忙，延迟一个时间槽

虚拟局域网（Virtual Local Area Network，VLAN）是一组逻辑上的设备和用户，通过端口分配、MAC地址分配等方式将同一局域网内的主机划分为不同的区域（VLAN），不同区域之间的主机无法直接通信（即使它们都在同一个有线局域网中），而同一区域内的主机之间可以正常通信，这就好像一个局域网一样，因此叫做虚拟局域网

泛型接口：interface Generator<T>{} 则对应的实现类声明正确的是

class TestGenerator<T> implements Generator{}

class TestGenerator<T> implements Generator<T>{}

class TestGenerator implements Generator<T>{}

class TestGenerator implements Generator{}