OSI，TCP/IP，五层协议的体系结构，以及各层协议

OSI 分层 （7 层）：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 分层（4 层）：网络接口层、 网际层、运输层、 应用层。

五层协议 （5 层）：物理层、数据链路层、网络层、运输层、 应用层。

每一层的协议如下：

物理层：RJ45、CLOCK、IEEE802.3 （中继器，集线器，网关）

数据链路：PPP、FR、HDLC、VLAN、MAC （网桥，交换机）

网络层：IP、ICMP、ARP、RARP、OSPF、IPX、RIP、IGRP、 （路由器）

传输层：TCP、UDP、SPX

会话层：NFS、SQL、NETBIOS、RPC

表示层：JPEG、MPEG、ASII

应用层：FTP、DNS、Telnet、SMTP、HTTP、WWW、NFS

每一层的作用如下：

物理层：通过媒介传输比特,确定机械及电气规范（比特 Bit）

数据链路层：将比特组装成帧和点到点的传递（帧 Frame）

网络层：负责数据包从源到宿的传递和网际互连（包 PackeT）

传输层：提供端到端的可靠报文传递和错误恢复（段 Segment）

会话层：建立、管理和终止会话（会话协议数据单元 SPDU）

表示层：对数据进行翻译、加密和压缩（表示协议数据单元 PPDU）

应用层：允许访问 OSI 环境的手段（应用协议数据单元 APDU）

IP 地址的分类

A 类地址：以 0 开头， 第一个字节范围：0~127（1.0.0.0 - 126.255.255.255）；

B 类地址：以 10 开头， 第一个字节范围：128~191（128.0.0.0 - 191.255.255.255）；

C 类地址：以 110 开头， 第一个字节范围：192~223（192.0.0.0 - 223.255.255.255）；

10.0.0.0—10.255.255.255， 172.16.0.0—172.31.255.255， 192.168.0.0—192.168.255.255。（Internet 上保留地址用于内部）

IP 地址与子网掩码相与得到主机号

ARP 是地址解析协议，简单语言解释一下工作原理。

1：首先，每个主机都会在自己的 ARP 缓冲区中建立一个 ARP 列表，以表示 IP 地址和 MAC 地址之间的对应关系。

2：当源主机要发送数据时，首先检查 ARP 列表中是否有对应 IP 地址的目的主机的 MAC 地址，如果有，则直接发送数据，如果没有，就向本网段的所有主机发送 ARP 数据包，该数据包包括的内容有：**源主机 IP 地址，源主机 MAC 地址，目的主机的 IP 地址**。

3：当本网络的所有主机收到该 ARP 数据包时，首先检查数据包中的 IP 地址是否是自己的 IP 地址，如果不是，则忽略该数据包，如果是，则首先从数据包中取出源主机的 IP 和 MAC 地址写入到 ARP 列表中，如果已经存在，则覆盖，然后将自己的 MAC 地址写入 ARP 响应包中，告诉源主机自己是它想要找的 MAC 地址。

4：源主机收到 ARP 响应包后。将目的主机的 IP 和 MAC 地址写入 ARP 列表，并利用此信息发送数据。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败。

广播发送 ARP 请求，单播发送 ARP 响应。

各种协议

ICMP 协议： 因特网控制报文协议。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。

TFTP 协议： 是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

HTTP 协议： 超文本传输协议，是一个属于应用层的面向对象的协议，由于其简捷、快速的方式，适用于分布式超媒体信息系统。

DHCP 协议： 动态主机配置协议，是一种让系统得以连接到网络上，并获取所需要的配置参数手段。

NAT 协议：网络地址转换属接入广域网(WAN)技术，是一种将私有（保留）地址转化为合法 IP 地址的转换技术，

DHCP 协议：一个局域网的网络协议，使用 UDP 协议工作，用途：给内部网络或网络服务供应商自动分配 IP 地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。

描述：RARP

RARP 是逆地址解析协议，作用是完成硬件地址到 IP 地址的映射，主要用于无盘工作站，因为给无盘工作站配置的 IP 地址不能保存。工作流程：在网络中配置一台 RARP 服务器，里面保存着 IP 地址和 MAC 地址的映射关系，当无盘工作站启动后，就封装一个 RARP 数据包，里面有其 MAC 地址，然后广播到网络上去，当服务器收到请求包后，就查找对应的 MAC 地址的 IP 地址装入响应报文中发回给请求者。因为需要广播请求报文，因此 RARP 只能用于具有广播能力的网络。

TCP 三次握手和四次挥手的全过程

三次握手：

第一次握手：客户端发送 syn 包(syn=x)到服务器，并进入 SYN_SEND 状态，等待服务器确认；

第二次握手：服务器收到 syn 包，必须确认客户的 SYN（ack=x+1），同时自己也发送一个 SYN 包（syn=y），即 SYN+ACK 包，此时服务器进入 SYN_RECV 状态；

第三次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(ack=y+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成三次握手。

握手过程中传送的包里不包含数据，三次握手完毕后，客户端与服务器才正式开始传送数据。理想状态下，TCP 连接一旦建立，在通信双方中的任何一方主动关闭连接之前，TCP 连接都将被一直保持下去。

四次握手

与建立连接的“三次握手”类似，断开一个 TCP 连接则需要“四次握手”。

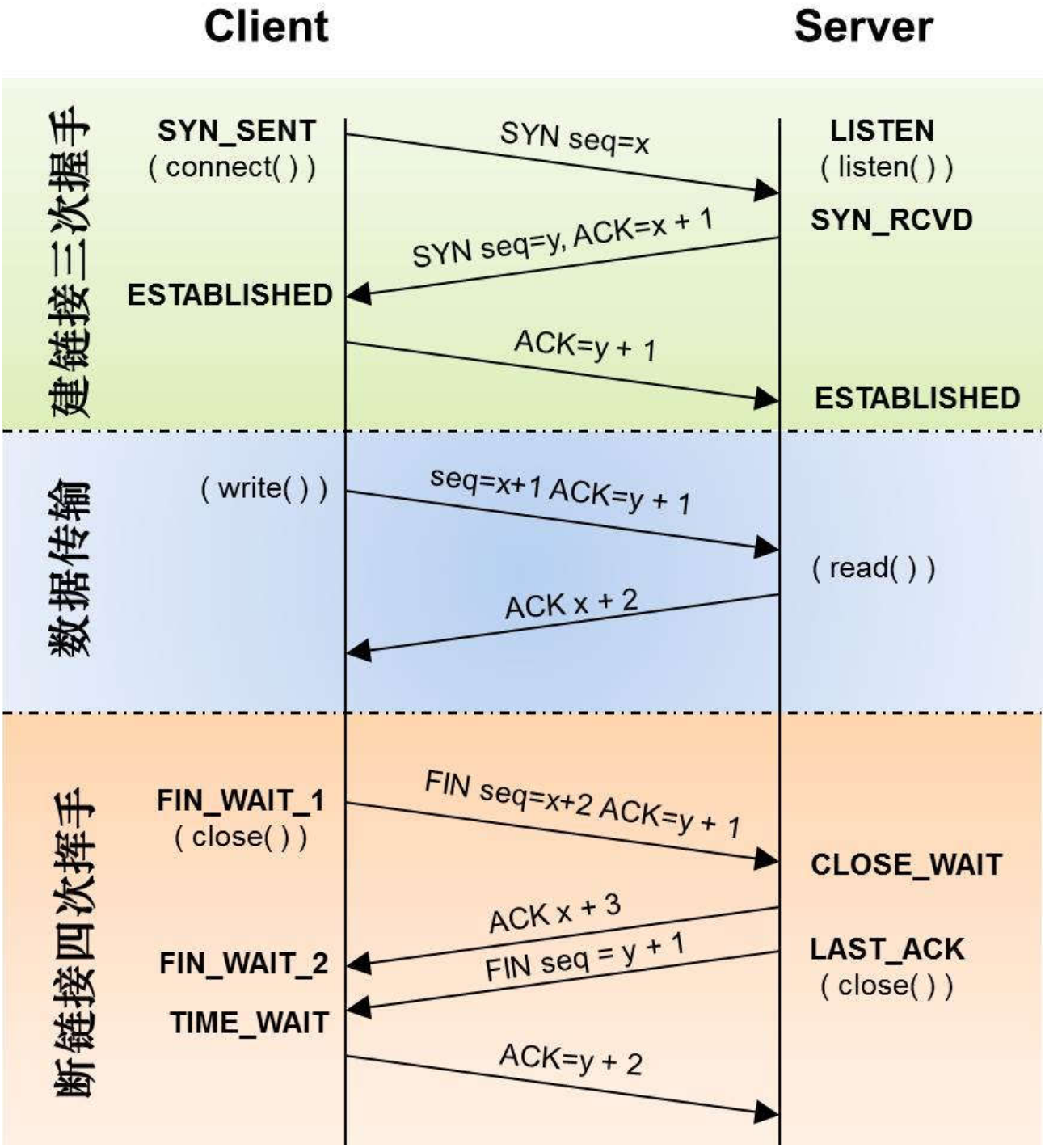
第一次挥手：主动关闭方发送一个 FIN，用来关闭主动方到被动关闭方的数据传送，也就是主动关闭方告诉被动关闭方：我已经不 会再给你发数据了(当然，在 fin 包之前发送出去

的数据，如果没有收到对应的 ack 确认报文，主动关闭方依然会重发这些数据)，但是，此时主动关闭方还可 以接受数据。

第二次挥手：被动关闭方收到 FIN 包后，发送一个 ACK 给对方，确认序号为收到序号+1（与 SYN 相同，一个 FIN 占用一个序号）。

第三次挥手：被动关闭方发送一个 FIN，用来关闭被动关闭方到主动关闭方的数据传送，也就是告诉主动关闭方，我的数据也发送完了，不会再给你发数据了。

第四次挥手：主动关闭方收到 FIN 后，发送一个 ACK 给被动关闭方，确认序号为收到序号+1，至此，完成四次挥手。



在浏览器中输入 www.baidu.com 后执行的全部过程

1、客户端浏览器通过 DNS 解析到 www.baidu.com 的 IP 地址 220.181.27.48，通过这个 IP 地址找到客户端到服务器的路径。客户端浏览器发起一个 HTTP 会话到 220.161.27.48，然后通过 TCP 进行封装数据包，输入到网络层。

2、在客户端的传输层，把 HTTP 会话请求分成报文段，添加源和目的端口，如服务器使用 80 端口监听客户端的请求，客户端由系统随机选择一个端口如 5000，与服务器进行交换，服务器把相应的请求返回给客户端的 5000 端口。然后使用 IP 层的 IP 地址查找目的端。

3、客户端的网络层不用关系应用层或者传输层的东西，主要做的是通过查找路由表确定如何到达服务器，期间可能经过多个路由器，这些都是由路由器来完成的工作，我不作过多的描述，无非就是通过查找路由表决定通过那个路径到达服务器。

4、客户端的链路层，包通过链路层发送到路由器，通过邻居协议查找给定 IP 地址的 MAC 地址，然后发送 ARP 请求查找目的地址，如果得到回应后就可以使用 ARP 的请求应答交换的 IP 数据包现在就可以传输了，然后发送 IP 数据包到达服务器的地址。

TCP 和 UDP 的区别？

TCP 提供面向连接的、可靠的数据流传输，而 UDP 提供的是非面向连接的、不可靠的数据流传输。

TCP 传输单位称为 TCP 报文段，UDP 传输单位称为用户数据报。

TCP 注重数据安全性，UDP 数据传输快，因为不需要连接等待，少了许多操作，但是其安全性却一般。

TCP 对应的协议和 UDP 对应的协议

TCP 对应的协议：

（1） **FTP**：定义了文件传输协议，使用 **21** 端口。

（2） **Telnet**：一种用于远程登陆的端口，使用 **23** 端口，用户可以以自己的身份远程连接到计算机上，可提供基于 DOS 模式下的通信服务。

（3） **SMTP**：邮件传送协议，用于发送邮件。服务器开放的是 **25** 号端口。

（4） **POP3**：它是和 SMTP 对应，POP3 用于接收邮件。POP3 协议所用的是 **110** 端口。

（5）**HTTP**：是从 Web 服务器传输超文本到本地浏览器的传送协议。

UDP 对应的协议：

（1） **DNS**：用于域名解析服务，将域名地址转换为 IP 地址。DNS 用的是 **53** 号端口。

（2） **SNMP**：简单网络管理协议，使用 **161** 号端口，是用来管理网络设备的。由于网络设备很多，无连接的服务就体现出其优势。

（3） **TFTP**(Trival File Tran 敏感词 er Protocal)，简单文件传输协议，该协议在熟知端口 **69** 上使用 UDP 服务。

DNS 域名系统，简单描述其工作原理。

当 DNS 客户机需要在程序中使用名称时，它会查询 DNS 服务器来解析该名称。客户机发送的每条查询信息包括三条信息：包括：指定的 DNS 域名，指定的查询类型，DNS 域名的指定类别。基于 UDP 服务，端口 53. 该应用一般不直接为用户使用，而是为其他应用服务，如 HTTP，SMTP 等在其中需要完成主机名到 IP 地址的转换。

面向连接和非面向连接的服务的特点是什么？

面向连接的服务，通信双方在进行通信之前，要先在双方建立起一个完整的可以彼此沟通的通道，在通信过程中，整个连接的情况一直可以被实时地监控和管理。

非面向连接的服务，不需要预先建立一个联络两个通信节点的连接，需要通信的时候，发送节点就可以往网络上发送信息，让信息自主地在网络上去传，一般在传输的过程中不再加以监控。

TCP 的三次握手过程？为什么会采用三次握手，若采用二次握手可以吗？

答：建立连接的过程是利用客户服务器模式，假设主机 A 为客户端，主机 B 为服务器端。

（1）TCP 的三次握手过程：主机 A 向 B 发送连接请求；主机 B 对收到的主机 A 的报文段进行确认；主机 A 再次对主机 B 的确认进行确认。

（2）采用三次握手是为了防止失效的连接请求报文段突然又传送到主机 B，因而产生错误。失效的连接请求报文段是指：主机 A 发出的连接请求没有收到主机 B 的确认，于是经过一段时间后，主机 A 又重新向主机 B 发送连接请求，且建立成功，顺序完成数据传输。考虑这样一种特殊情况，主机 A 第一次发送的连接请求并没有丢失，而是因为网络节点导致延迟达到主机 B，主机 B 以为是主机 A 又发起的新连接，于是主机 B 同意连接，并向主机 A 发回确认，但是此时主机 A 根本不会理会，主机 B 就一直在等待主机 A 发送数据，导致主机 B 的资源浪费。

（3）采用两次握手不行，原因就是上面说的实效的连接请求的特殊情况。

端口及对应的服务？

服务	端口号	服务	端口号
FTP	21	SSH	22
telnet	23	SMTP	25
Domain(域名服务器)	53	HTTP	80

IP 数据包的格式

POP3	110	NTP（网络时间协议）	123
MySQL 数据库服务	3306	Shell 或 cmd	514
POP-2	109	SQL Server	1433

IP 数据报由**首部** 和**数据** 两部分组成。首部由**固定部分和可选部分** 组成。**首部的固定部分有 20 字节**。可选部分的长度变化范围为 1——40 字节。固定部分的字段：

字段名	位数（bit）	字段名	位数
版本	4 Ipv4	首部长度	4（表示的最大数为 15 个单位，一个单位表示 4 字节）
服务类型	8 以前很少用	总长度	16 （首部和数据部分的总长度，因此数据报的最大长度为 65535 字节，即 64KB，但是由于链路层的 MAC 都有一定的最大传输单元，因此 IP 数据报的长度一般都不会有理论上的那么大，如果超出了 MAC 的最大单元就会进行分片）
标识	16 （相同的标识使得分片后的数据报片能正确的重装成原来的数据报）	标志	3 （最低位 MF=1 表示后面还有分片，MF=0 表示这是若干个数据报片的最后一个中间位 DF=0 才允许分片）
片偏移	片偏移指出较长的分组在分片后，某片在原分组中的相对位置，都是 8 字节的偏移位置	生存时间	数据报在网络中的生存时间，指最多经过路由器的跳数
协议	8 （指出该数据报携带的数据是何种协议，以使得目的主机的 IP 层知道应将数据部分上交给哪个处理程序）如 ICMP=1 IGMP=2 TCP=6 EGP=8 IGP=9 UDP=17 Ipv6=41 OSPF=89	首部校验和	这个部分只校验首部，不包括数据部分，计算方法：将首部划分为多个 16 位的部分，然后每个 16 位部分取反，然后计算和，再将和取反放到首部校验和。接收方收到后按同样的方法划

			分，取反，求和，在取反，如果结果为零，则接收，否则就丢弃
源地址	32	目的地址	32

TCP 数据报的格式？

一个 TCP 报文段分为首部和数据两部分。首部由固定部分和选项部分组成，固定部分是 20 字节。TCP 首部的最大长度为 60。首部固定部分字段：

字段名	字节（Byte）	字段名	字节（Byte）
源端口	2	目的端口	2
序号	4	确认号	4，是期望收到对方的下一个报文段的数据的第一个字节的序号
数据偏移	4bit 指出 TCP 报文段的数据起始处距离 TCP 报文段的起始有多远	保留	6bit
紧急比特 URG		确认比特 ACK	只有当 ACK=1 时，确认号字段才有效
推送比特 PSH		复位比特 RST	
同步比特 SYN		终止比特 FIN	
窗口	2	检验和	2（包括首部和数据两部分，同时还要加 12 字节的伪首部进行校验和计算）
选项	长度可变（范围 1——40）		

TCP 的 12 字节伪首部：

源 IP 地址（4）	目的 IP 地址（4）	0 (1)	6(1) 代表这是 TCP，IP 协议中提到过	TCP 长度（2）

TCP 数据报的格式？

用户数据报 UDP 由首部和数据部分组成。首部只有 8 个字节，由 4 个字段组成，每个字段都是两个字节。

字段名	字节	字段名	字节
源端口	2	目的端口	2
长度	2	检验和	2 （检验首部和数据，加 12 字节的伪首部）

UDP 的 12 字节伪首部：

源 IP 地址（4）	目的 IP 地址（4）	0 (1)	17(1) 代表这是 UDP	UDP 长度（2）

以太网 MAC 帧格式？

前导码	前定界符	目的地址	源目的地址	长度字段	数据字段	校验字段
7B	1B	6B	6B	2B	46-1500	4B

了解交换机、路由器、网关的概念，并知道各自的用途

1）交换机

在计算机网络系统中，交换机是针对共享工作模式的弱点而推出的。交换机拥有一条高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条背 部总线上，当控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的 MAC（网卡的硬件地址）的 NIC（网卡）挂接在哪个端口上，通过内部 交换矩阵迅速将数据包传送到目的端口。目的 MAC 若不存在，交换机才广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部地址表 中。

交换机工作于 OSI 参考模型的第二层，即数据链路层。交换机内部的 CPU 会在每个端口成功连接时，通过 ARP 协议学习它的 MAC 地址，保存成一张 ARP 表。在今后的通讯中，发往该 MAC 地址的数据包将仅送往其对应的端口，而不是所有的端口。因此，交换机可用于划分数据链路层广播，即冲突域；但它不 能划分网络层广播，即广播域。

交换机被广泛应用于二层网络交换，俗称“二层交换机”。

交换机的种类有：二层交换机、三层交换机、四层交换机、七层交换机分别工作在 OSI 七层模型中的第二层、第三层、第四层盒第七层，并因此而得名。

2）路由器

路由器（**Router**）是一种计算机网络设备，提供了路由与转送两种重要机制，可以决定数据包从来源端到目的端所经过 的路由路径（host 到 host 之间的传输路径），这个过程称为路由；将路由器输入端的数据包移送至适当的路由器输出端(在路由器内部进行)，这称为转 送。路由工作在 OSI 模型的第三层——即网络层，例如网际协议。

路由器的一个作用是连通不同的网络，另一个作用是选择信息传送的线路。 路由器与交换器的差别，路由器是属于 OSI 第三层的产品，交换器是 OSI 第二层的产品(这里特指二层交换机)。

3）网关

网关（Gateway），**网关**顾名思义就是连接两个网络的设备，区别于路由器（由于历史的原因，许多有关 TCP/IP 的文献曾经把网络层使用的路由器（Router）称为网关，在今天很多局域网采用都是路由来接入网络，因此现在通常指的网关就是路由器的 IP），经常在家 庭中或者小型企业网络中使用，用于连接局域网和 Internet。 网关也经常指把一种协议转成另一种协议的设备，比如语音网关。

在传统 TCP/IP 术语中，网络设备只分成两种，一种为网关（gateway），另一种为主机（host）。网关能在网络间转递数据包，但主机不能 转送数据包。在主机（又称终端系统，end system）中，数据包需经过 TCP/IP 四层协议处理，但是在网关（又称中介系统，intermediate system）只需要到达网际层（Internet layer），决定路径之后就可以转送。在当时，网关 （gateway）与路由器（router）还没有区别。

在现代网络术语中，网关（gateway）与路由器（router）的定义不同。网关（gateway）能在不同协议间移动数据，而路由器（router）是在不同网络间移动数据，相当于传统所说的 IP 网关（IP gateway）。

网关是连接两个网络的设备，对于语音网关来说，他可以连接 PSTN 网络和以太网，这就相当于 VOIP，把不同电话中的模拟信号通过网关而转换成数字信号，而且加入协议再去传输。在到了接收端的时候再通过**网关**还原成模拟的电话信号，最后才能在电话机上听到。

对于以太网中的**网关**只能转发三层以上数据包，这一点和路由是一样的。而不同的是**网关**中并没有路由表，他只能按照预先设定的不同网段来进行转发。网关最重要的一点就是端口映射，子网内用户在外网看来只是外网的 IP 地址对应着不同的端口，这样看来就会保护子网内的用户。