

网络七层协议

网络七层协议由下往上分别为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

其中物理层、数据链路层和网络层通常被称作媒体层，是网络工程师所研究的对象；

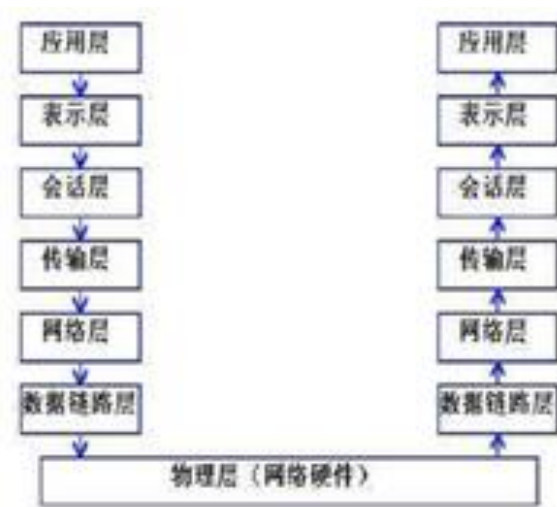
传输层、会话层、表示层和应用层则被称作主机层，是用户所面向和关心的内容。

HTTP协议对应于应用层，TCP协议对应于传输层，IP协议对应于网络层，HTTP协议是基于TCP连接的,三者本质上没有可比性。

TCP/IP是传输层协议，主要解决数据如何在网络中传输；

而HTTP是应用层协议，主要解决如何包装数据。

Socket是应用层与TCP/IP协议族通信的中间软件抽象层，是它的一组接口。



TCP/IP五层模型

TCP/IP五层模型的协议分为：应用层、传输层、网络层、数据链路层和物理层。

中继器、集线器、还有我们通常说的双绞线也工作在物理层；

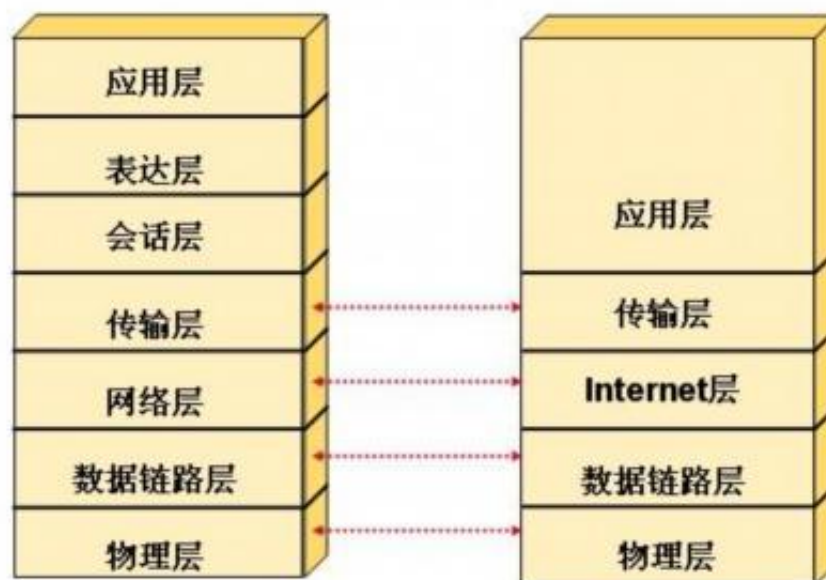
网桥（现已很少使用）、以太网交换机（二层交换机）、网卡（其实网卡是一半工作在物理层、一半工作在数据链路层）在数据链路层；

路由器、三层交换机在网络层；

传输层主要是四层交换机、也有工作在四层的路由器。

TCP/IP协议中的应用层处理七层模型中的第五层、第六层和第七层的功能。

TCP/IP协议中的传输层并不能总是保证在传输层可靠地传输数据包，而七层模型可以做到。TCP/IP协议还提供一项名为UDP（用户数据报协议）的选择。UDP不能保证可靠的数据包传输。



TCP：面向连接、传输可靠(保证数据正确性,保证数据顺序)、用于传输大量数据(流模式)、速度慢，建立连接需要开销较多(时间，系统资源)。

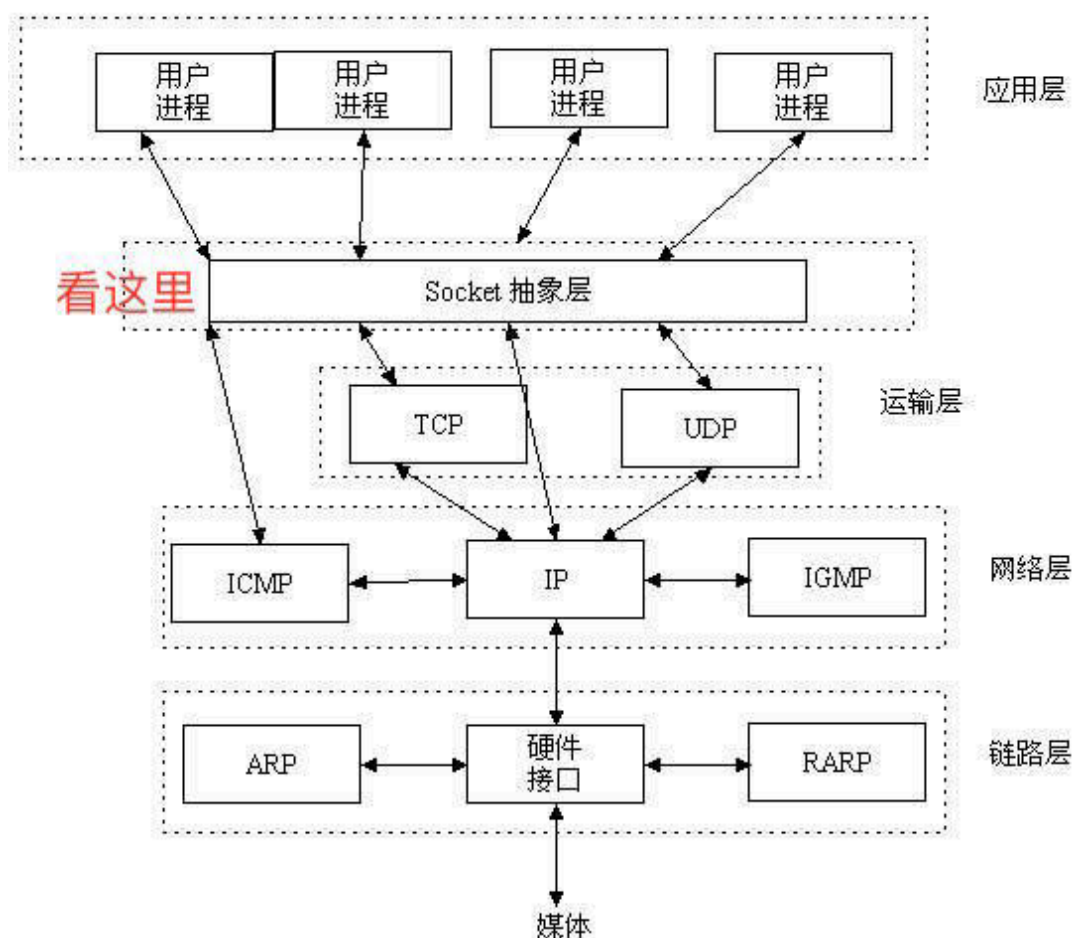
UDP：面向非连接、传输不可靠、用于传输少量数据(数据包模式)、速度快。

TCP是一种流模式的协议，UDP是一种数据报模式的协议。

在传输数据时，可以只使用传输层（TCP/IP），但是那样的话，由于没有应用层，便无法识别数据内容，如果想要使传输的数据有意义，则必须使用应用层协议（HTTP、FTP、TELNET等），也可以自己定义应用层协议。

WEB使用Tcp作传输层协议，以封装HTTP文本信息，然后使用TCP/IP做传输层协议将它发送到网络上。

Socket是对TCP/IP协议的封装，**Socket**本身并不是协议，而是一个调用接口（API），通过**Socket**，我们才能使用TCP/IP协议。



TCP连接

要想明白Socket连接，先要明白TCP连接。手机能够使用联网功能是因为手机底层实现了TCP/IP协议，可以使手机终端通过无线网络建立TCP连接。TCP协议可以对上层网络提供接口，使上层网络数据的传输建立在“无差别”的网络之上。

建立起一个TCP连接需要经过“三次握手”：

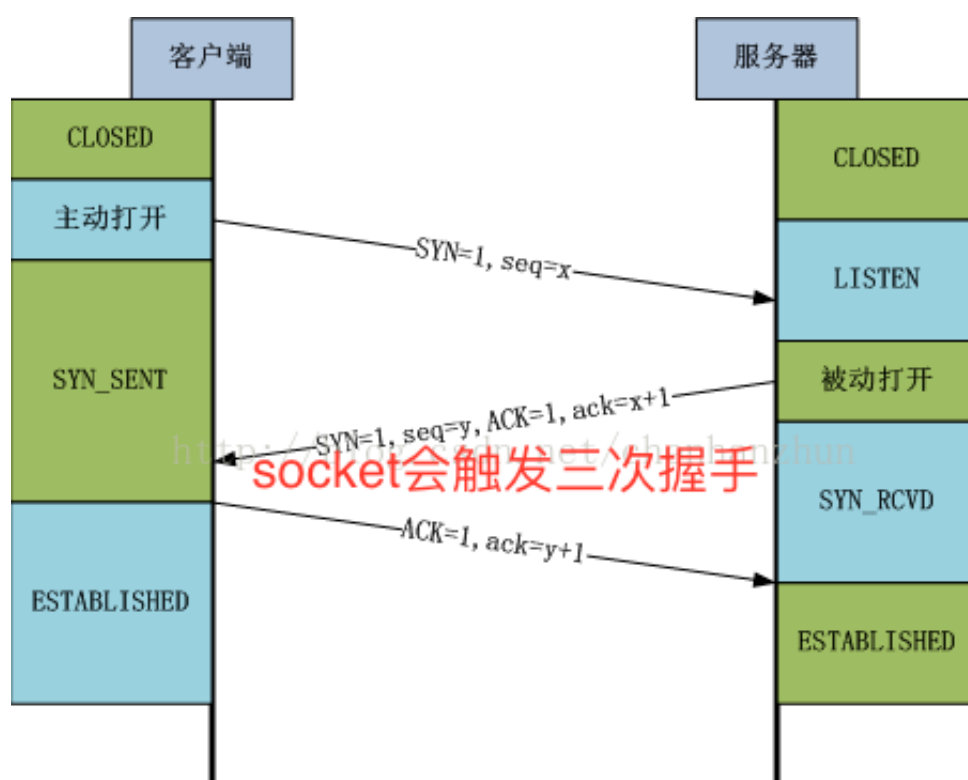
第一次握手：客户端发送syn包($\text{syn}=j$)到服务器，并进入SYN_SEND状态，等待服务器确认；

第二次握手：服务器收到syn包，必须确认客户的SYN ($\text{ack}=j+1$)，同时自己也发送一个SYN包 ($\text{syn}=k$)，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

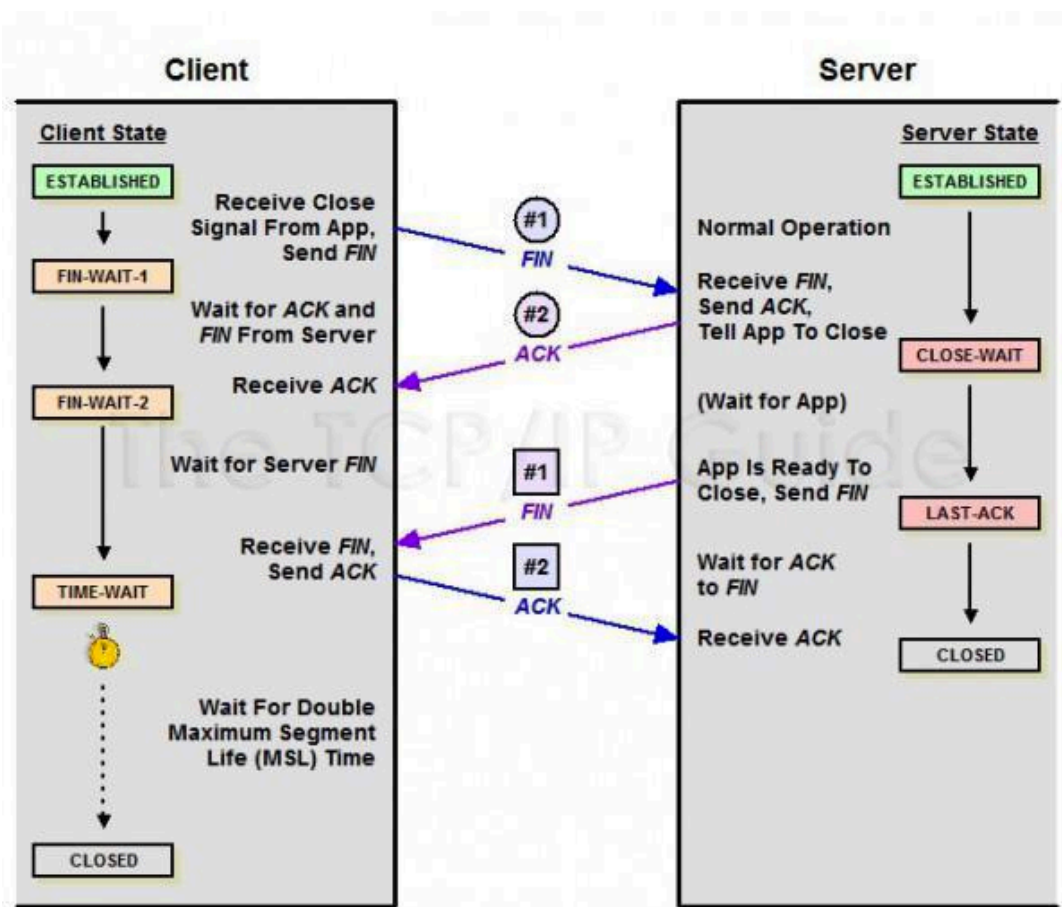
ACK(ack=k+1), 此包发送完毕, 客户端和服务器进入ESTABLISHED状态, 完成三次握手。

三次握手(Three-way Handshake)即建立一个TCP连接时, 需要客户端和服务端总共发送3个包。三次握手的目的是连接服务器指定端口, 建立TCP连接,并同步连接双方的序列号和确认号并交换TCP 窗口大小信息。在socket编程中, 客户端执行connect()时,将触发三次握手。



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。断开连接时服务器和客户端均可以主动发起断开TCP连接的请求, 断开过程需要经过“四次握手”。

TCP连接的拆除需要发送四个包, 因此称为四次握手(four-way handshake)。在socket编程中, 任何一方执行close()操作即可产生握手 (有地方称为“挥手”) 操作。



之所以有“三次握手”和“四次握手”的区别，是因为连接时当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，很可能并不会立即关闭SOCKET，所以只能先回复一个ACK报文，告诉Client端，“你发的FIN报文我收到了”。只有等到我Server端所有的报文都发送完了，我才能发送FIN报文，因此不能一起发送。故需要四次握手。

HTTP连接

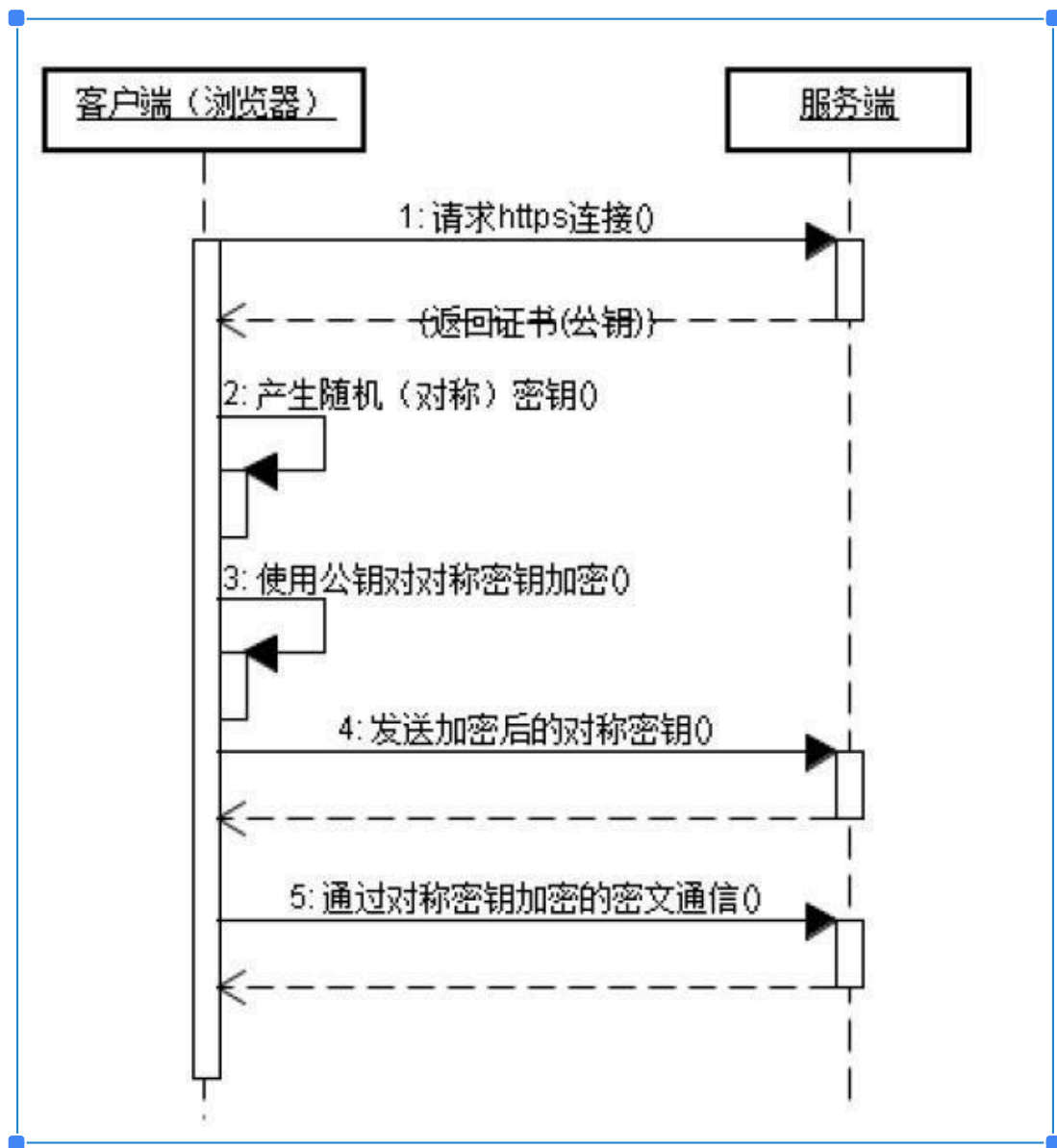
HTTP协议即超文本传送协议(HypertextTransfer Protocol)，是Web联网的基础，也是手机联网常用的协议之一，HTTP协议是建立在TCP协议之上的一种应用。

HTTP连接最显著的特点是客户端发送的每次请求都需要服务器回送响应，在请求结束后，会主动释放连接。从建立连接到关闭连接的过程称为“一次连接”。因此HTTP连接是一种“短连接”，要保持客户端程序的在线状态，需要不断地向服务器

发起连接请求。若服务器长时间无法收到客户端的请求，则认为客户端“下线”，若客户端长时间无法收到服务器的回复，则认为网络已经断开。在HTTP 1.0中，客户端的每次请求都要求建立一次单独的连接，在处理完本次请求后，就自动释放连接。在HTTP 1.1中则可以在一次连接中处理多个请求，并且多个请求可以重叠进行，不需要等待一个请求结束后再发送下一个请求。

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) ，是以安全为目标的HTTP通道，是HTTP的安全版。在HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层（在HTTP与TCP之间）。HTTP协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了Web浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此HTTP协议不适合传输一些敏感信息。

https协议需要到ca申请证书；http是超文本传输协议，信息是明文传输，https则是具有安全性的ssl加密传输协议；http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443；http的连接很简单，是无状态的，HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议。



Socket连接与HTTP连接的不同

通常情况下**Socket**连接就是**TCP**连接，因此Socket连接一旦建立，通信双方即可开始相互发送数据内容，直到双方连接断开。但在实际应用中，客户端到服务器之间的通信防火墙默认会关闭长时间处于非活跃状态的连接而导致 Socket 连接断开，因此需要通过轮询告诉网络，该连接处于活跃状态。

而HTTP连接使用的是“请求—响应”的方式，不仅在请求时需要先建立连接，而且需要客户端向服务器发出请求后，服务器端才能回复数据。

