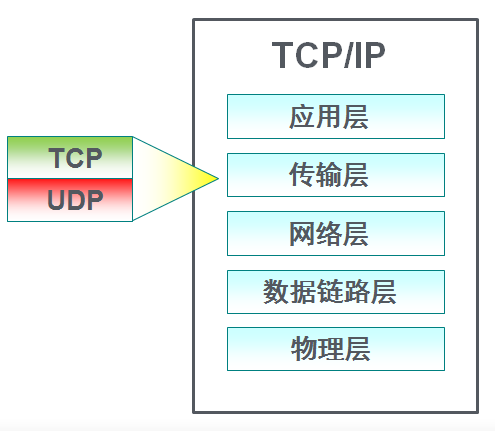
**传输层----及访问控制列表ACL**

**一、传输层协议：**

**1）TCP/IP协议族的传输层协议主要有两个：**

TCP（Transmission Control Protocol ） ：传输控制协议

UDP（User Datagram Protocol ） ：用户数据报协议



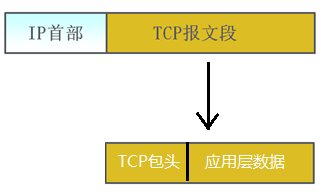
**2）TCP协议特点：**

TCP是面向连接的服务、可靠的进程到进程通信的协议1

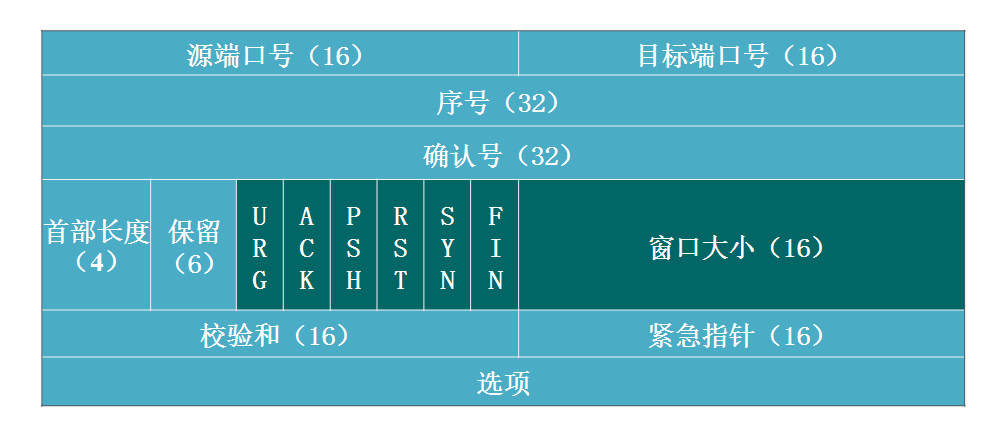
TCP提供全双工服务，即数据可在同一时间双向传输

**3）TCP报文段/封装**

TCP报文段封装在IP数据22报中



**4）TCP包头分析：**



**注释：**

端口号范围：0-65535

源端口号：是客户端进程随机生成的，一般是从50000开始的

目标端口号：一般是服务器固定的。如：mysql：3306

序列号seq：TCP为每个字节都进行了编号。

确认号ack：通过ack来确认每个字节是否收到，判断是否需要重传！

控制位：SYN：请求建立连接位

FIN：请求断开连接位

RST：重置位，强制对方断开连接，释放会话

PSH：推送位，推送数据到应用层，为1时为有应用层数据

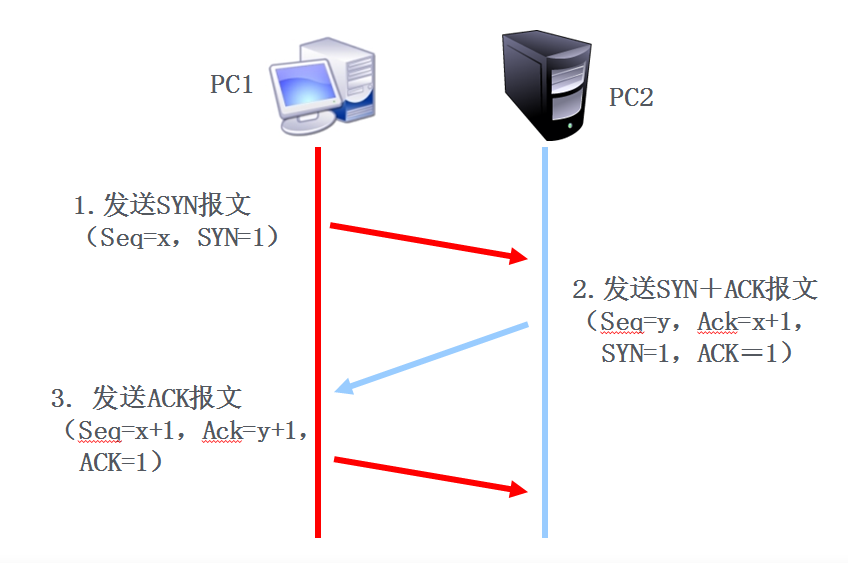
ACK：确认位，该位为开关，为1时，ack号有效，为0时，ack无效。

URG：紧急位，为1时，代表有些字节为紧急数据，需要第一时间推送到应用层，需要与紧急指针配合。

窗口大小：win窗口，用于通知发送方自己的缓存大小。

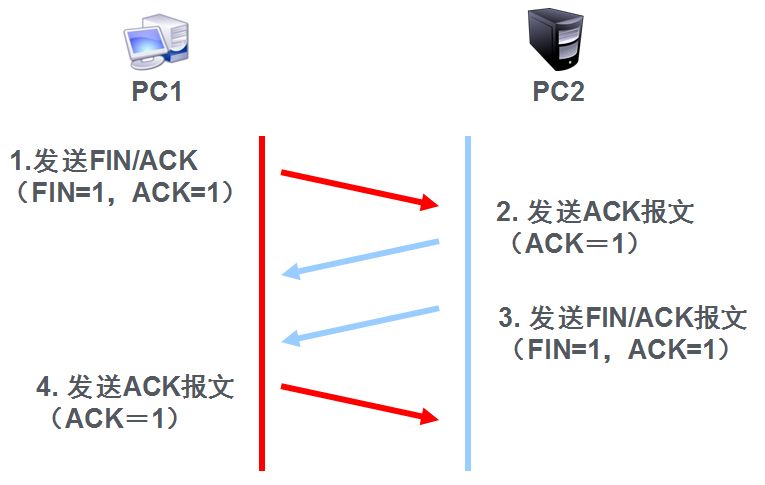
校验和：校验整个TCP段

**5）TCP的三次握手建立连接2**



TCP半连接----SYN Flood攻击/SYN泛洪攻击

**6）TCP的四次握手断开连接**

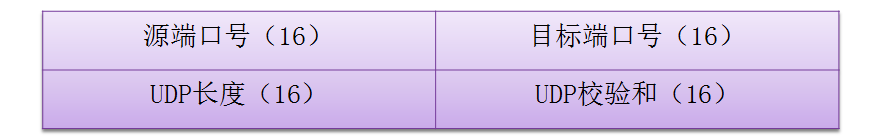


**7）UDP协议特点**

无连接、不可靠的传输协议

花费的开销小、传输效率较高

**8）UDP协议包头：**



**注释：**

UDP长度：用来指出UDP的总长度，为首部加上数据

校验和：用来完成对UDP数据的差错检验，它是UDP协议提供的唯一的可靠机制