OSI七层模型、数据封装与解封装过程、TCP三次握手、四次挥手

原创 GeorgeKai 2018-01-16 14:15:00 评论(0) 1014人阅读

作者：Georgekai
归档：学习笔记
2018/1/16

网络运维基础（二）

1.1 OSI七层模型
应用层：应用程序与接口（如qq和其他三方软件的对接——对应设备（计算机）
协议：http dns telnet nfs ftp tftp smtp（25） snmp（161）
表示层：表示数据的格式、压缩、加密
会话层：作用：建立、维护、管理应用程序之间的会话。
功能：对话控制、同步
传输层：作用：负者建立端到端的连接、保证报文在端到端之间的传输。——对应设备（防火墙）
功能：服务点编址，分段与重组、连接控制、流量控制、差错控制。
协议：TCP UDP
网络层：作用：负者将分组数据从源端传输到目的端——对应设备（路由器）
网络层功能：为网络设备提供逻辑地址，进行路由选择、分组转发
IP地址=网络位+主机位

IP地址是三层地址

协议：IP ARP RARP ICMP（Internet控制报文协议） IGMP

数据链路层：作用：在局域网内部实现主机与主机之间的通讯——对应设备（交换机）

协议：PPP FDDI

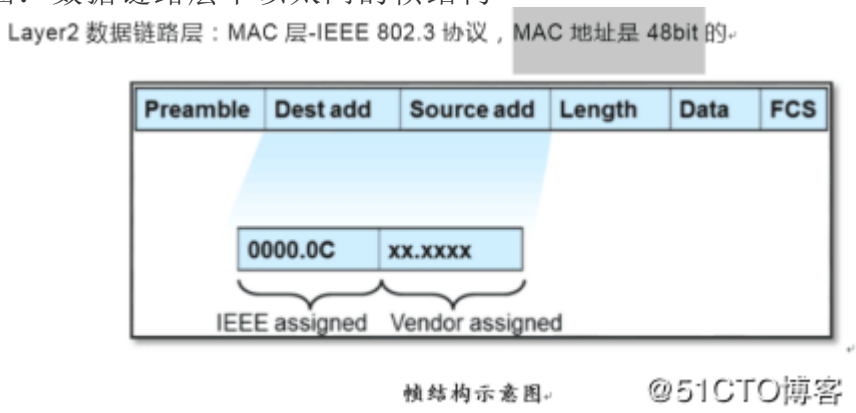
物理层：作用：负者把逐个的比特从一跳（结点）移动到另一跳（结点）。——（网卡）

功能：1）定义接口和媒体的物理特性

2）定义比特的表示、数据传输速率、信号的传输模式（单工、半双工、全双工）

3）定时网络物理拓扑（网状、星型、环形、总线型、等拓扑）

下图：数据链路层中以太网的帧结构



1）mac地址就是二层地址，全球网络设备唯一的地址

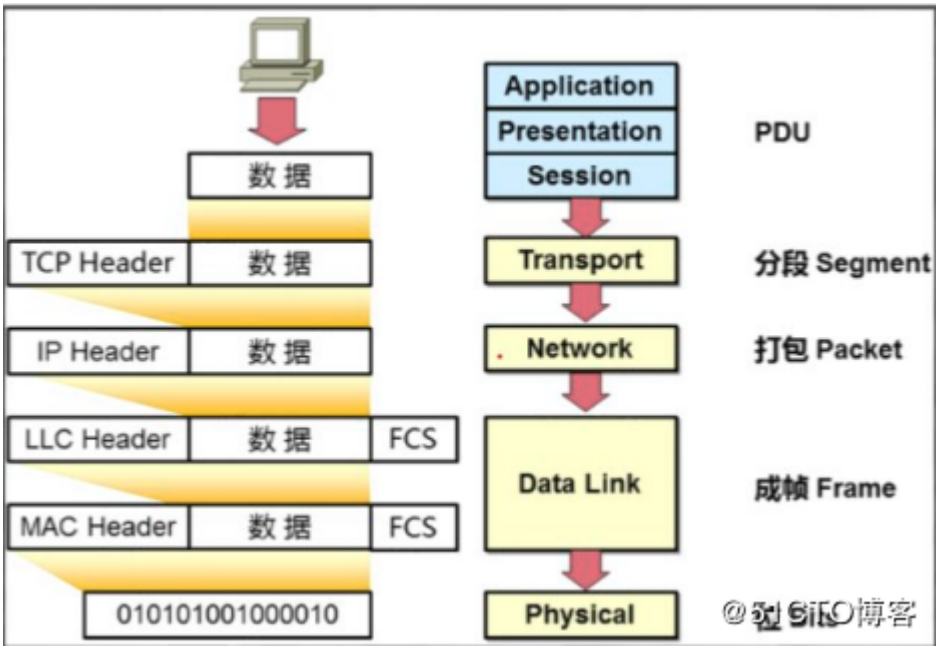
2）根据作用的域不同：IP作用在不同的网络之间，MAC地址作用在相同的网络内部

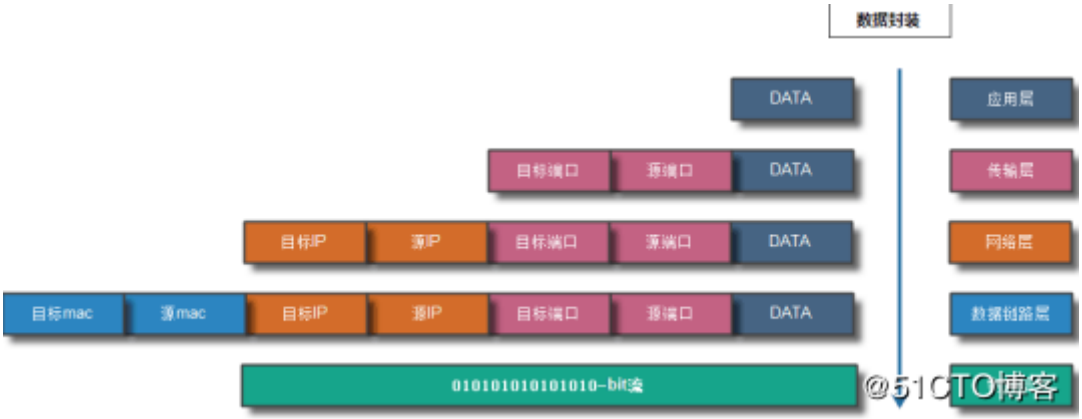
3）MAC地址48位的地址，采用16进制进行表示，MAC地址是硬件地址

4）IP地址会被是逻辑地址

1.2 数据封装与解封装过程：

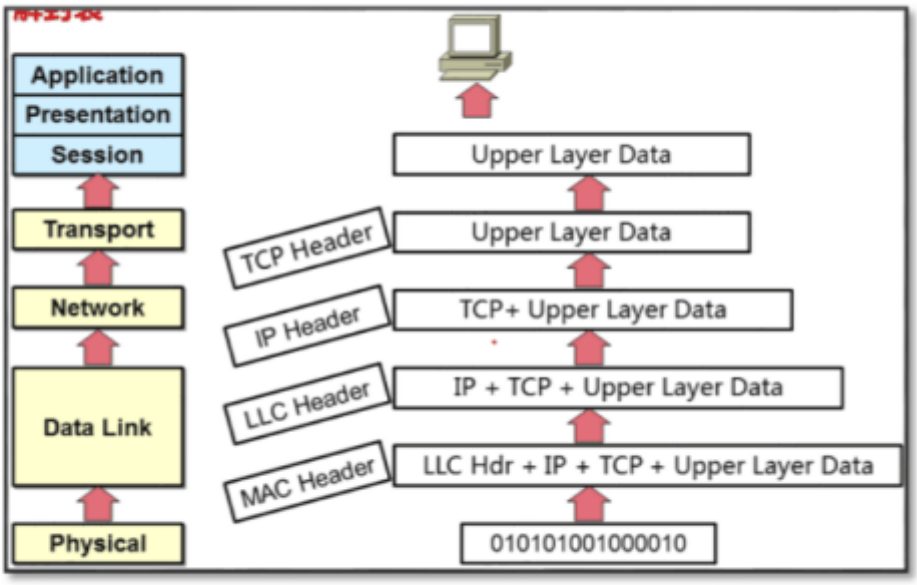
1.2.1 数据封装过程：



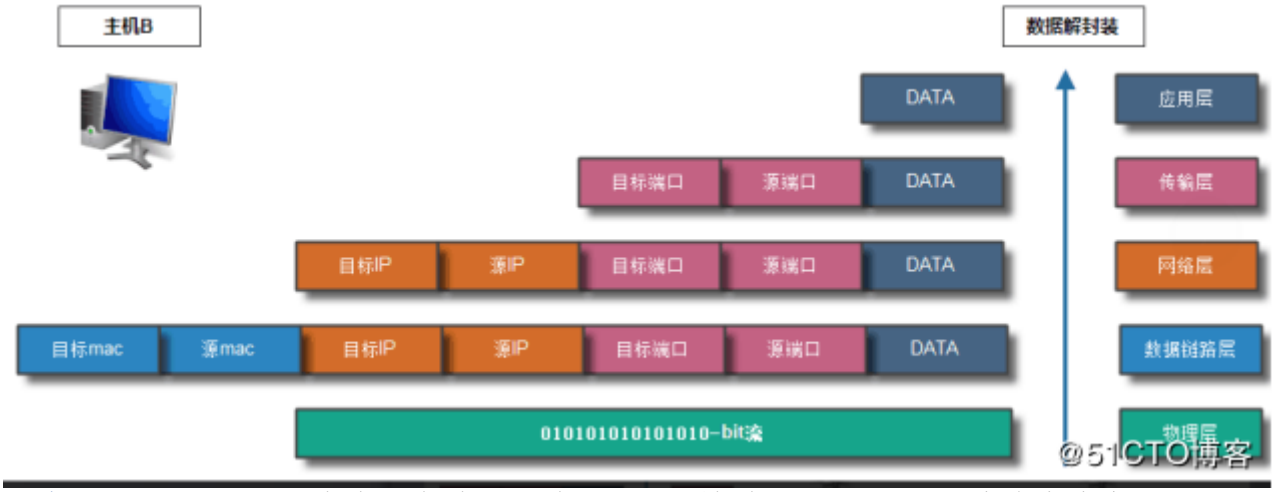


1.2.2 数据解封装过程：

▪ 8.7.2 OSI 互联数据包解封装过程



数据传输解封装过程示意图。 @51CTO博客



注意： 1. mac地址只在本地有效，通过路由器传输过程，mac地址信息会发生变化

2. 路由器根据路由表识别目标IP地址网段信息，确认是否可以进行转发，或是进行数据包的丢弃

1.2.3 DOD四层模型

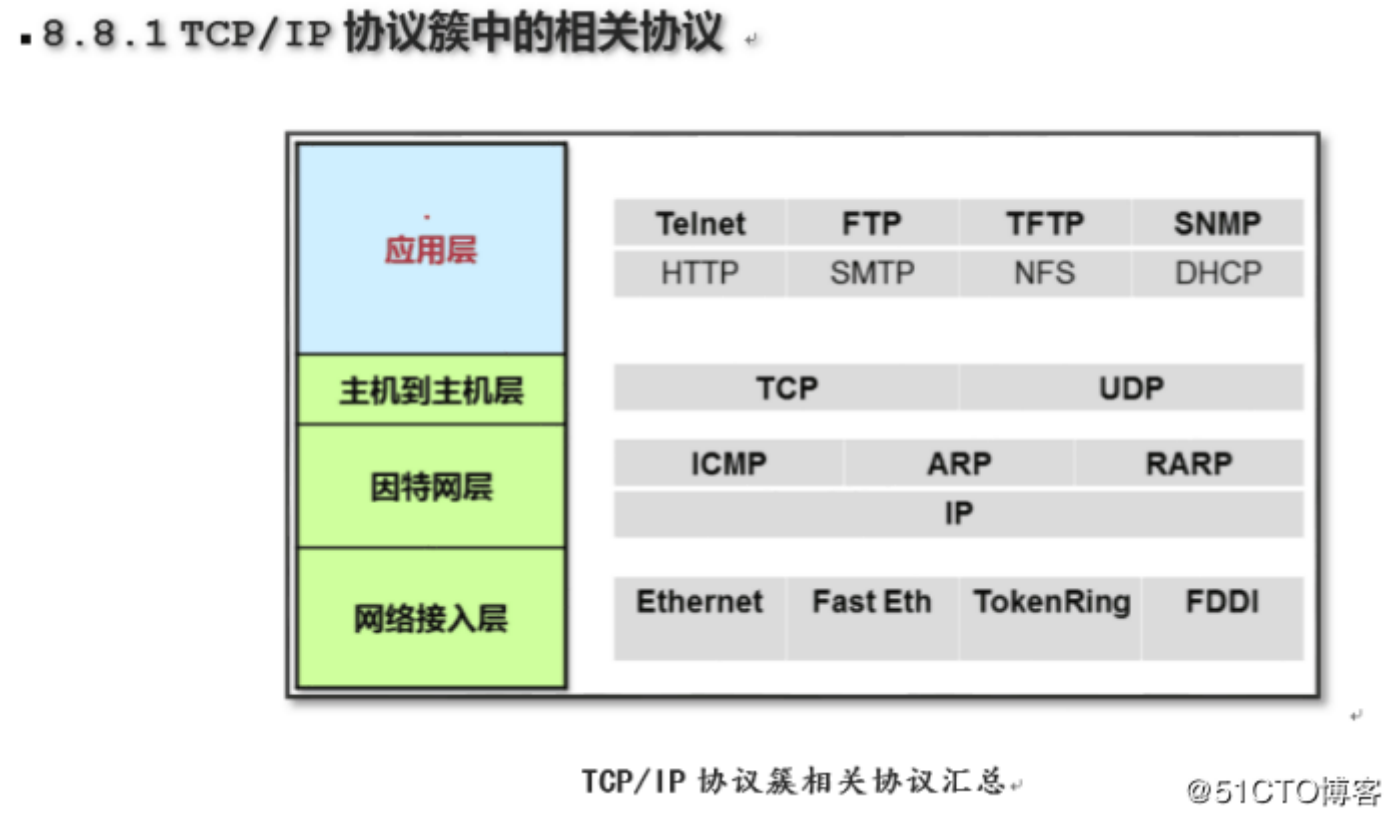
应用层——主机到主机层——因特网层——网络接入层

1.2.4 DHCP工作原理

参考文档：

http://www.zyops.com/dhcp-working-procedure

1.2.5 TCP/IP协议簇相关协议



1.3 传输层的俩种协议：（拿QQ在线传输和离线传输作例子）

1.3.1 **TCP**：传输控制协议

- 属于面向连接的网络协议
- 同步
- 安全，可靠传输 ，速度传输慢
- 流量控制（Qos）
- 使用TCP的应用：WEB浏览器，电子邮件，文件传输程序

1.3.2 **UDP**： 用户数据报协议

- 属于无连接的网络协议
- 异步
- 不安全，速度传输快
- 尽力而为，不管你是否收到
- 使用UDP的应用：DNS，视频流，IP语音（VoIP）

1.4 TCP相关报文结构

1.4.1 端口号计算：

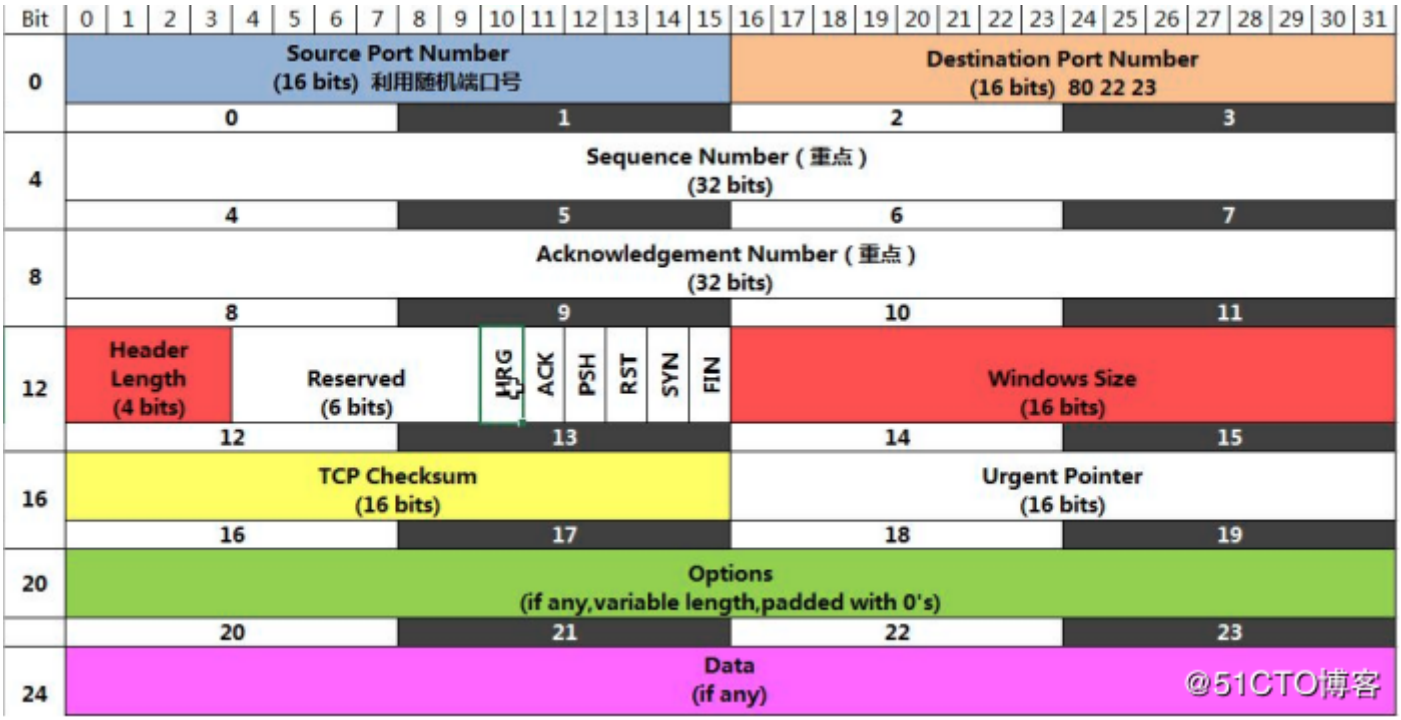
1. 在TCP报头中端口号占16个比特位，那么它的范围就是2的16次方=65536
   0号端口不用，所以就是1-65535个端口

1.4.2 著名端口号范围1-1024，自定义端口的时候不要使用（避免冲突）

1.4.3 源端口随机端口号分配

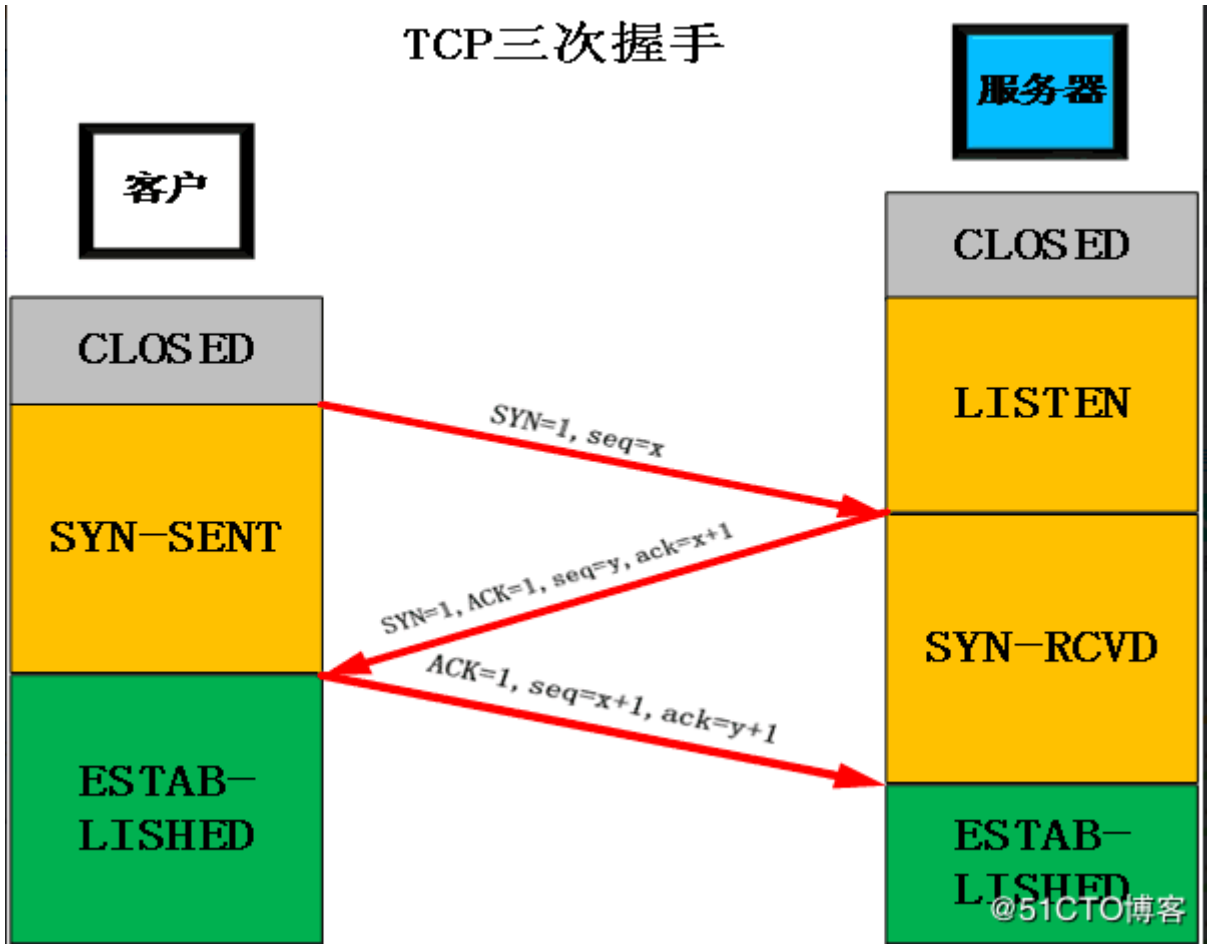
1. 取决于这个配置文件
   cat /proc/sys/net/ipv4/ip_local_port_range
   32768 —— 60999

1.4.4 TCP报头 （配合snifer抓包软件会更好理解，去网上下载一个即可）



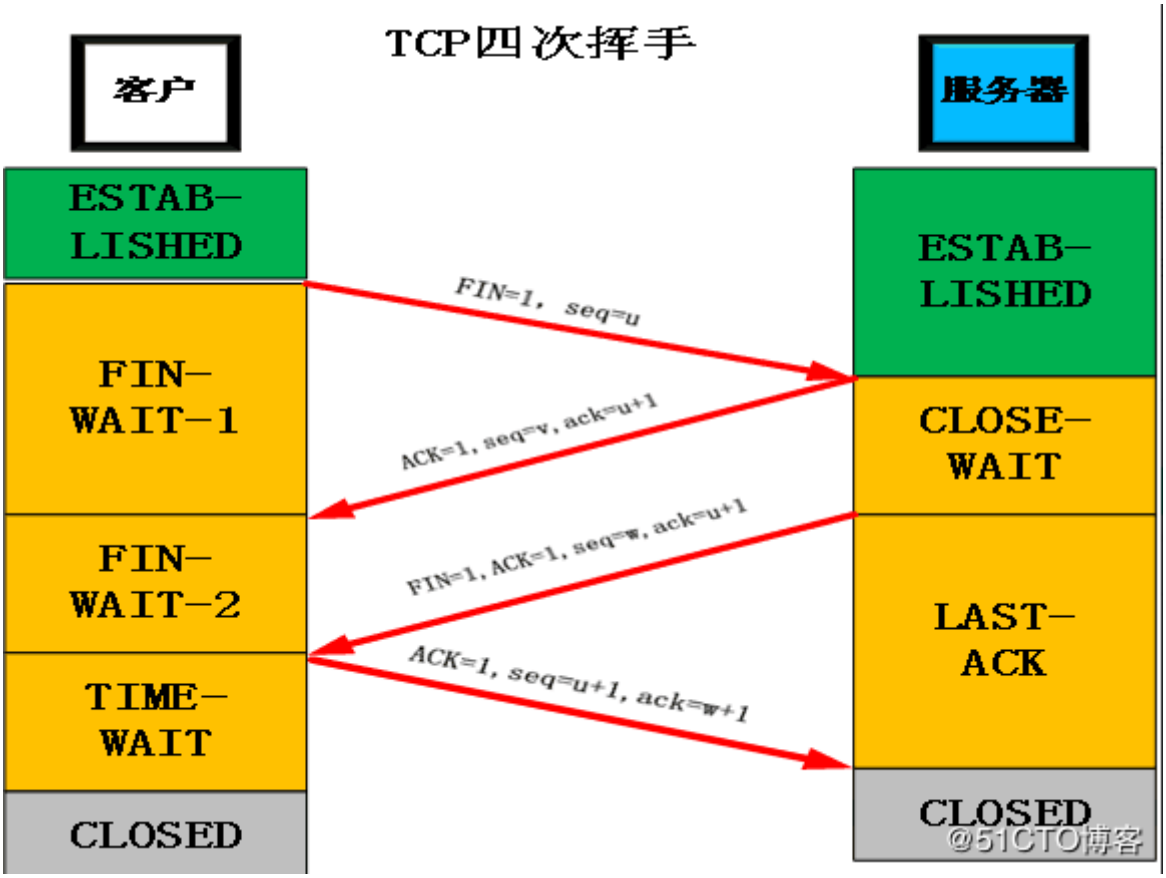
1. 源端口号：发送端端口号
2. 目的端口号：接收端端口号
3. TCP报文重要控制位：
   1）syn：请求建立连接
   2）fin：请求断开连接
   3）ack：确认控制字段

1.4.5 TCP的三次握手

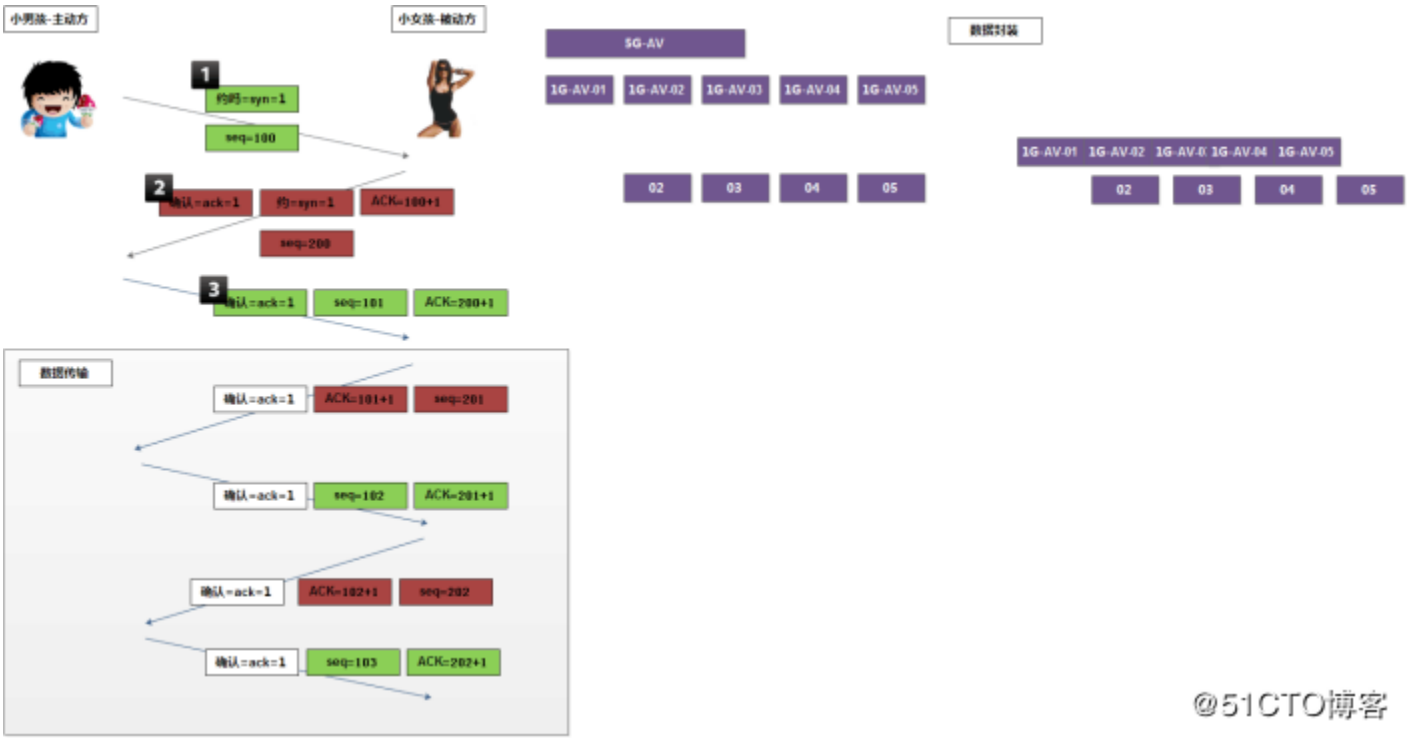


数据传输过程中：每发送一次数据，都会产的ACK（表示收到了对方seq对应的信息），ack（表示确认收到），seq（请求序列号）

1.4.6 TCP的四次挥手



如果把三次握手和四次挥手总结起来用（用约妹子的方法）就是这样：



最进这5天左右先科普下网络必会的些此处知识，上面的过程可使用snifer抓包进行分析，效果会更好理解

小伙伴们可以关注我的微信公众号：linux运维菜鸟之旅