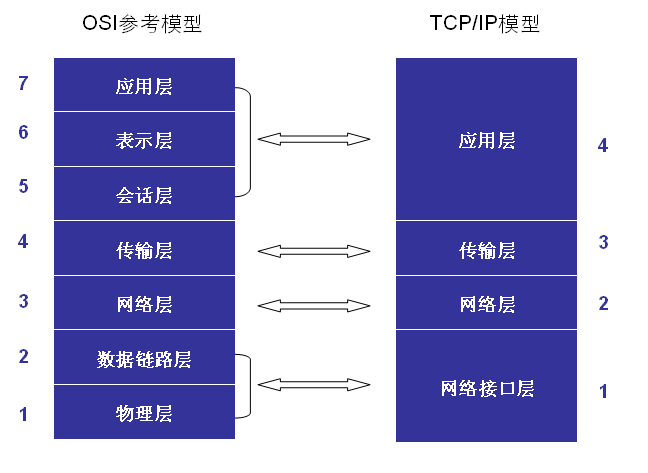
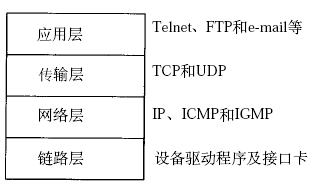
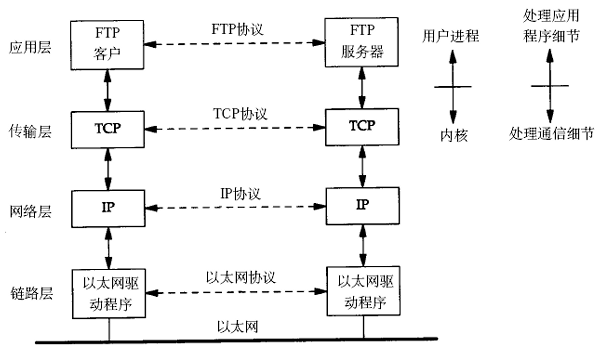
1. **OSI七层模型和TCP四层模型**

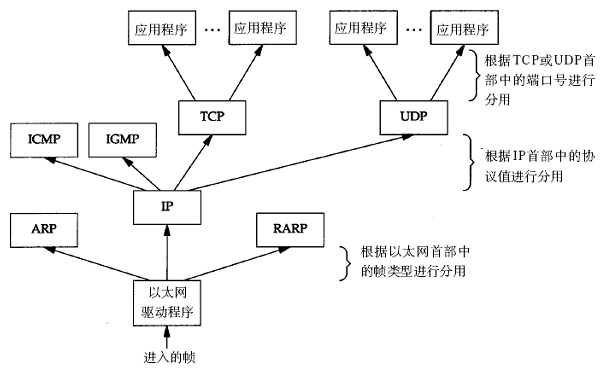




1. **TCP/IP通信过程**



1. **multiplexing过程**



1. **MAC地址**

MAC地址也叫物理地址、硬件地址，由网络设备制造商生产时烧录在网卡，是全球唯一的。IP地址是32位，MAC地址是48位（如：40-8D-5C-9F-B2-BA）。

网络中数据帧从一个路由节点到下一跳路由节点，是依靠MAC地址而非IP地址进行传输的，因此数据传输时需要知道传输路径上的节点的MAC地址，通过ARP协议获取某IP主机的MAC地址。

1. **ARP协议**

地址解析协议，可以实现通过IP地址获得对应主机的物理地址（MAC地址）。

ARP协议要求通信的主机双方必须在同一个物理网段。

ARP协议具体通信过程：

①每台主机都会在自己的ARP高速缓冲区建立一个ARP列表，用于存储IP地址与MAC地址的对应关系。当源主机需要发数据包到目标主机时，先检查自己的ARP列表中是否存在该IP地址对应的MAC地址，如果存在则直接将数据包发送到该MAC地址。

②如果源主机没有目标主机的MAC地址时就需要向本地网段发一个ARP请求（ARPrequest）的广播包，用于查询目标主机对应的MAC地址。此ARP请求数据包里包括源主机的IP地址、NAC地址及目标地址的IP地址。

③网段中所有主机收到这个ARP请求后，看数据包中包含的IP地址是否与自己的IP地址一致，如果不一样就忽略；如果一致就把发送端的MAC地址和IP地址添加到自己的ARP列表中，如果该对应关系已经存在，则将其覆盖掉，然后给源主机发送一个ARP响应包(ARPreply)（单播），响应包包括自己的IP地址和MAC地址。

④源主机收到目标主机的响应后，将目标主机的IP地址的和MAC地址添加到自己的ARP列表中，并用此消息开始数据的传输。

⑤如果源主机一直没有收到ARP响应包，则提示ARP查询失败。

1. **RARP协议**

RARP协议通过MAC地址获取IP地址。

当设置一台新机器时，其RARP客户端需要向路由器上的RARP服务器请求相应的IP地址。假设在路由表中已经设置了一个记录，RARP服务器将返回IP地址给机器，此机器就会存储起来以便日后使用。

1. **ARP攻击**

ARP协议是建立在信任局域网内所有节点的基础上的，效率很高但是不安全。ARP协议是无状态的协议，它不会检查自己是否发过请求包，也不知道自己是否发过请求包。它也不管是否合法的应答，只要收到目标mac地址是自己的ARPreply或者ARP广播包（包括ARPreply和ARPrequest），都会接受并缓存。