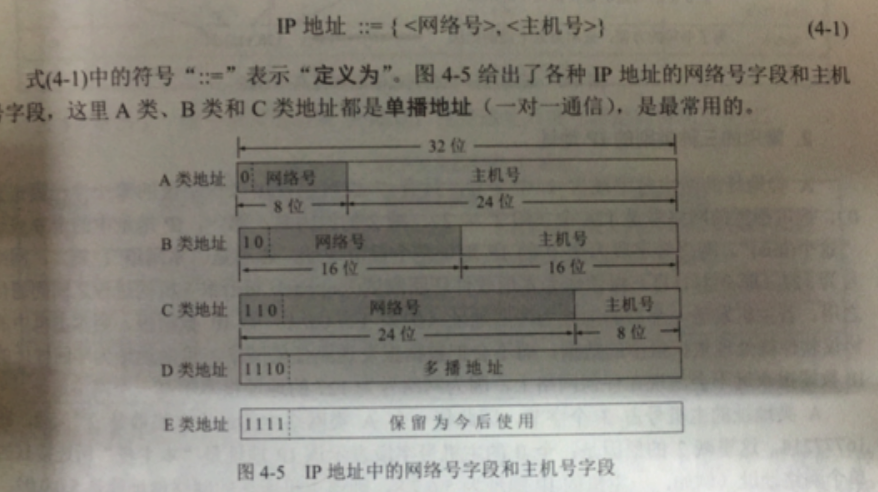
[http://www.cnblogs.com/maybe2030/p/4781555.html#\_label3](http://www.cnblogs.com/maybe2030/p/4781555.html" \l "_label3)

**一、网络层次划分（OSI七层模型，自下而上）**

1. 物理层（Physical Layer）
   * 该层为上层协议提供了一个传输数据的可靠的物理媒体。
   * 重要设备：中继器（Repeater，也叫放大器）、集线器
2. 数据链路层（Data Link Layer）
   * 为网络层提供可靠的数据传输
   * 基本数据单位：帧（frame）
   * 主要的协议：以太网协议
   * 重要设备：网桥、交换机
   * 作用：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等
3. 网络层（Network Layer）
   * 负责对子网间的数据进行路由选择。还可以实现拥塞控制、网际互连等功能；
   * 基本数据单位：IP数据报
   * 包含的协议：IP协议、ICMP协议、ARP协议、RARP协议
   * 重要设备：路由器
4. 传输层（Transport Layer）
   * 负责将数据可靠地传送到相应的端口
   * 基本数据单位：段或报文
   * 包含的协议：TCP协议、UDP协议
   * 重要设备：网关
5. 会话层
   * 负责建立、管理、终止进程之间的会话
   * 一个程序就是一个进程
   * 基本数据单位：报文
   * 包含的协议：FTP协议、Telnet协议、DNS、SMTP、POP3协议、HTTP协议
6. 表示层
   * 对上层数据或信息进行变换以保证一个主机应用层信息可以被另一个主机的应用程序理解。
   * 基本数据单位：报文
   * 包含的协议：FTP协议、Telnet协议、DNS、SMTP、POP3协议、HTTP协议
7. 应用层
   * 为操作系统或网络应用程序提供访问网络服务的接口
   * 基本数据单位：报文
   * 包含的协议：FTP协议、Telnet协议、DNS、SMTP、POP3协议、HTTP协议

**二、IP地址**



1. 网络地址（主机号全为0）
   * IP地址由网络号（包括子网号）和主机号组成，一共有32位。
   * 如B类地址以10开头（10000000），前两个字节作为网络号，地址范围是：128.0.0.0~191.255.255.255;
2. 广播地址（主机号全为1）
   * 也叫直接广播地址，区分于受限广播地址
   * 向某个网络的广播地址发送消息时，该网络内的所有主机都能收到该广播消息
3. 组播地址
   * 以1110开头，地址范围是224.0.0.0~239.255.255.255
   * 可以进行一对多的通信
4. 255.255.255.255（受限的广播地址）
   * 受限的广播地址只能用于本地网络
   * 路由器不会转发以受限广播地址为目的地址的分组
5. 0.0.0.0
   * 常用于寻找自己的IP地址
6. 回环地址
   * 127.0.0.0/8被用作回环地址，回环地址表示本机的地址，常用于对本机的测试，用的最多的是127.0.0.1。
7. A、B、C类私有地址
   * 不会在全球使用，只具有本地意义
8. A、B、C、D类地址
   * A类地址以0开头，第一个字节作为网络号，地址范围为：0.0.0.0~127.255.255.255
   * B类地址以10开头，前两个字节作为网络号，地址范围是：128.0.0.0~191.255.255.255;
   * C类地址以110开头，前三个字节作为网络号，地址范围是：192.0.0.0~223.255.255.255。
   * D类地址以1110开头，地址范围是224.0.0.0~239.255.255.255，D类地址作为组播地址（一对多的通信）；
   * E类地址以1111开头，地址范围是240.0.0.0~255.255.255.255，E类地址为保留地址，供以后使用。
   * 注：只有A,B,C有网络号和主机号之分，D类地址和E类地址没有划分网络号和主机号。

**三、子网掩码及网络划分**

1. 子网掩码产生的背景
   * 越来越多的终端使用互联网，这就导致网络号占位太多，而主机号位太少，所以能提供的主机地址也越来越稀缺。
   * 将分配的IP地址主机号的高位部分取作为子网号，从网络位界限中扩展或压缩子网掩码，用来创建某类地址的更多子网。
2. 子网掩码
   * 子网掩码是标志两个IP地址是否同属于一个子网的，也是32位二进制地址，其每一个为1代表该位是网络位，为0代表主机位。
   * 如果两个IP地址在子网掩码的按位与的计算下所得结果相同，即表明它们共属于同一子网中。
   * 在计算子网掩码时，我们要注意IP地址中的保留地址，即“ 0”地址和广播地址，它们是指主机地址或网络地址全为“ 0”或“ 1”时的IP地址，它们代表着本网络地址和广播地址，一般是不能被计算在内的。
3. 子网掩码计算：
   * 无须再划分子网的IP地址，子网掩码按照定义即可写出，如B类IP地址的子网掩码255.255.0.0，C类IP地址的子网掩码为255.255.255.0。
   * 利用**子网数**来计算，如欲将B类IP地址168.195.0.0划分成27个子网
     + 将子网数目转化为二进制：27 = 11011
     + 取得该二进制的位数，N = 5
     + 取得该IP地址的类子网掩码，将其主机地址部分的的前N位置1即得出该IP地址划分子网的子网掩码。将B类地址的子网掩码255.255.0.0的主机地址前5位置成1后3位置成0，得到255.255.248.0
   * 利用**主机数**来计算，如欲将B类IP地址168.195.0.0划分成若干子网，每个子网内有主机700台
     + 将主机数目转化为二进制来：700 = 1010111100
     + 取得该二进制的位数，N=10
     + 使用255.255.255.255来将该类IP地址的主机地址位数全部置1，然后从后向前的将N位全部置为 0，即为子网掩码值。将该B类地址的子网掩码255.255.0.0的主机地址全部置1，得到255.255.255.255，然后再从后向前将后10位置0，即为：11111111.11111111.11111100.00000000，即255.255.252.0。这就是该欲划分成主机为700台的B类IP地址 168.195.0.0的子网掩码。
   * 根据每个网络的主机数量进行子网地址的规划和计算子网掩码，如一个子网有10台主机，那么这个子网需要的IP地址是多少？
     + 10+1+1+1=13 （加的第一个1是指网络连接时所需的网关地址，接着的两个1分别是网络地址和广播地址）
     + 因为13小于16（16等于2的4次方），所以主机位为4位。而256（从0~255一共有256个数）－16＝240，所以该子网掩码为255.255.255.240。
     + 如果一个子网有14台主机，不少人常犯的错误是：依然分配具有16个地址空间的子网，而忘记了给网关分配地址。这样就错误了，因为14＋1＋1＋1＝17，17大于16，所以我们只能分配具有32个地址（32等于2的5次方）空间的子网，而256-32=224，这时子网掩码为255.255.255.224。

**四、ARP/RARP协议**

1. 地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。
2. 逆地址解析协议，即RARP，功能和ARP协议相对，其将局域网中某个主机的物理地址转换为IP地址的协议。
3. 主机发送信息（包含目标IP地址）-> 网络上的所有主机 -> 接收返回消息 -> 确定目标的物理地址 -> 存入本机ARP缓存
4. ARP命令可用于查询本机ARP缓存中IP地址和MAC地址的对应关系、添加或删除静态对应关系等
5. ARP工作流程举例：
   * 主机A的IP地址为192.168.1.1，MAC地址为0A-11-22-33-44-01；
   * 主机B的IP地址为192.168.1.2，MAC地址为0A-11-22-33-44-02；
     + 当主机A要与主机B通信时，地址解析协议（ARP）可以将主机B的IP地址（192.168.1.2）解析成主机B的MAC地址，以下为工作流程：
       - （1）根据主机A上的路由表内容，IP确定用于访问主机B的转发IP地址是192.168.1.2。然后A主机在自己的本地ARP缓存中检查主机B的匹配MAC地址。
       - （2）如果主机A在ARP缓存中没有找到映射，它将询问192.168.1.2的硬件地址，从而将ARP请求帧广播到本地网络上的所有主机。源主机A的IP地址和MAC地址都包括在ARP请求中。本地网络上的每台主机都接收到ARP请求并且检查是否与自己的IP地址匹配。如果主机发现请求的IP地址与自己的IP地址不匹配，它将丢弃ARP请求。
       - （3）主机B确定ARP请求中的IP地址与自己的IP地址匹配，则将主机A的IP地址和MAC地址映射添加到本地（主机B的）ARP缓存中。
       - （4）主机B将包含其MAC地址的ARP回复消息直接发送回主机A。
       - （5）当主机A收到从主机B发来的ARP回复消息时，会用主机B的IP和MAC地址映射更新ARP缓存。本机缓存是有生存期的，生存期结束后，将再次重复上面的过程。主机B的MAC地址一旦确定，主机A就能向主机B发送IP通信了。
     + RARP协议工作流程：
       - （1）给主机发送一个本地的RARP广播，在此广播包中，声明自己的MAC地址并且请求任何收到此请求的RARP服务器分配一个IP地址；
       - （2）本地网段上的RARP服务器收到此请求后，检查其RARP列表，查找该MAC地址对应的IP地址；
       - （3）如果存在，RARP服务器就给源主机发送一个响应数据包并将此IP地址提供给对方主机使用；
       - （4）如果不存在，RARP服务器对此不做任何的响应；
       - （5）源主机收到从RARP服务器的响应信息，就利用得到的IP地址进行通讯；如果一直没有收到RARP服务器的响应信息，表示初始化失败。

**五、路由选择协议**

1. RIP协议：选择路由的度量标准metric是跳数，最大跳数是15跳，如果大于15跳，就会丢弃数据包
2. OSPF协议：Open Shortest Path First开放式最短路径优先，是链路状态路由选择协议，选择路由的度量标准是带宽、延迟。

**六、TCP/IP Protocol**

1. It’s the most basic protocol, the base of internet. It consists of IP protocol in Network layer and TCP protocol in Transport layer.
2. The process of setting up TCP connection:
   * Client send a connection request to a Server > Server: accept the connection, reply ACK to the Client and allocate resources > Client: reply ACK to Server and allocate resource
3. The process of failure setting up TCP connection:
   * Client send a disconnection request(FIN) to a Server > Server: send ACK to the Client and ask the Client to wait for a message > Client: the status is FIN\_WAIT now and keep waiting for FIN message from the Server. > If no data need to send to the Client, Server will send FIN message to the Client. > Client: after receiving FIN message, it will send ACK to the server, and the status will be changed to TIME\_WAIT. > If the server doesn’t receive ACK, the Client can resend it. > If the Server receives ACK, it means the Server can disconnect now. > Client can disconnect when it waits for 2MSL and no responded from the Server.
4. Protocol using TCP protocol: FTP, Telnet(remote login protocol), SMTP(simple mail transportation protocol), POP3, HTTP