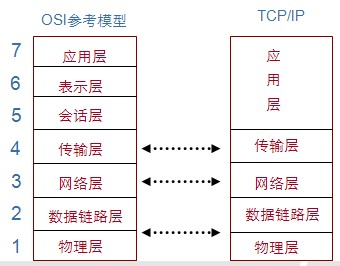
# 为了学习nginx fastcgi而去了解了下面这些基础概念。

# 一、TCP/IP分层模型

参考博客：http://blog.csdn.net/be\_happy\_mr\_li/article/details/52243006

TCP/IP模型分为5层：应用层、传输层、网络层、数据链路层及物理层。

Osi参考模型与TCP/IP模型比较



1. 应用层

应用层是我们经常接触使用的部分，比如常用的http协议、ftp协议（文件传输协议）、snmp（网络管理协议）、telnet （远程登录协议 ）、smtp（简单邮件传输协议）、dns（域名解析），这次主要是面向用户的交互的。这里的应用层集成了osi分层模型中 的应用、会话、表示层三层的功能。

1. 传输层

传输层的作用就是将应用层的数据进行传输转运。比如我们常说的tcp（可靠的传输控制协议）、udp（用户数据报协议）。传输单位为报文段。

tcp（Transmission Control Protocol）

面向连接（先要和对方确定连接、传输结束需要断开连接，类似打电话）、复杂可靠的、有很好的重传和查错机制。一般用与高速、可靠的通信服务

udp（user datagram protocol）

面向无连接（无需确认对方是否存在，类似寄包裹）、简单高效、没有重传机制。一般用于即时通讯、广播通信等

1. 网络层

网络层用来处理网络中流动的数据包，数据包为最小的传递单位，比如我们常用的ip协议、icmp协议、arp协议（通过分析ip地址得出物理mac地址）。

1. 数据链路层

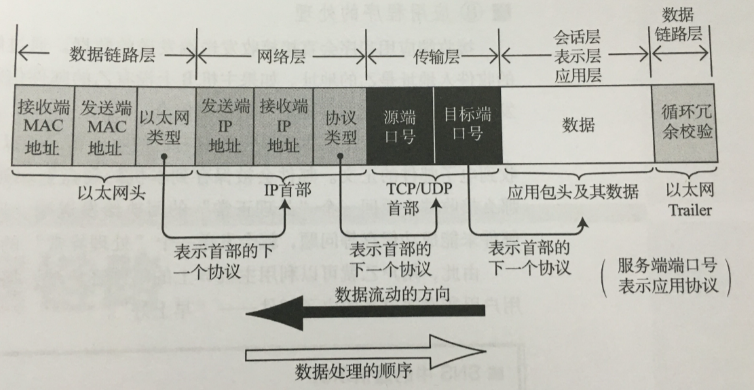
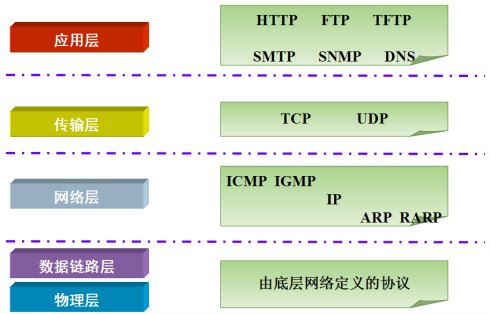
数据链路层一般用来处理连接硬件的部分，包括控制网卡、硬件相关的设备驱动等。传输单位数据帧。

1. 物理层

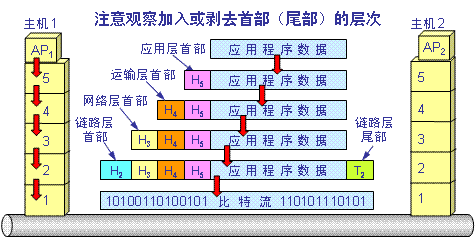
物理层一般为负责数据传输的硬件，比如我们了解的双绞线电缆、无线、光纤等。比特流光电等信号发送接收数据。

**数据传递**

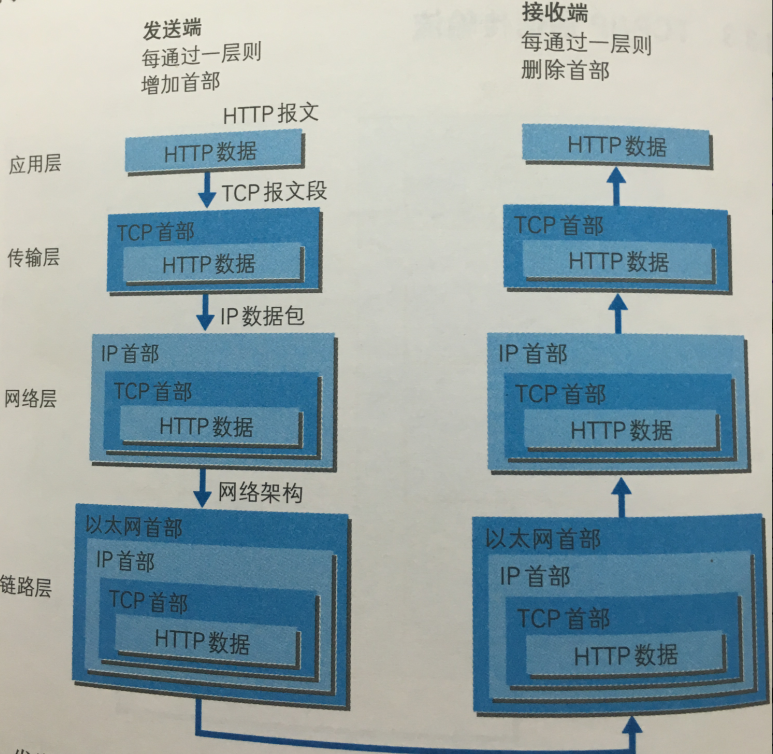
首先应用层将数据报文按照协议封装格式压缩然后传递给传输层、传输层通过协议将数据报封装为数据报段、然后传递给网络层，网络层将数据报段封装为数据包，并传递给数据链路层，数据链路层收到数据包，封装为数据帧，然后又将数据帧转比特流传递给物理层，物理层将比特流通过光或电信号发送给目标。



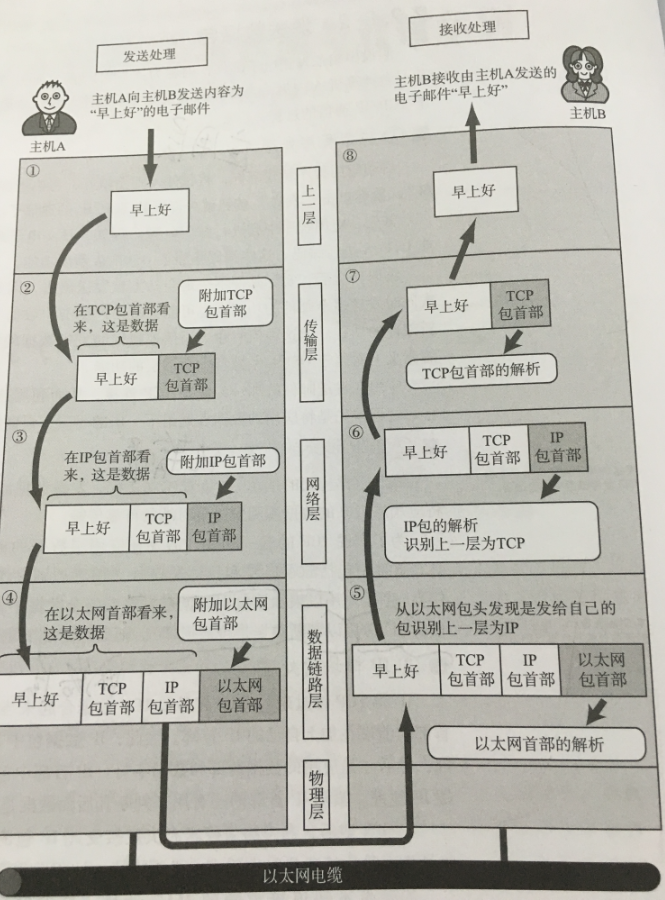
**数据交互**



**http报文通过tcp发送的举例**



**应用交互举例**



# 二、网络相关基本概念

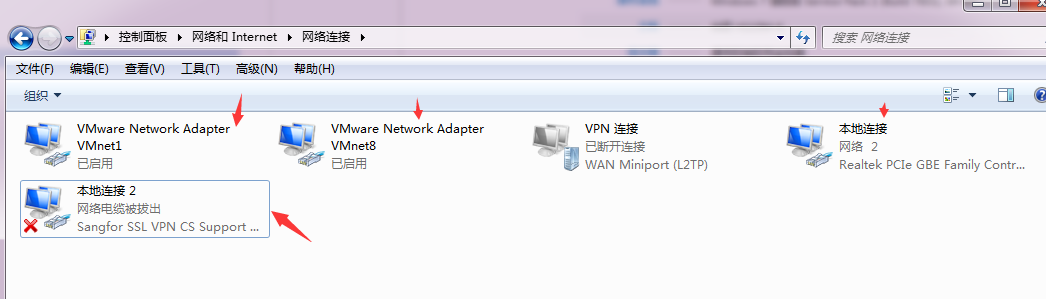
# 1. 网卡

网卡是工作在数据链路层的网络组件，是局域网中连接计算机和传输介质的接口，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及到帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据的缓存的功能等。

**拓展：**

传输介质：指网络传输介质，是网络中发送方与接收方之间的物理通路，它对网络的数据通信具有一定的影响。常用的传输介质有：双绞线、同轴电缆、光纤、无线传输媒介(无线电波、微波、红外线、激光)。

网卡：计算机与外界局域网的连接是通过主机箱内插入一块网络接口板。网卡的别名有：网络接口板、网络适配器、网络接口卡，一般都称网卡。如我自己的计算机网卡截图如下，包括虚拟机的网卡：



# 网卡的功能

网卡上面装有处理器和存储器（包括RAM和ROM）。网卡和局域网之间的通信是通过电缆或双绞线以串行传输方式进行的，而网卡和计算机之间的通信则是通过计算机主板上的I/O总线以并行传输方式进行的。因此，网卡的一个重要功能是进行串行/并行转换。由于网络上的数据率和计算机总线上的数据率并不相同，因此在网卡中必须有对数据进行缓存的存储芯片。

在安装网卡时必须将管理网卡的设备驱动程序安装在计算机的操作系统中。这个驱动程序以后就会告诉网卡，应当从存储器的什么位置上将局域网传送过来的数据块存储下来。网卡还要能够实现以太网协议。

网卡并不是独立的自治单元，因为网卡本身不带电源而是必须使用所插入的计算机的电源，并受该计算机的控制。因此网卡可看成为一个半自治的单元。当网卡收到一个有差错的帧时，它就将这个帧丢弃而不必通知它所插入的计算机。当网卡收到一个正确的帧时，它就使用中断来通知该计算机并交付给协议栈中的网络层。当计算机要发送一个IP数据包时，它就由协议栈向下交给网卡组装成帧后发送到局域网。

随着集成度的不断提高，网卡上的芯片的个数不断的减少，虽然各个厂家生产的网卡种类繁多，但其功能大同小异

1. 数据的封装与解封

发送时将上一层(即网络层)交下来的数据加上首部和尾部，成为以太网的帧。接收时将以太网的帧剥去首部和尾部，然后交给上一层（即网络层）

2、链路管理

主要是CSMA/CD（Carrier Sense Multiple Access with Collision Detection ，带冲突检测的载波监听多路访问）协议的实现

3、编码与译码

即曼彻斯特编码与译码。

**拓展：**

# 数据帧、数据包、数据报以及数据段

OSI模型有7层：  
上四层协议有：  
第7层应用层（Application）协议和应用：http,ftp,tftp,telnet,dns,smtp  
此层是用户与计算机进行实际通信的地方.只是当马上就要访问网络时,才会实际上用到这一层.  
第6层表示层（Presnation）协议和应用：ebcdic,ascii,jpeg,tiff,midi,mpeg  
第5层会话层（Session）协议和应用：nfs,sql,rpc,x-windows,netbios  
下四层协议有：  
第4层传输层（Transport 此层数据单位【段segment】）协议和应用：tcp,udp,spx  
第3层网络层（Network   此层数据单位【包packet】）协议和应用：ip,ipx,appletalk,icmp  
第2层链路层（Data Link 此层数据单位【帧Frame】）协议和应用：802.3,802.2,atm,fr  
第1层物理层（Physical此层数据单位【比特流Bit】）协议和应用：v.35,eia/tia 323

信息交换发生在对等OSI层之间，在源端机中每一层把控制信息附加到数据中，而目的机器的每一层则对接收到的信息进行分析，并从数据中移去控制信息，下面是各信息单元的说明：

数据帧（Frame）：是一种信息单位，它的起始点和目的点都是数据链路层。

数据包（Packet）：也是一种信息单位，它的起始和目的地是网络层。

数据报（Datagram）：通常是指起始点和目的地都使用无连接网络服务的的网络层的信息单元。

段（Segment）：通常是指起始点和目的地都是传输层的信息单元。

消息（message）：是指起始点和目的地都在网络层以上（经常在应用层）的信息单元。

元素（cell）是一种固定长度的信息，它的起始点和目的地都是数据链路层。

元素通常用于异步传输模式（ATM）和交换多兆位数据服务（SMDS）网络等交换环境。

数据单元（data unit）指许多信息单元。常用的数据单元有服务数据单元（SDU）、协议数据单元（PDU）。

SDU是在同一机器上的两层之间传送信息。PDU是发送机器上每层的信息发送到接收机器上的相应层（同等层间交流用的）。

Packet（数据包）：封装的基本单元，它穿越网络层和数据链路层的分解面。通常一个Packet映射成一个Frame，但也有例外：即当数据链路层执行拆分或将几个Packet合成一个Frame的时候。

数据链路层的PDU叫做Frame（帧）；

网络层的PDU叫做Packet（数据包）；

TCP的叫做Segment（数据段）；

UDP的叫做Datagram。（数据报）——在网络层中的传输单元（例如IP）。一个Datagram可能被封装成一个或几个Packets，在数据链路层中传输

帧和数据包都是数据的传输形式。帧，工作在二层，数据链路层传输的是数据帧，包含数据包，并且增加相应MAC地址与二层信息；数据包，工作在三层，网络层传输的是数据包，包含数据报文，并且增加传输使用的IP地址等三层信息。

# 子网

问题：

不同子网的主机如何通信？如何实际划分子网？

IP地址是以网络号和主机号来表示网络上的主机的，只有在一个网络号下的计算机之间才能“直接”互通，不同网络号的计算机要通过网关（Gateway）才能互通。但这样的粗略划分并不灵活，需要更精细的控制，为此IP网络还允许划分为更小的网络，称为子网（subnet）。

划分子网后，只有在同一子网的主机才能“直接”互通。

**拓展：**

# IP地址分类

|  |
| --- |
| IP地址根据[网络号](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%8F%B7)和[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)号的数量而分为A、B、C三类：IP地址用二进制来表示，每个IP地址长32bit，比特换算成字节，就是4个字节。例如一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址，人们处理起来也太费劲了。为了方便人们的使用，IP地址经常被写成[十进制](https://baike.baidu.com/item/%E5%8D%81%E8%BF%9B%E5%88%B6)的形式，中间使用符号“.”分开不同的字节。于是，上面的IP地址可以表示为“10.0.0.1”。IP地址的这种表示法叫做“[点分十进制](https://baike.baidu.com/item/%E7%82%B9%E5%88%86%E5%8D%81%E8%BF%9B%E5%88%B6)表示法”，这显然比1和0容易记忆得多。  A类IP地址  [A类IP地址](https://baike.baidu.com/item/A%E7%B1%BBIP%E5%9C%B0%E5%9D%80)：用可变的7位（bit）来标识[网络号](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%8F%B7)，可变的24位标识[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)号，最前面一位为"0"，即A类地址的第一段取值介于1～126之间。A类地址通常为大型网络而提供，全世界总共只有126个A类网络，每个A类网络最多可以连接16777214台主机。  B类IP地址  [B类IP地址](https://baike.baidu.com/item/B%E7%B1%BBIP%E5%9C%B0%E5%9D%80)：用可变的14位来标识[网络号](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%8F%B7)，可变的16位标识[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)号，前面两位是"10"。B类地址的第一段取值介于128～191之间(网络号不能以数字127开头，数字127是专门保留给诊断用的，如127.0.0.1是[回送地址](https://baike.baidu.com/item/%E5%9B%9E%E9%80%81%E5%9C%B0%E5%9D%80)，用于回路测试），第一段和第二段合在一起表示网络号。B类地址适用于中等规模的网络，全世界大约有16000个B类网络，每个B类网络最多可以连接65534台主机。  C类IP地址  [C类IP地址](https://baike.baidu.com/item/C%E7%B1%BBIP%E5%9C%B0%E5%9D%80)：用可变的21位来标识网络号，可变的8位标识[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)号，前面三位是"110"。C类地址的第一段取值介于192～223之间，第一段、第二段、第三段合在一起表示网络号。最后一段标识网络上的主机号。C类地址适用于校园网等小型网络，每个C类网络最多可以有254台主机。 |

**自己总结：**

IP地址采用“点分十进制”表示，根据网络号和主机号的数量一般分为A、B、C三类。

（|线自己加的做一个简单隔断，红色网络号，黑色主机号，共32bit，4字节）

A类IP地址： 0XXXXXXX|XXXXXXXX|XXXXXXXX|XXXXXXXX

B类IP地址： 10XXXXXX|XXXXXXXX|XXXXXXXX|XXXXXXXX

C类IP地址： 110XXXXX|XXXXXXXX|XXXXXXXX|XXXXXXXX

A类地址的第一位总是0，8位分配给网络号，24位分配给主机号。

B类地址的前两位总是10，16位分配给网络号，16位分配给主机号。

C类地址的前三位总是110，24位分配给网络号，8位分配给主机号。

十进制表示：

A类IP段　1.0.0.0 到126.255.255.255 (0段和127段不使用)

B类IP段　128.0.0.0 到191.255.255.255

C类IP段　192.0.0.0 到223.255.255.255

如： 202.105.139.140 (广东省深圳市电信)，该IP属于C类IP段，可通过十进制第一段取值介于192-223之间简单判断，可以通过对第一段202进行短除法（除2）换算成二进制的11001010来判断。

注：十进制转二进制高位补零，如52转为二进制时结果是00110100.

# 子网掩码

|  |
| --- |
| 子网掩码(subnet mask)又叫网络掩码、地址掩码、子网络遮罩，它是一种用来指明一个IP地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的位掩码。子网掩码不能单独存在，它必须结合IP地址一起使用。子网掩码只有一个作用，就是将某个IP地址划分成网络地址和主机地址两部分。  子网掩码是一个32位地址，用于屏蔽IP地址的一部分以区别网络标识和主机标识，并说明该IP地址是在局域网上，还是在远程网上。  **规则**  子网掩码的设定必须遵循一定的规则。与二进制IP地址相同，子网掩码由1和0组成，且1和0分别连续。子网掩码的长度也是32位，左边是网络位，用二进制数字“1”表示，1的数目等于网络位的长度；右边是主机位，用二进制数字“0”表示，0的数目等于主机位的长度。这样做的目的是为了让掩码与ip地址做按位与运算时用0遮住原主机数，而不改变原网络段数字，而且很容易通过0的位数确定子网的主机数（2的主机位数次方-2，因为主机号全为1时表示该网络广播地址，全为0时表示该网络的网络号，这是两个特殊地址）。只有通过子网掩码，才能表明一台主机所在的子网与其他子网的关系，使网络正常工作。 |

**表示方式：**

子网掩码通常有以下2种格式的表示方法：

1． 通过与IP地址格式相同的点分十进制表示

如：255.0.0.0 或255.255.255.128

2． 在IP地址后加上"/"符号以及1-32的数字，其中1-32的数字表示子网掩码中网络标识位的长度

通过“IP+/网络标识位的长度”，可以知道主机的IP地址及子网掩码。并能知道其所在的网络地址（IP地址 & 子网掩码,二进制计算）。

华分子网后，不同子网的子网掩码可能相同也可能不同。子网掩码相同不表示在同一子网。

如：192.168.1.1/24 的子网掩码也可以表示为255.255.255.0

子网掩码一般为255.255.255.0

划分子网将产生子网掩码，子网掩码的作用就是用来判断任意两个IP地址是否属于同一个子网络，这时只有在同一个子网的计算机才能“直接”互通。那么如何确定子网掩码呢？

|  |
| --- |
| 前面讲到IP地址分网络号和主机号，要将一个网络划分为多个子网，因此网络号将要占用原来的主机位，如对于一个C类地址，它用24位来标识网络号，要将其划分为2个子网则需要占用1位原来的主机标识位。此时[网络号](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%8F%B7)位变为25位，[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)标示变为7位。同理借用2个主机位则可以将一个C类网络划分为4个子网……那计算机是怎样才知道这一网络是否划分了子网呢？这就可以从子网掩码中看出。子网掩码和IP地址一样有32bit，确定[子网掩码](https://baike.baidu.com/item/%E5%AD%90%E7%BD%91%E6%8E%A9%E7%A0%81)的方法是其与IP地址中标识网络号的所有对应位都用"1"，而与主机号对应的位都是"0"。如分为2个子网的C类IP地址用25位来标识网络号，则其子网掩码为：11111111 11111111 11111111 10000000即255.255.255.128。于是我们可以知道，A类地址的缺省子网掩码为255.0.0.0,B类为255.255.0.0,C类为255.255.255.0。下表是C类地址[子网划分](https://baike.baidu.com/item/%E5%AD%90%E7%BD%91%E5%88%92%E5%88%86)及相关子网掩码：  子网位数 　子网掩码 　[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)数 可用主机数 子网数  1 　255.255.255.128 　128 　 126 2  2 　255.255.255.192　 64 　 62 4  3 　255.255.255.224 　32 　 30 8  4 　255.255.255.240 　16 　14 16  5　 255.255.255.248 　8 　 6 32  6 　255.255.255.252 　4　 　 2 64 |

**自己总结：**

C类缺省子网掩码为255.255.255.0，是因为缺省没有对该C类IP地址进行子网划分。

# 网段

同一网段指的是IP地址和子网掩码相与得到相同的网络地址。想在同一网段，必须做到网络标识相同。各类IP的网络标识算法都是不一样的，需要根据子网掩码的位数来判断。

同一网段：判断两台主机在不在同一网段可以使用掩码计算，即网络地址=IP地址 & 子网掩码。如果两主机的网络地址（或称网络标识）相同则是同一网段，如果不同就是不同网段。

如：如：IP1=192.168.1.15/25与IP2=192.168.1.156/25，经过计算IP1的网络地址是192.168.1.0，而IP2的网络地址是192.168.1.128，因此它们不在同一个网段。如果掩码是24（255.255.255.0）则它们的网络地址都是192.168.1.0，那么它们就在一个网段。

**拓展：**

# 同网段和不同网段设备通信原理详解

|  |
| --- |
| 在当今的以太网络通信中，在IP数据包中有两个必不可少的地址，那就是IP地址和网卡地址（即MAC地址），在数据包中，无论是IP地址还是MAC地址，都有源地址和目标地址，因为通信是双方的，所以就必须同时拥有双方的地址！在同一IP网络中通信，将会发生以下事件：  主机A与主机B通信，这时主机A肯定首先要封装这些需要发给主机B的数据包，那么对于主机A来说，自己的IP地址和MAC自己肯定能够轻易得到，对于主机B的IP地址这时主机A也应该知道，要不然它就不清楚自己将要和谁通信，当有了自己的IP地址，MAC地址以及主机B的IP地址后，主机A在数据包中可以正确地写上源IP地址，目标IP地址，接下来的工作就是写入自己的MAC地址（即源MAC），最后还必须正确写入目标主机B的MAC地址，可这时主机A才发现自己根本没有目标主机B的MAC地址，那该怎么办呢？这时主机A就通过比较上面已经封装好的源IP和目标IP，通过子网掩码计算一下，发现源IP和目标IP恰好在同一个IP网络内，那么它想要得到目标主机B的MAC地址就有办法了，首先主机A就向本网段发过一个ARP请求，这个ARP请求包中包括主机A的源IP地址，源MAC地址，目标主机B的IP地址，而目标MAC地址为广播MAC地址（全部为F），因为我们要找的就是目标MAC，所以这里用广播MAC地址，又因为是以太网，所以整个局域网的所有主机都能收到这个请求MAC地址的数据包，当然主机B也能收到，因此在主机B收到此ARP请求后，立即构建一个包括自己的MAC地址的ARP回应包，回应给主机A，当主机A收到这个ARP回应后，终于完成了找寻目标MAC的重大任务，从而把目标主机B的MAC地址正确封装进上面还未封装结束的正准备发给主机B的数据包，在这时，源IP和源MAC以及目标IP和目标MAC都已正确存在于数据包中，那么这里主机A向网络内发出这些数据包，因为目标地址在本网段，所以本网段所有主机都能收到这个数据包（这是以太网的特性），最后只有真正的目标主机B能够打开这些数据包，在此，同网段两台主机之间的通信就此圆满结束！  在这里应该注意另外一个问题，因为主机A要寻找的目标主机B在同一网络，所以主机A能够通过ARP得到目标主机B的MAC地址，从而完成通信，当主机A在封装数据包时检测到目标主机并不在本网段，在这时，数据包不能把目标主机的MAC地址顺利封装进去，那么就用到另一种方法，那就是网关，主机A在准备发向主机B的数据中，封装好自己的IP地址和MAC地址，同时也封装好目标主机B的IP地址，数据包封装到这里，主机A就利用上面得到同网段目标主机B的方法去请求得到网关的MAC地址，同样也是用ARP去广播，因为网关必须和本机在同一网段，理所当然，网关能够收到这个ARP请求并能正确回应给主机A，这时主机A在数据包中封装好自己的IP地址和MAC地址，同时也封装好目标主机B的IP地址和网关的MAC地址，把数据包从网卡发出去，因为目标MAC是网关的，所以网关收到这个数据包后，发现目标MAC是自己，而目标IP却是别人，所以它不可以再往上打开这个数据包，它要做的工作就是把这些数据包发给下一跳路由器（如果网关自身就是一台路由器的话），如果网关是一台普通PC，那么它就发给路由器，让路由器把这些数据包正确传输到远程目标网络，到达远程网络后，它们的网关再将数据包发给数据包中的目标IP，即源主机A苦苦寻找的目标主机B，从而真正结束不同网络之间的通信，回应的数据包也是用同样的方法到达目的地，在这里，还需要注意的是，当网关把数据包发给下一跳路由器时，这个数据包必须由网关把目标MAC改成下一跳路由器的MAC地址（通过ARP得到），而源端MAC改成发出端口的MAC地址，否则下一跳路由器收到目标MAC不是自己的数据包，会丢弃不予理睬，下一跳路由器再发给下一跳路由器同样要把目标MAC地址改为下一跳路由器的MAC地址再发出去！  最后还可以总结出：在网段通信时，数据包中的地址就是源IP，目标IP，源MAC，目标MAC，根本用不到网关，而当检测到需要把数据包发到远程网络时，这时，目标MAC就必须改变了，在还没有出内网时，目标MAC必须写成网关的MAC地址发出去，当网关收到时，再把目标MAC地址改成下一跳的MAC地址发出去，同时源MAC地址要始终保持为发出端口的MAC地址（回应报文可以依靠它路由回去），而源IP及目标IP不曾改变（用于判断收到数据包的本机IP和数据包IP是否一致，若一致不转发），就算到达了公网上，目标MAC仍然在不断改变着，直到最后，这个数据包到达目标IP的网络，最终通信结束！ |

**自己总结：**

同一网段：主机A->主机B

不同网段：主机A->网关->主机B

# 网段和子网

子网是网络层的概念，网段是物理层的定义。

在不要求精确性的情况下，子网、局域网和网段可以理解为同一个意思，但是同一个局域网/同一个子网/同一个网段 和 同一个网络不是同一个概念

# 网关

网关（Gateway）[1] 就是一个网络连接到另一个网络的“关口”。也就是网络关卡。

那么网关到底是什么呢？网关实质上是一个网络通向其他网络的IP地址。比如有网络A和网络B，网络A的IP地址范围为“192.168.1.1~192. 168.1.254”，子网掩码为255.255.255.0；网络B的IP地址范围为“192.168.2.1~192.168.2.254”，子网掩码为255.255.255.0。在没有路由器的情况下，两个网络之间是不能进行TCP/IP通信的，即使是两个网络连接在同一台交换机（或集线器）上，TCP/IP协议也会根据子网掩码（255.255.255.0）判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信，则必须通过网关。如果网络A中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B的某个主机（如附图所示）。网络A向网络B转发数据包的过程。

所以说，只有设置好网关的IP地址，TCP/IP协议才能实现不同网络之间的相互通信。那么这个IP地址是哪台机器的IP地址呢？网关的IP地址是具有路由功能的设备的IP地址，具有路由功能的设备有路由器、启用了路由协议的服务器（实质上相当于一台路由器）、代理服务器（也相当于一台路由器）。