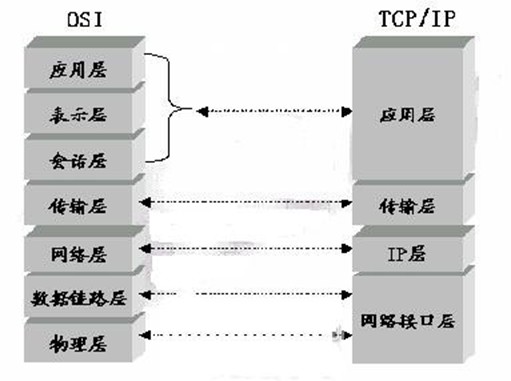
从Wireshark的抓包分析了解网络的分层结构

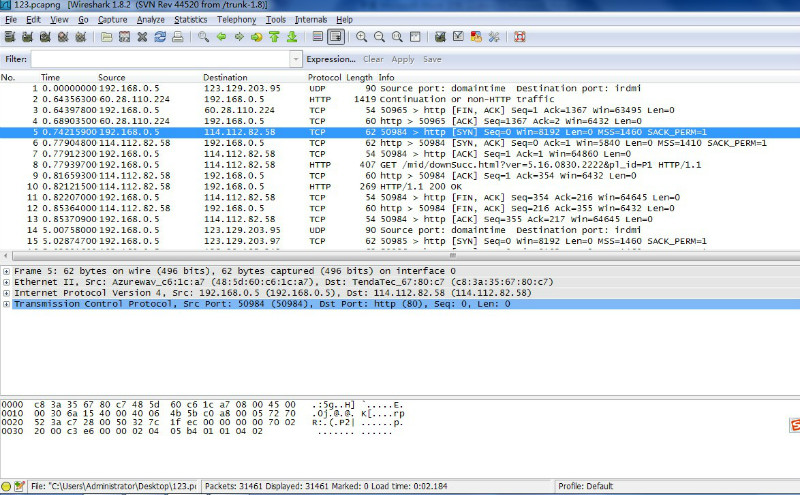
http://edu.qzs.qq.com/ac/b.gif

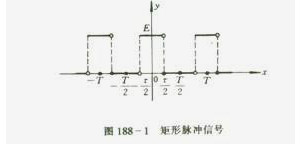
抓包分析,又叫网络嗅探,在计算机网络安全领域,属于被动攻击。即在不干扰正常信息流的前提下,监听整个局域网的通信内容。同时，监听者还可以观察和分析某个PDU（protocol date unit）的协议信息控制部分，了解正在通信的协议实体的地址和身份，研究PDU的长度和传输的频度，以便了解所交换数据的某种性质。

仅从学习的角度来讲，通过抓包分析，可以清楚地了解网络协议的性质及网络的分层结构。  


网络模型主要有两种，即OSI的七层模型和TCP/IP协议簇的四层模型。由于TCP/IP协议簇是互联网上的事实的标准协议，故本文按TCP/IP的体系结构讲述。但为了把原理描述清楚，将网络接口层分为数据链路层和物理层来讲。  
 

为讲解方便，先来了解笔者电脑的一些参数。  
 

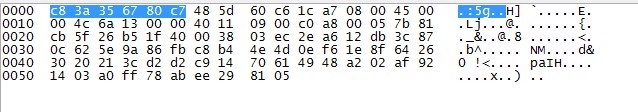
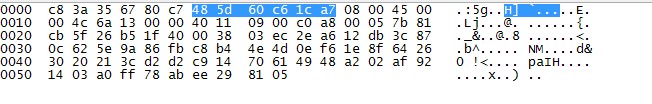
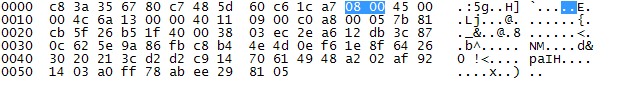
当开始抓包后，我们可以看到如下信息。  


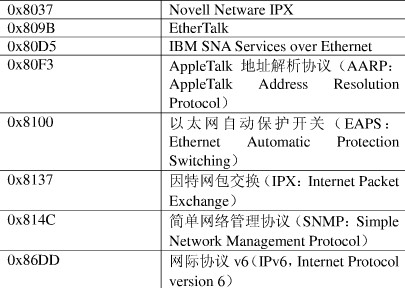
这是在网络接口层抓取到的信息，也就是数据链路层的数据帧，除去前面0000、0010、0020、-------等为帧同步信息外，其他皆为数据中的内容，全部用十六进制表示，这便是数据在链路层的表示形式，当数据链路层把这些十六进制数据交给物理层来发送时，要把十六进制转化为二进制，即c8 3a ………..化为11001000、00111010、……….等，在物理层1、0分别表示高、低电平，一般是一连串矩形脉冲波。  
 

称为数字基带信号。在传输时，根据不同的介质选择不同的调制方式。在有线局域网中，一般用曼彻斯特和差分曼彻斯特编码。在光纤中传输时，用波分复用技术。而在无线局域网中，用CCK(补码键控)、OFDM(正交频分复用技术)和多入多出(Multiple-Input Multiple-Output)技术

。由于信号的调制与解调涉及复制的数学运算和通信的专业知识，这里不做讨论。有兴趣的读者可以再任何一本《通信原理》书中找到相关内容。

在数据链路层，PDU被称为数据帧，有帧首部、数据部分和帧尾部组成，其中数据部分为ip数据包,帧头和帧尾为帧控制和校验信息。由于数据链路层有许多帧类型，如ppp帧、以太网帧等，所以各种帧的控制信息并不相同，但无论那种帧格式，大致都要实现封装成帧、透明传输和差错控制等功能。因此下面以以太网帧为例。

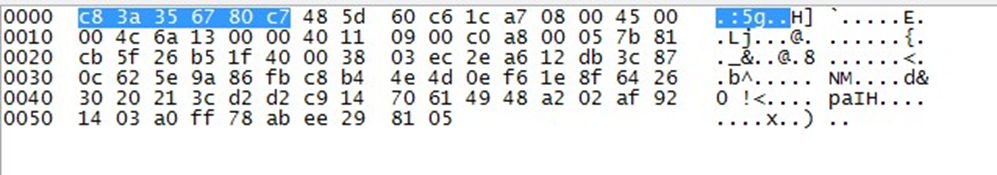
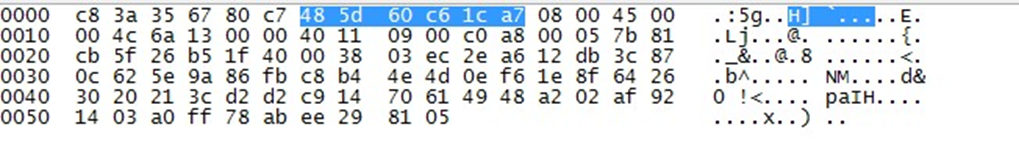
以太网帧的首部有目的地址、源地址、协议类型组成，在抓取的数据包中分别为.  
  
  
  
  
  


由图可知，以太网帧的地址为物理地址，有48为二进制数组成，化为十六进制恰为12位，协议类型有两个字节（16个二进制）组成，其中0800代表该帧的数据部分存放的为ip数据包，如为其他数值，则代表不同的网络层数据.下面是常见的协议代码.  
  
  
  


在研究帧在数据链路层的传输时，我们说数据帧每过一个路由器就换一次物理地址，


以上三个截图分别是本机无线网卡、无线AP接入点、路由器的物理地址（MAC地址）

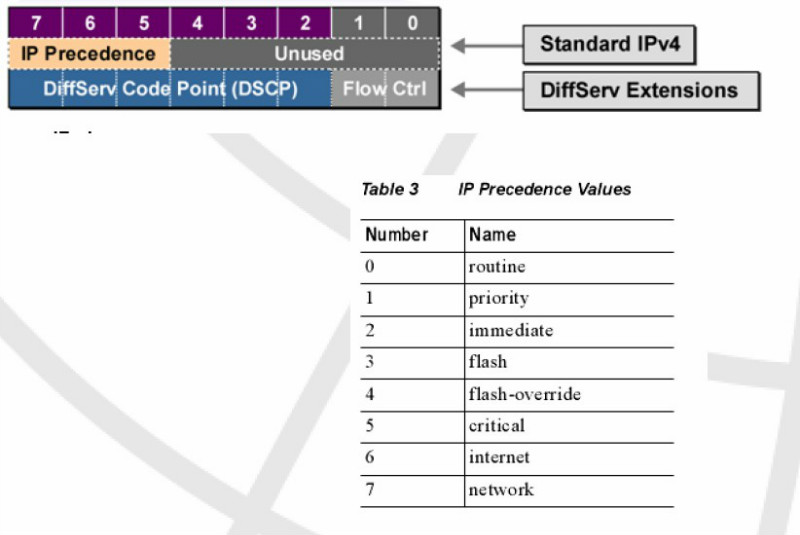
下面的图为抓取的数据  
  
  
  


两个蓝色部分对应的路由器和本机无线网卡的硬件地址，在抓取的三万多数据帧中，只有这两个物理地址而没有出现无线接入点AP的MAC地址94  44  52  B8  39  CB。这就说明MAC地址没过一个路由器就会改变，也说明数据帧经过接入点、交换机时，不改变物理地址，交换机虽有MAC地址，却用于其他用途。

当程序识别出0800字段后，便会把前面的数据删除掉（包括0800），将后面的数据交给网络层。  
                              网络层

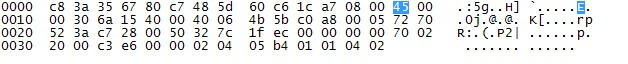
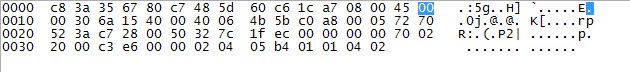
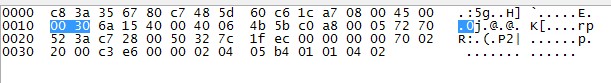
ip数据包。其首部结构如下图。



其中，ip的版本只有ipv4和ipv6，故第一个十六进制数应为4或6，ip数据包的首部长度介于20~60个字节，且单位为4字节，故第二个十六进制数应在5~F之间。8位服务类型主要用于提供qos服务，在一般情况下，前三位表示ip优先级，后五位不用，而在区分服务模型中，用前六位表示优先级（DSCP）,后两位用于流控制（显式拥塞通知）  


同时ip优先级和DSCP有一定的映射关系。关于8位TOS如何使用，可以去查阅Qos方面的书籍，本文不深入讨论。

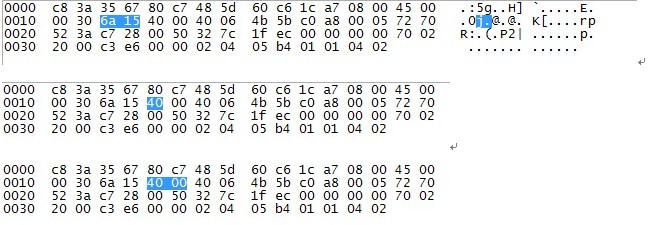
 16位总长度是指ip数据包的总长度，一般小于1500字节。

以上三个图的蓝色部分表示该数据包是一个ipv4包，且头长度为20个字节，ip优先级为普通，总长度192个字节。

16位标识符用于标记ip数据包的顺序，用于数据分段，一个数据报在传输过程中可能分成若干段，标识符可以区分某分段属于某报文，一个数据报的所有分段具有相同的标识符。

3位标志中，只有两位能用，中间位DF=1时，表示该数据不能再分割了，最低位MF=1时，表示该数据是一个大数据中间的一小段，后面还有分片。13位片偏移指出了该分段在原数据报中的相对位置，以8字节为偏移单位。



上面三个图表示抓取到的该数据包是一个大数据报的号码为27157（0X6a15）,40 00 化为二进制为0100 0000 0000 0000 ，DF=1、MF=0，表示不能分片、且后面没有分片。这三幅图加在一起说明序号为27157的数据报仅有这一片。

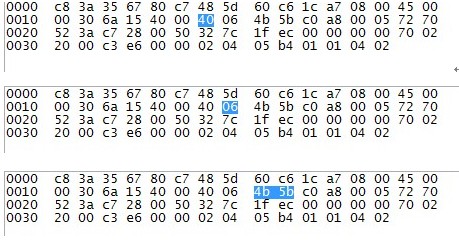
TTL最初表示数据报在网络中的存活时间，现在改为跳数限制，即一个数据包在网络中最多经过路由器的个数，最大为255。



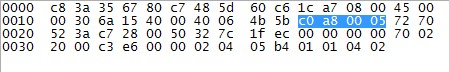
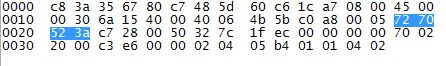
从上图可以知道，从本机到百度的其中一个服务器或服务器群，要经过9个路由器，且百度的该服务器用的是window的操作系统。

8位协议指出了ip的数据部分包含的是什么，如TCP为6，UDP为17 。OSPF为89 。

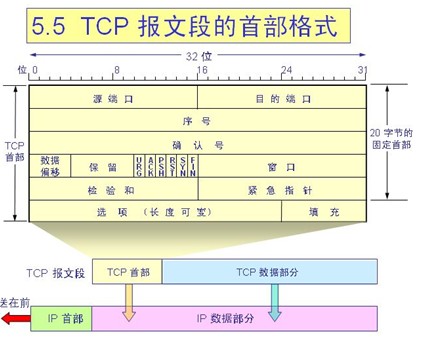
16位的首部检验和是为了检验ip首部在传输的过程中是否出错，由于TTL每过路由器就会改变，因此检验和也要每次都计算。



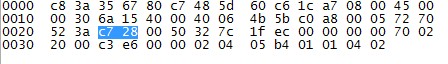
这三个图表明该数据包TTL为64，运输层使用TCP协议，且该数据包在传输时ip包头错误，因此是要被丢弃的数据。

源ip和目的ip为机器在互联网中唯一的逻辑地址。选项部分有严格源路由、松散源路由和时间戳，除了打游戏时用的网游加速器使用了源路由外，一般生活中使用的数据选项都为空。  
  
  
  
  
  
上面的两个图表明源ip和目的ip为192.168.0.5   114.112.82.58。选项为空字节。

                                            运输层



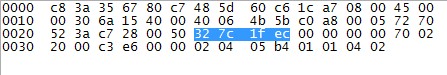
源端口和目的端口都表示一个应用进程的接口，其中源端口只具有本地意义，即在同一台电脑上区分不同应用进程的通信。而目的端口一般为知名端口（Well-known port number）。

  
  
  
  
  
  
  
图片

由上图可以看出，这是一个http网页服务数据。50984（c7 28）为本机的浏览器开放的一个临时端口，目的端口为80端口，即一个网页请求。

32位序号占4个字节,使用mod2^32运算。TCP面向字节流，所以在TCP连接中传送到每一个字节都要按顺序编号，这样也可以保障TCP的可靠传输。4字节的确认号是和序号配合使用的。表示接收方期望收到的下一个报文段的第一个数据字节的序号。如：接收方收到一个序号为2000，长度为500字节的一个数据，那他给发送方的确认号应为2501。

4位的数据偏移指明了TCP报文段的数据部分的起始处距离TCP报文段的起始处有多远，即指TCP报文的首部长度。保留的六位现在没有定义用途，全部置为0。

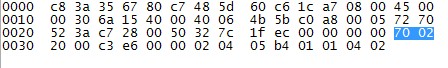
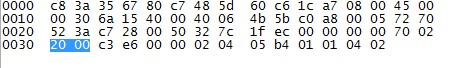
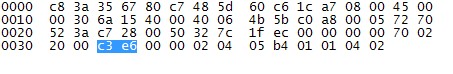


有图知，蓝色部分为序号，后面的8个0为确认号。由以上两点知，该数据的传输出现了差错。

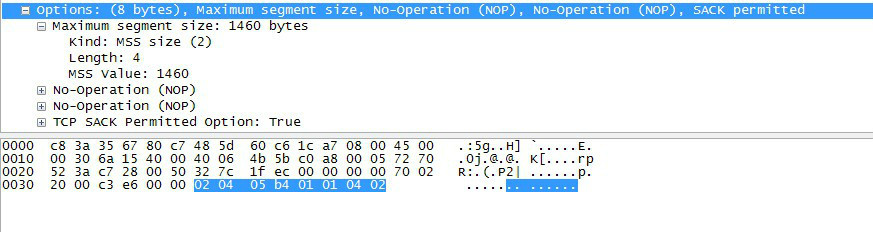
图片

 70 即0111 0000 表示该TCP报文首部长度为28个字节保留位全部置零。

接下来的六个控制位，分别为URG（紧急）、确认ACK、推送PSK、复位RST、同步SYN、终止FIN，每个占一位。当U RG=1时，表明该字段有效，它告诉系统此报文段有紧急数据，应立即传送，一般和后面的紧急指针配合使用。后面的几个控制功能，都和TCP的工作机制有关，由于TCP是面向连接的，可靠的传输协议，便需要确认、重传、流量控制、拥塞控制等，其他协议不需要的功能，以保证其可靠性。

窗口机制是为了接收已发送数据的确认信息而设计的，TCP的可靠传输，需要确认机制，如果每发送一个数据，就停下来等待确认信息，那么TCP的传输效率将会很低，如果一直传输数据而不等待确认信息，则无法保证可靠性。窗口机制属于一种折中方案，在保证可靠性的前提下兼顾效率。窗口值的大小决定了在收到已发送的数据的确认之前，还能传输多少数据，当传输的数据达到窗口值却仍没有收到以前数据的确认信息时，TCP歇息就会停下来等待确认信息。关于TCP可靠传输的实现细节与原理，是TCP协议的精髓所在，由于其非常复杂，限于篇幅，这里不讨论。  
  
  
  
  
  


上面的三个图说明：02表示0000 0010，即URG=0、ACK=0、PSK=0、RST=0、SYN=1、FIN=0。说明这是一个http的连接请求报文段。20 00 为窗口值，大小为2\*16^3=8192，即再接收到该数据的确认前，还可在发送8192字节的数据。C3 e6 为检验和，与ip的检验和大致一样，都使用循环冗余检验（CRC），不同的是ip只对包头做CRC检验，而TCP对整个数据做CRC检验。



最后这幅图蓝色表示的是TCP的选项部分，长度可变，包含最大数据尺寸、MSS、TCP的SACK等内容，也涉及了TCP的传输原理，这里不讨论。

                                                      应用层

运输层为应用层提供通信服务，属于面向通信部分的最高层，同时也是用户功能中的最底层。其实到应用层以后，就和通信的关联不大了。运输层将数据交给应用层后，操作系统便会通过window的应用程序接口（API）将数据转交给相应的应用进程（假设机器用的是微软的操作系统），浏览器的数据给浏览器，QQ的数据交给QQ程序。然后数据在各自的应用程序中经过各种各样的加工和处理后，还原出来我们发送的最原始的信息。

这便是数据在经过网络传输时所经过的详细的变化过程，由于作者水平有限，难免会挂一漏万。文中如有错误之处，希望大家多多批评指正。