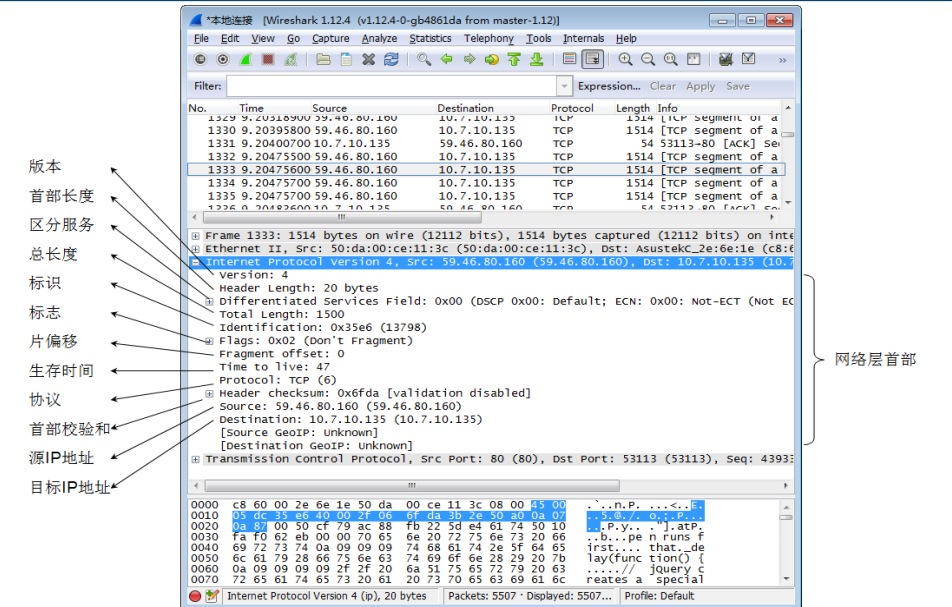
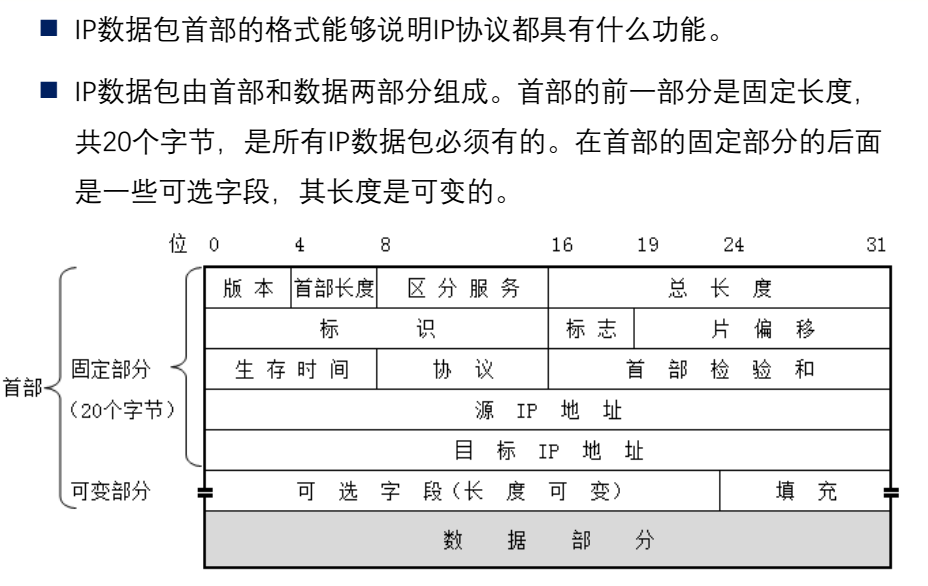


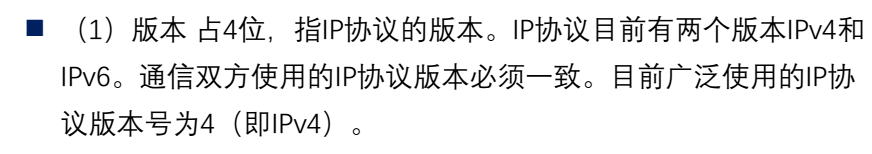
网络层的协议部分

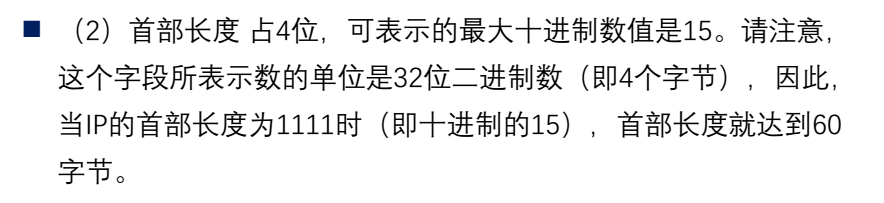
ARP为IP协议提供服务，IP协议为ICMP/IGMP提供服务

IP协议是一个统称，包含RIP OSPF协议等等。。。

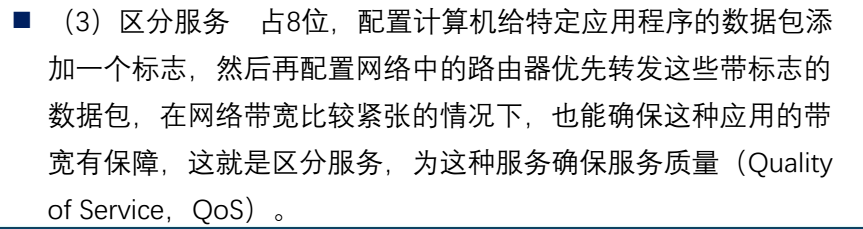




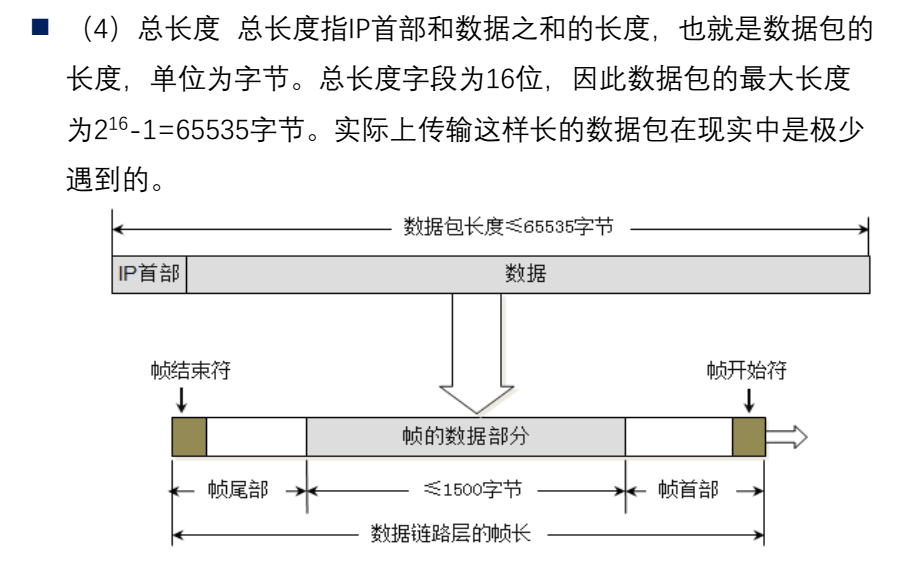




首部长度代表的十进制数 \* 4个字节 = 首部的长度 （基本都是20个字节）



感觉就是优先服务的意思，加个标记来进行区分服务。必须是路由器支持才行。

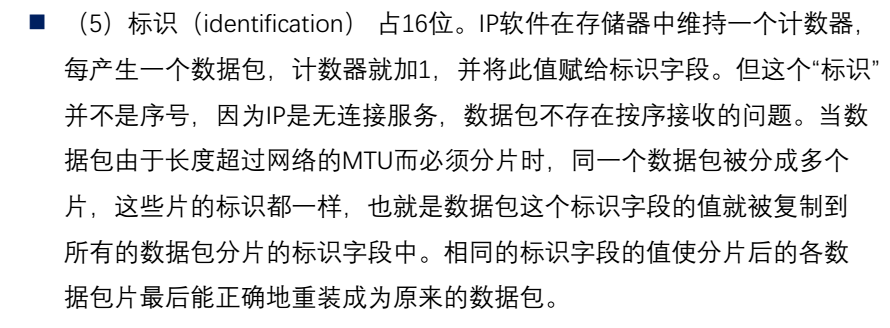


总长度其实就是加上数据包的总共的长度.最大的取值是65535个字节.

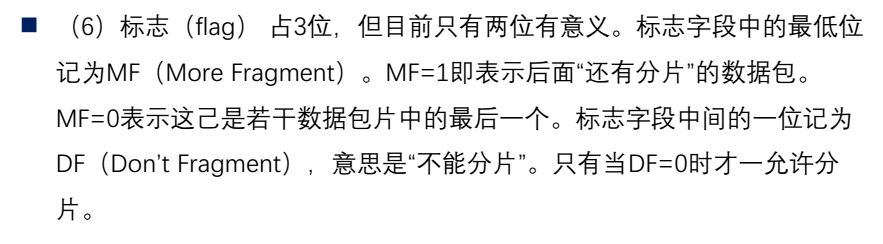
数据链路层中，以太网网卡接口能传输的最大数据长度是1500个字节，所以，理论上来讲的话，网络层的总长度最好也不要超过1500个字节，不要让网络层去分片。

网络层负责分片，组合分片...

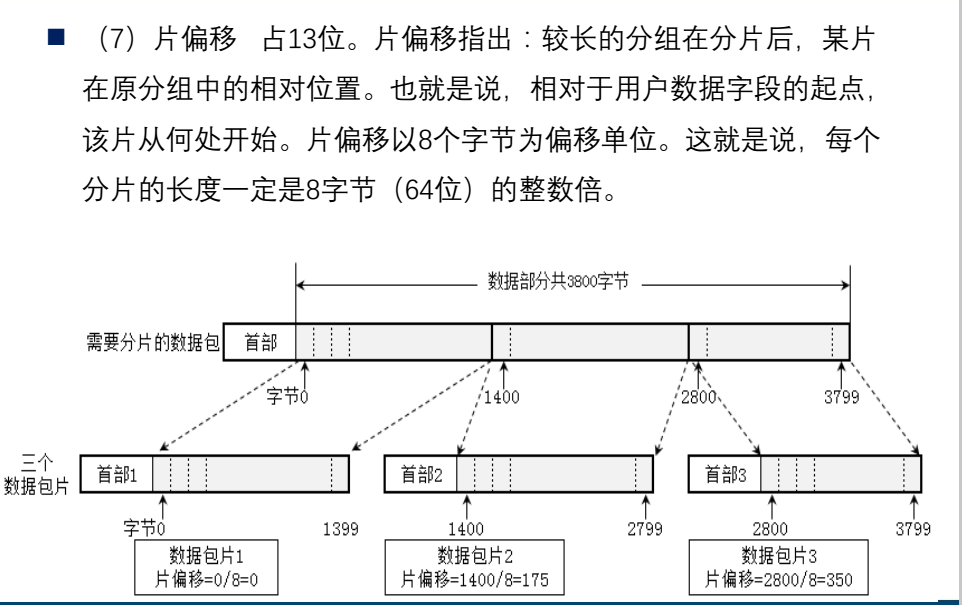
网络层分片根据标识来进行.....



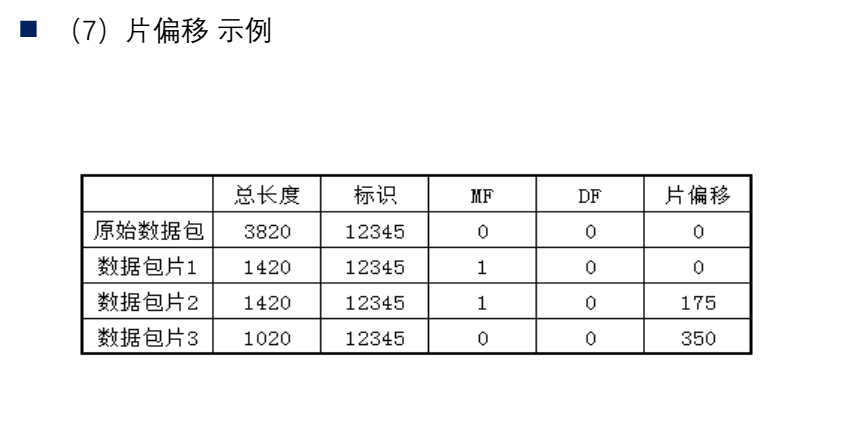
一个数据包有相同的标识



假设4000字节的数据，肯定要网络层进行分片，网络层分为1500,1500,1000三个片，对于前两个，标志位MF都是1，最后一个标志位MF为0,DF都为0

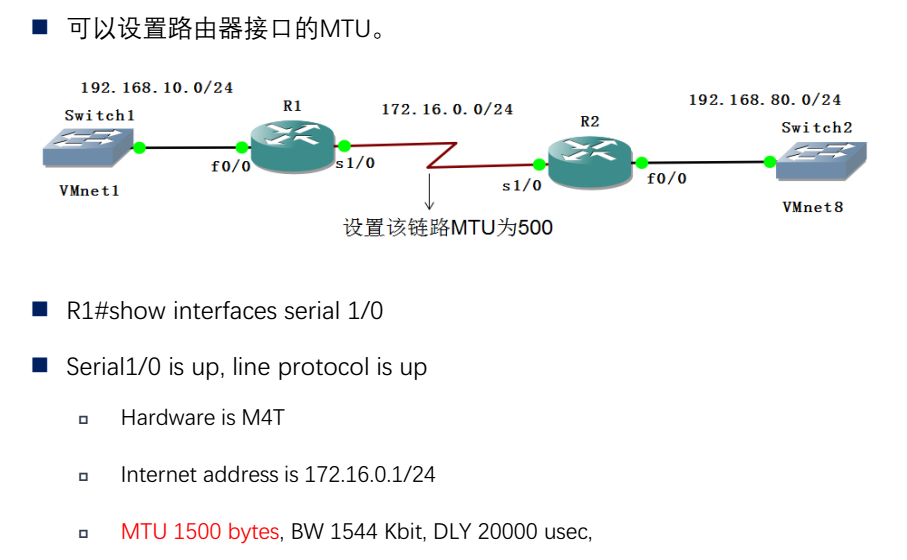


偏移是以8字节为单位的，所以，偏移的量要除以8，最终算出偏移的长度.



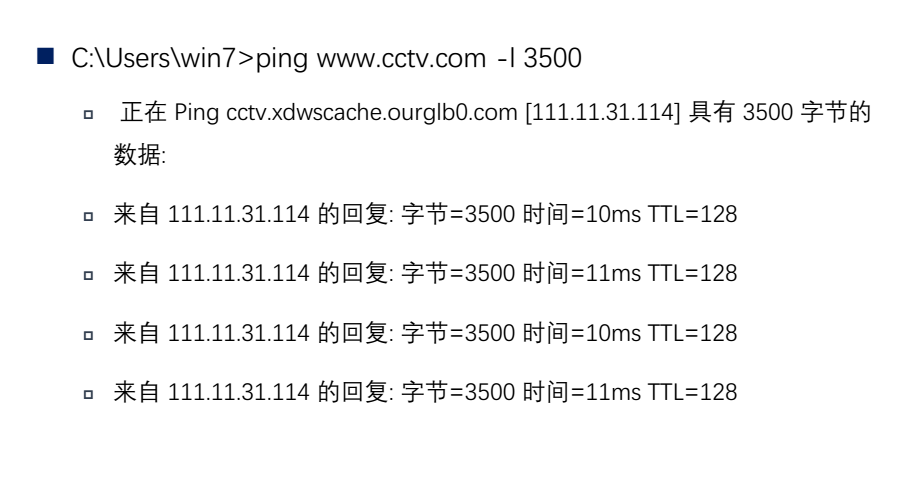
实战----观察路由的分片

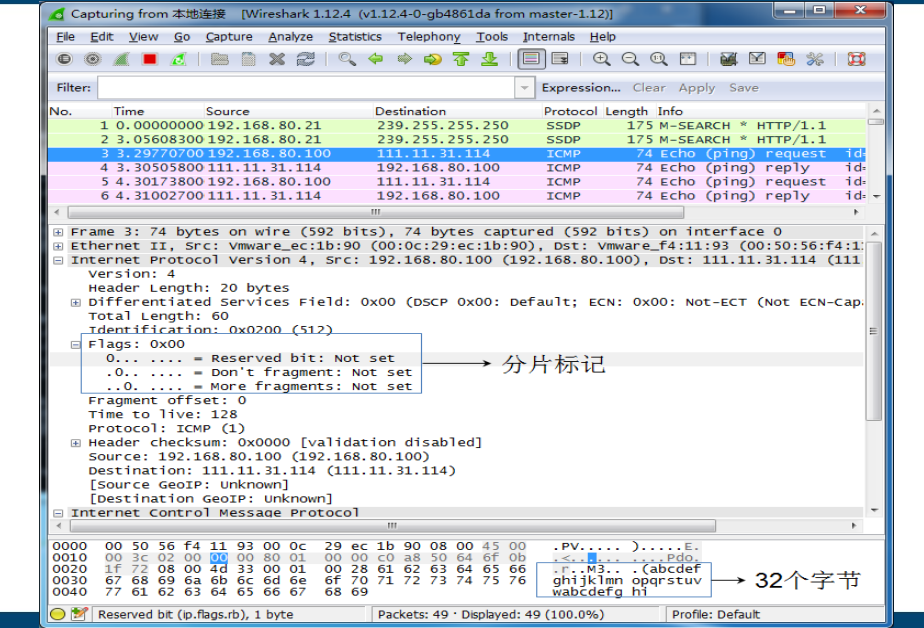
1. 设置路由的MTU

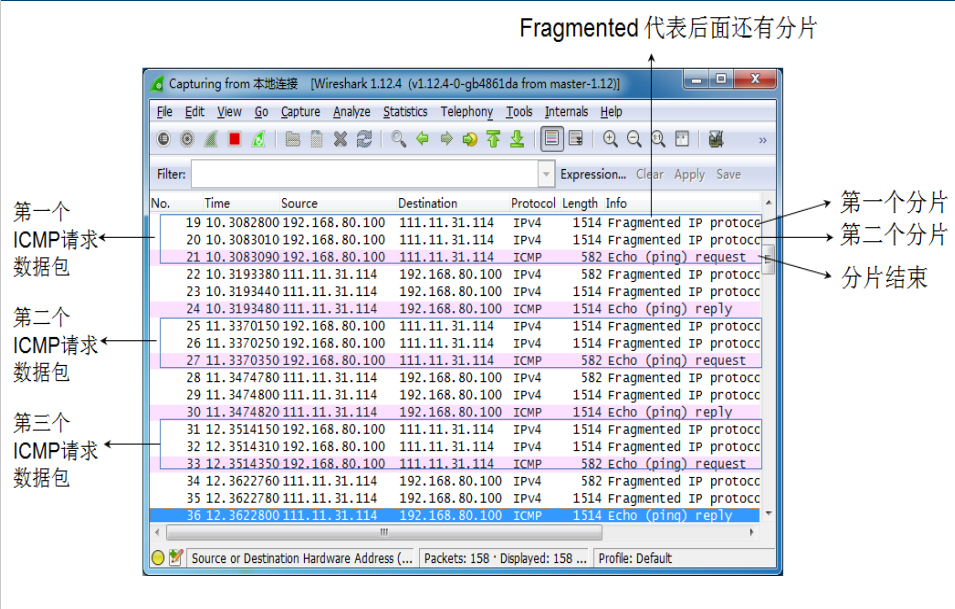


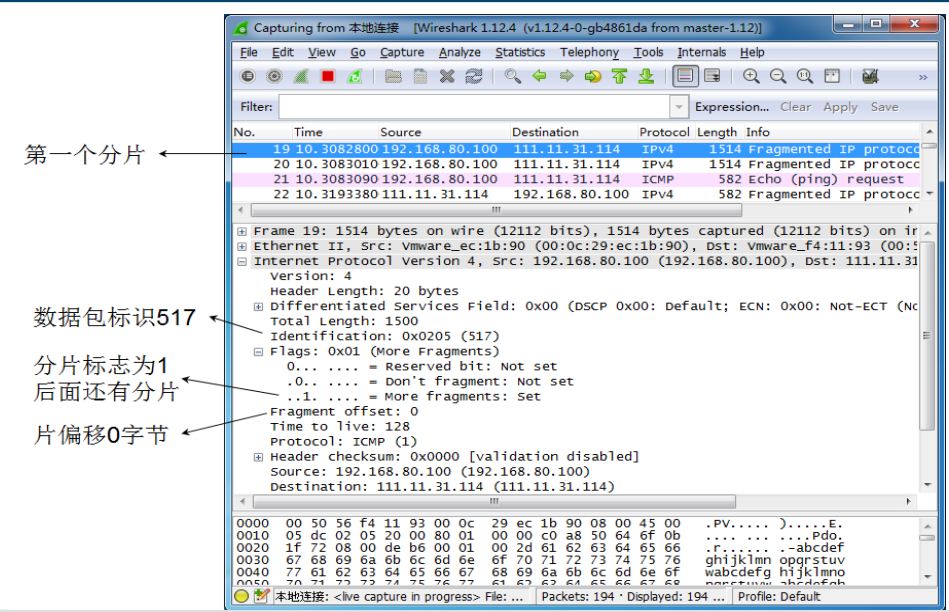


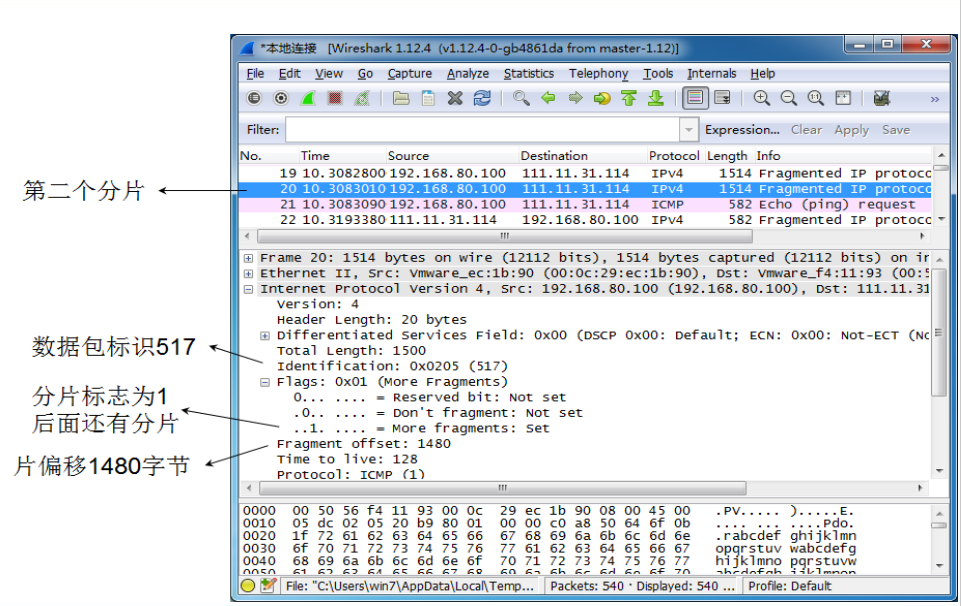
1. 观察路由的分片

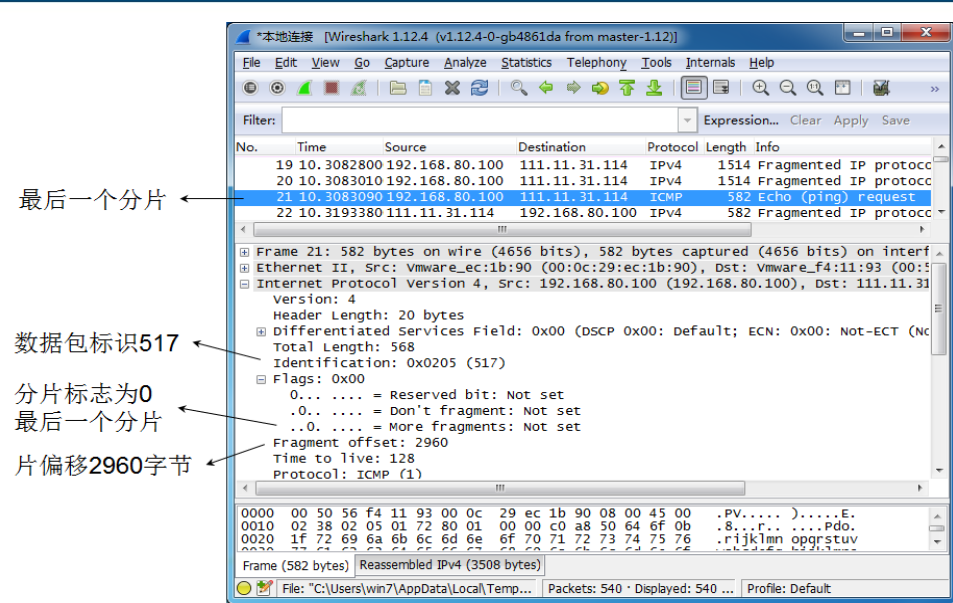


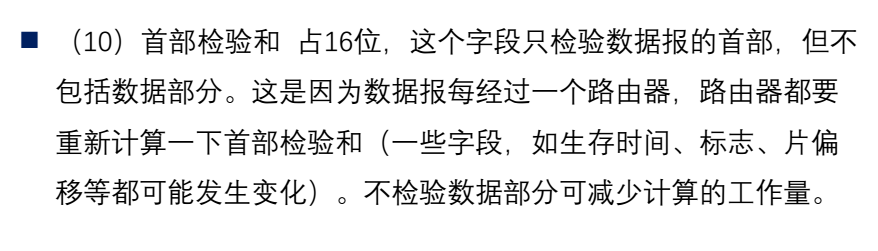
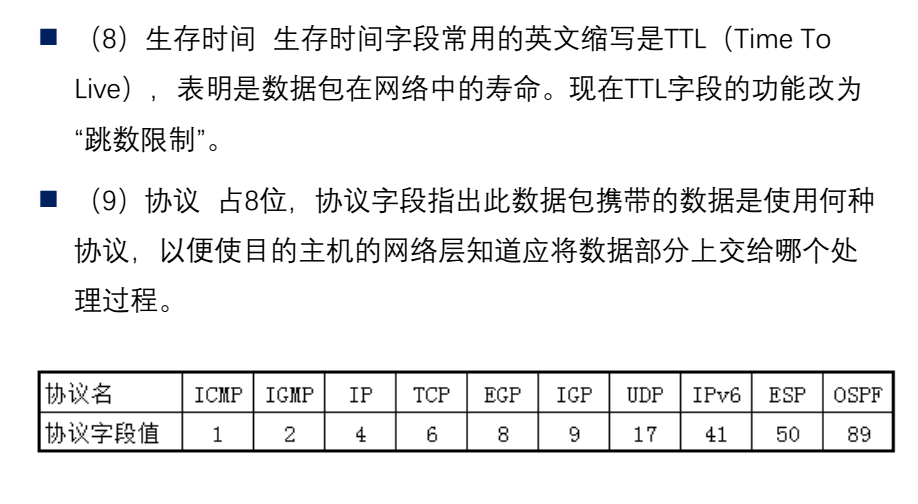




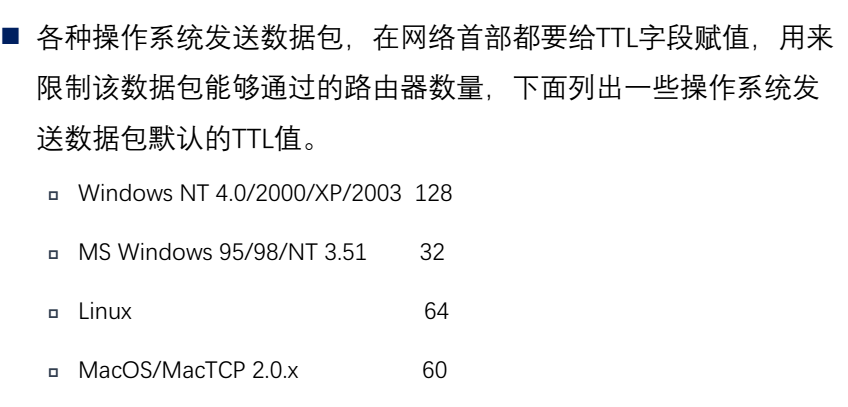








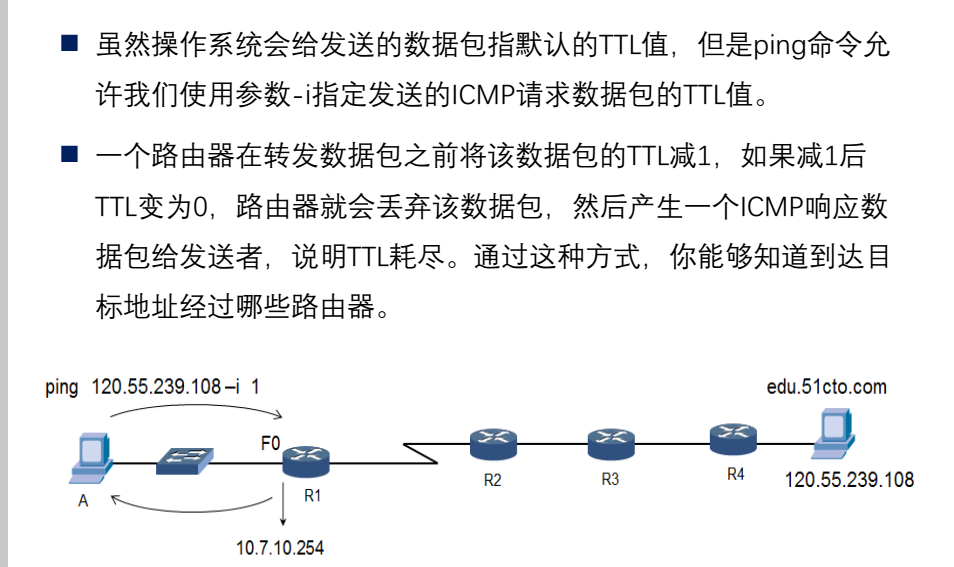
TTL实战----查看TTL生存时间

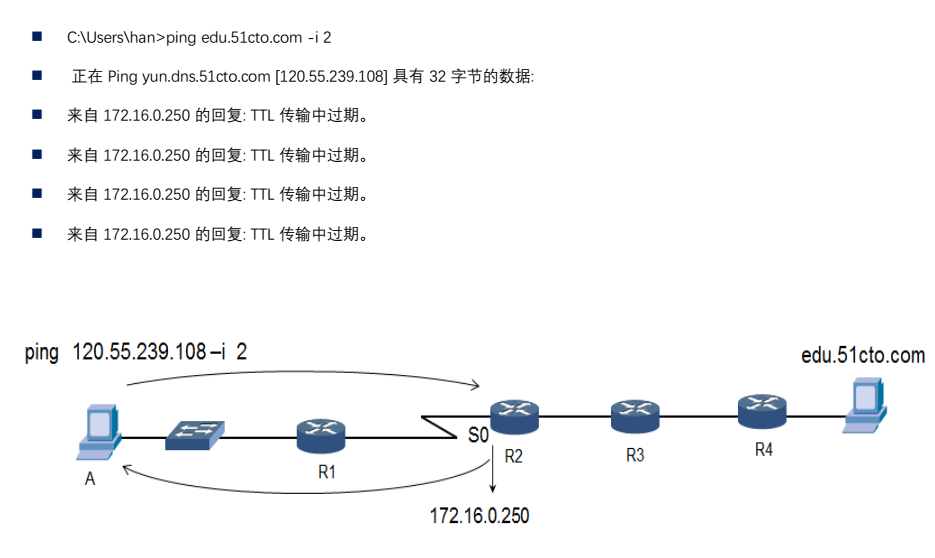


各个操作系统的默认TTL值，操作系统默认，如果大于TTL的值，就把数据包扔掉了。

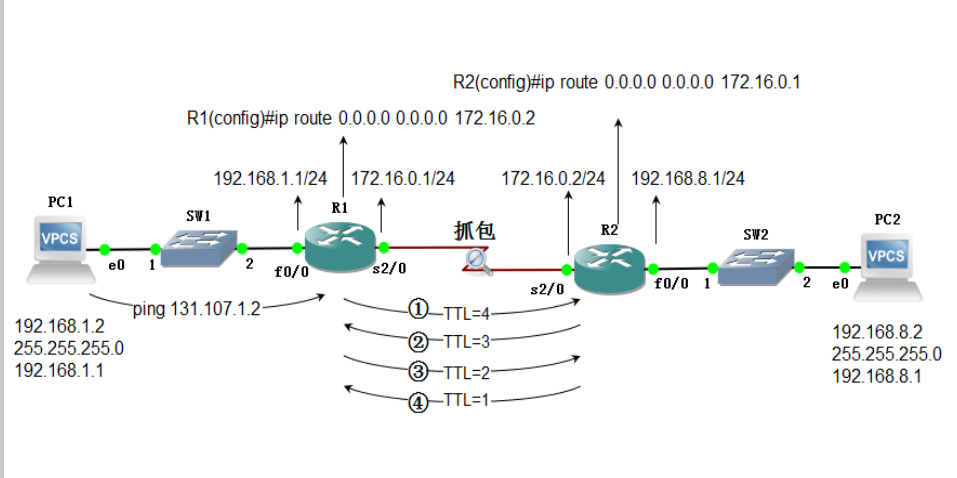


从右往做看，TTL的值最后的值会显示在PING中。每经过一个路由器，TTL的值就会减1



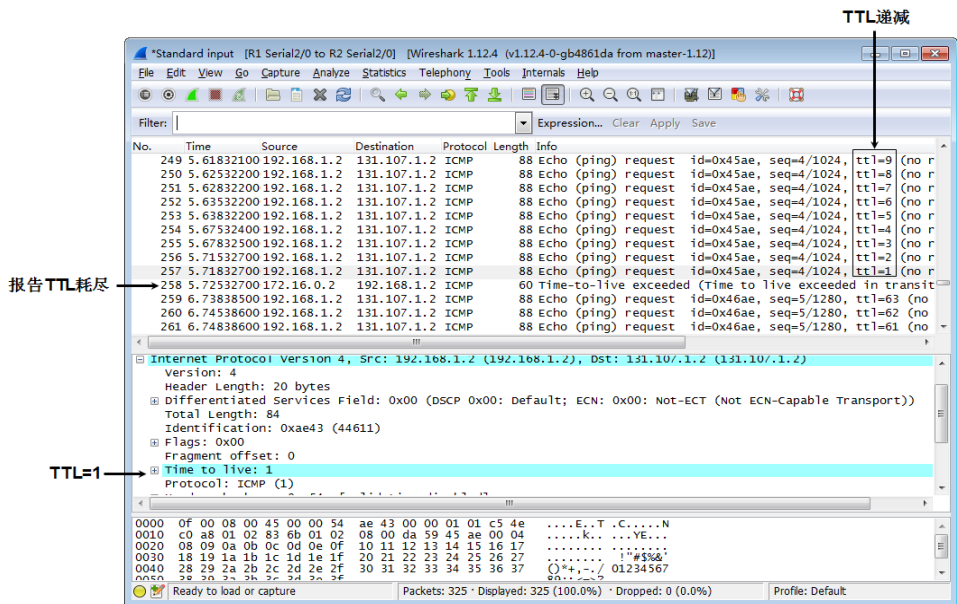






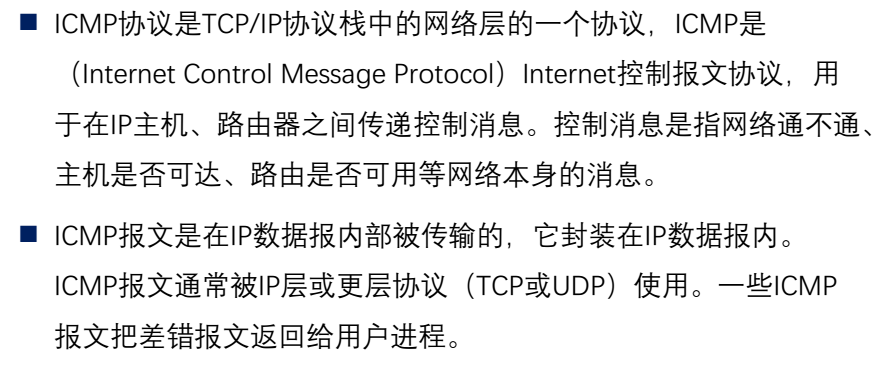
数据包如何不设置跳转次数，那么它就会在这两边挑来挑去的。。。

设置了TTL，如果次数达到的时候，数据包直接扔掉...



如果不设置TTL，那么如果你给一个不存在的地址发数据包的时候，当它的TTL耗尽的时候，数据包就扔掉了，要不然，这个数据包永远都不会消失。

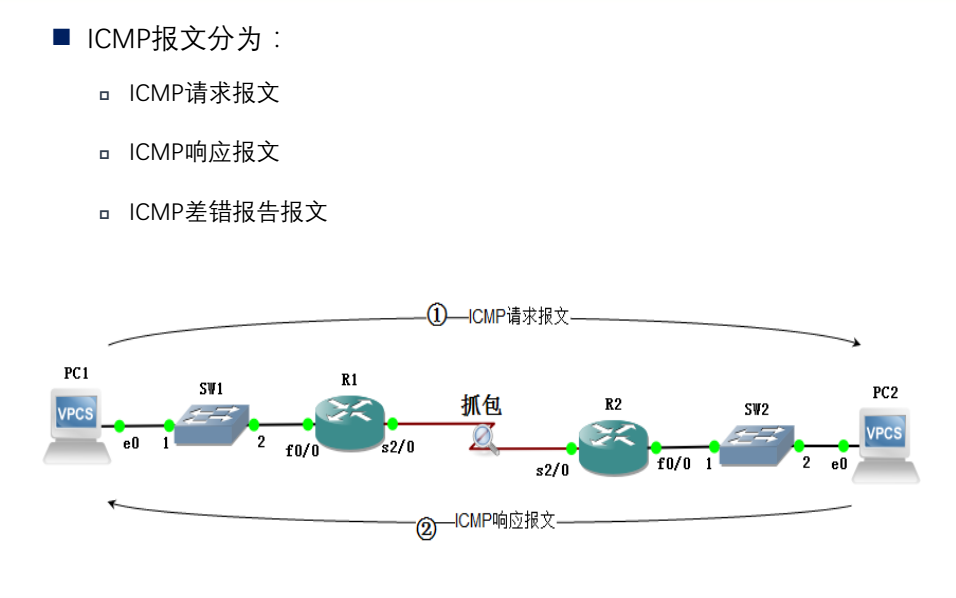
## ICMP协议

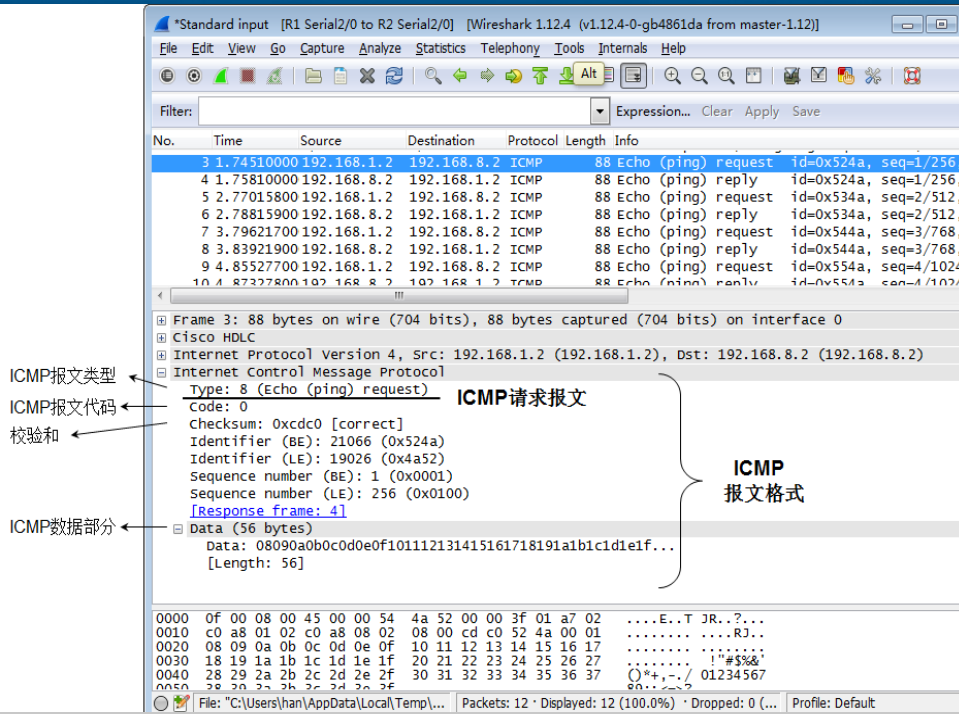


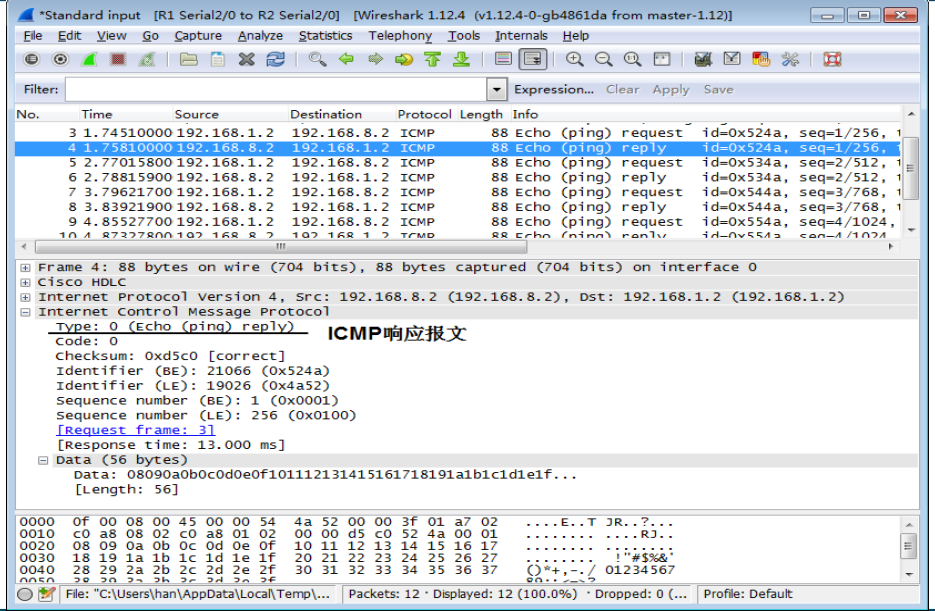
首先，Ping命令会构建一个固定格式的ICMP请求数据包，然后由ICMP协议将这个数据包连同地址“192.168.1.2”一起交给IP层协议（和ICMP一样，实际上是一组后台运行的进程），IP层协议将以地址“192.168.1.2”作为目的地址，本机IP地址作为源地址，加上一些其他的控制信息，构建一个IP数据包，并在一个映射表中查找出IP地址192.168.1.2所对应的物理地址（也叫MAC地址，熟悉网卡配置的朋友不会陌生，这是数据链路层协议构建数据链路层的传输单元——帧所必需的），一并交给数据链路层。后者构建一个数据帧，目的地址是IP层传过来的物理地址，源地址则是本机的物理地址，还要附加上一些控制信息，依据以太网的介质访问规则，将它们传送出去。

其中映射表由ARP实现。ARP(Address Resolution Protocol)是地址解析协议,是一种将IP地址转化成物理地址的协议。ARP具体说来就是将网络层（IP层，也就是相当于OSI的第三层）地址解析为数据连接层（MAC层，也就是相当于OSI的第二层）的MAC地址。  
  
    主机B收到这个数据帧后，先检查它的目的地址，并和本机的物理地址对比，如符合，则接收；否则丢弃。接收后检查该数据帧，将IP数据包从帧中提取出来，交给本机的IP层协议。同样，IP层检查后，将有用的信息提取后交给ICMP协议，后者处理后，马上构建一个ICMP应答包，发送给主机A，其过程和主机A发送ICMP请求包到主机B一模一样。

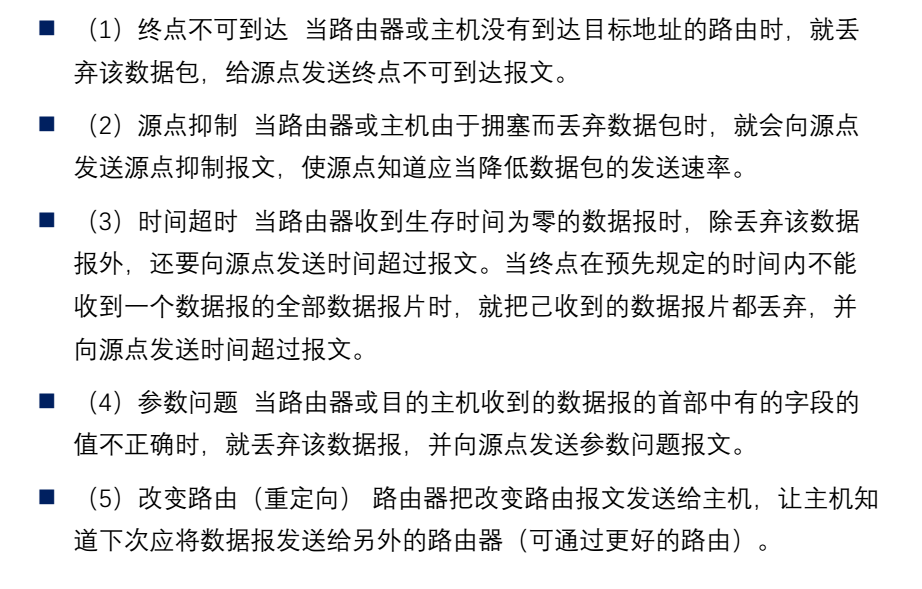
即先由IP地址，在网络层传输，然后再根据mac地址由数据链路层传送到目的主机

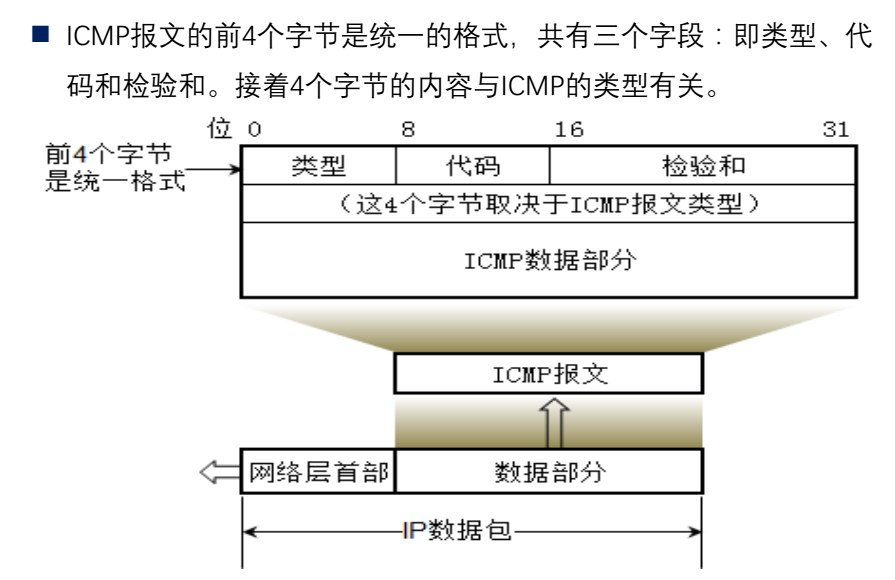




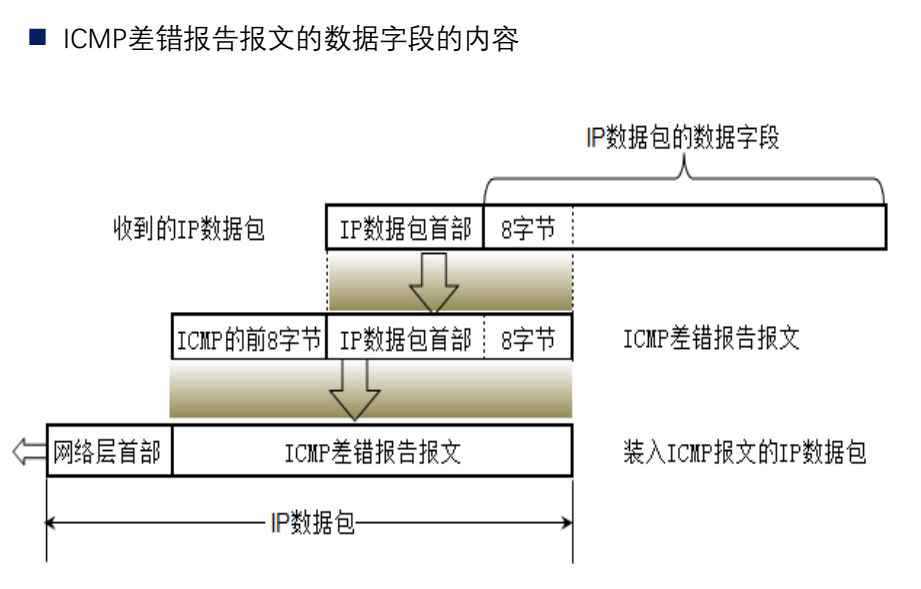




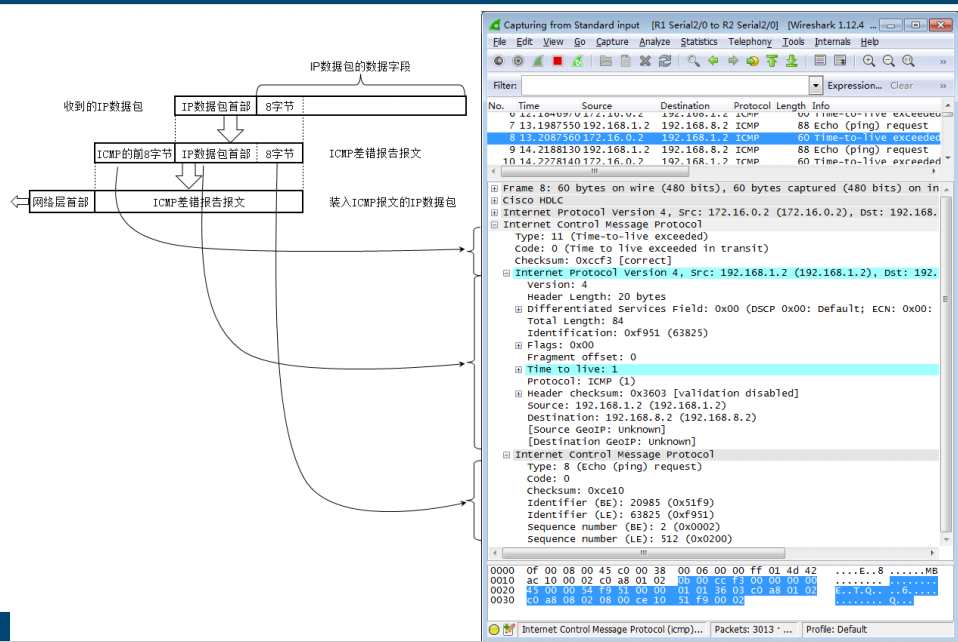




PING命令就是一个ICMP协议的IP包，它的ICMP信息放在IP包的数据部分.主要的有ICMP报文类型、报文代码、校验和以及数据部分.

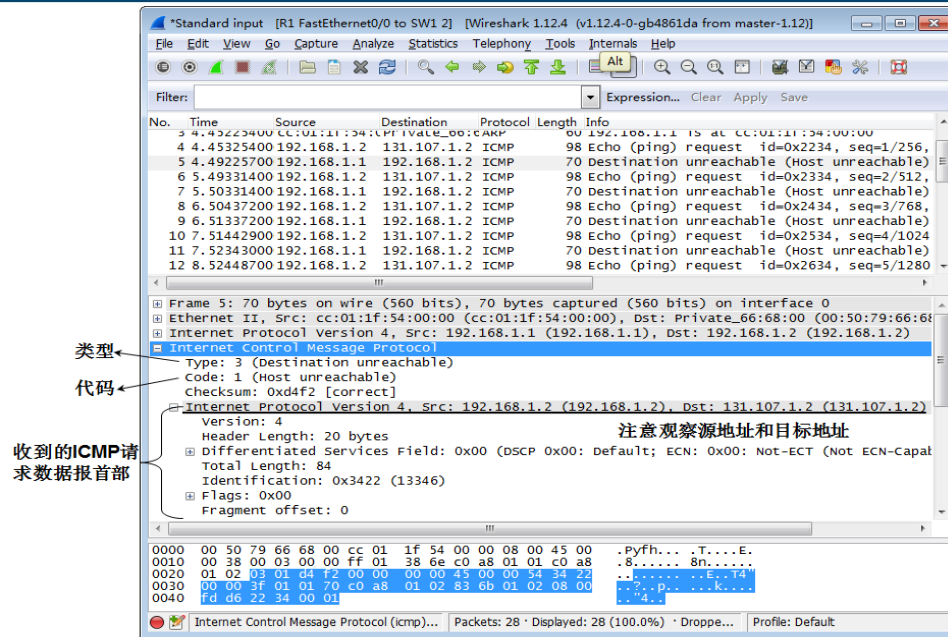


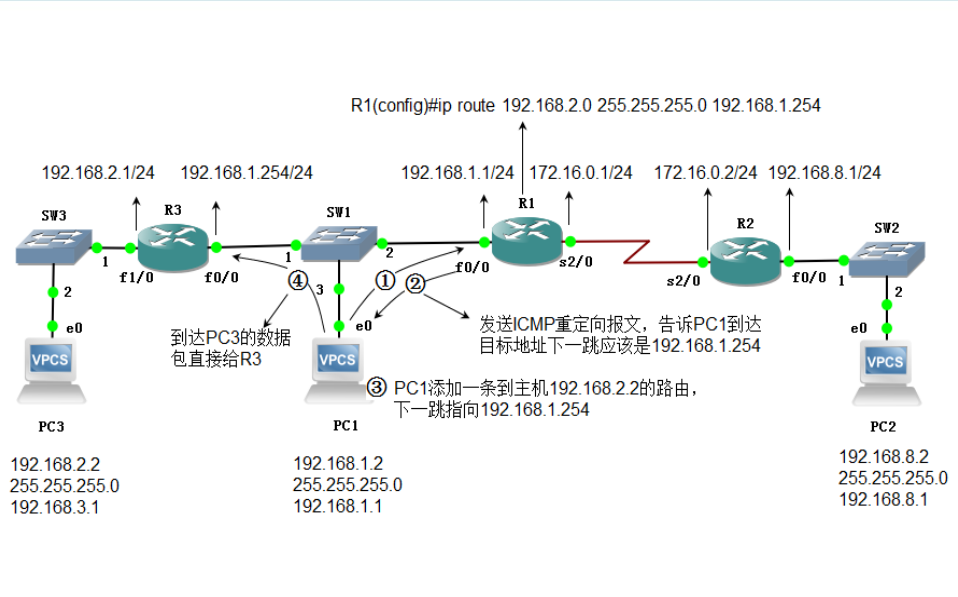
这里一定注意，如果是个差错报告的IP数据包，那么它的数据部分就全部是差错报告报文，并且里面包含了IP数据包的首部(产生错误的那个数据包的首部).



TTL过期的情况

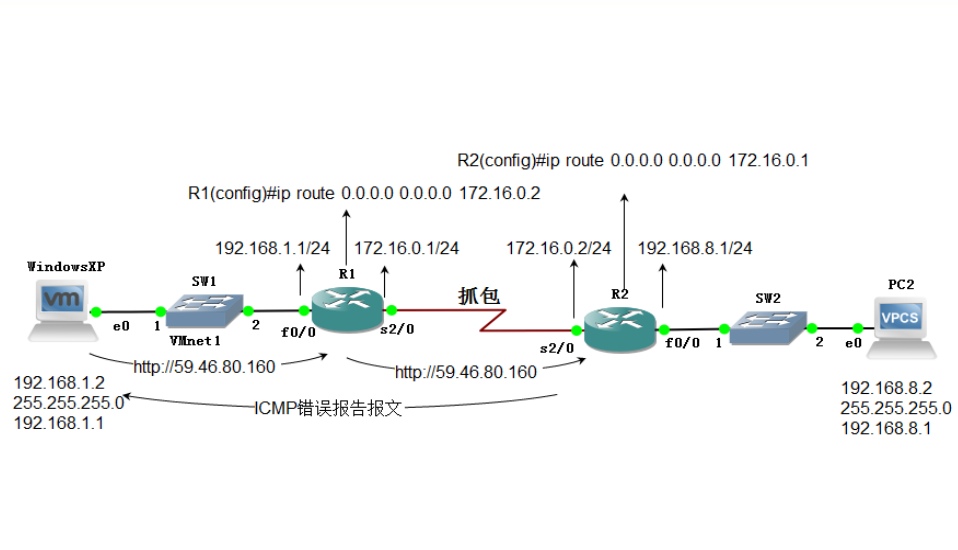
目标不可达的情况

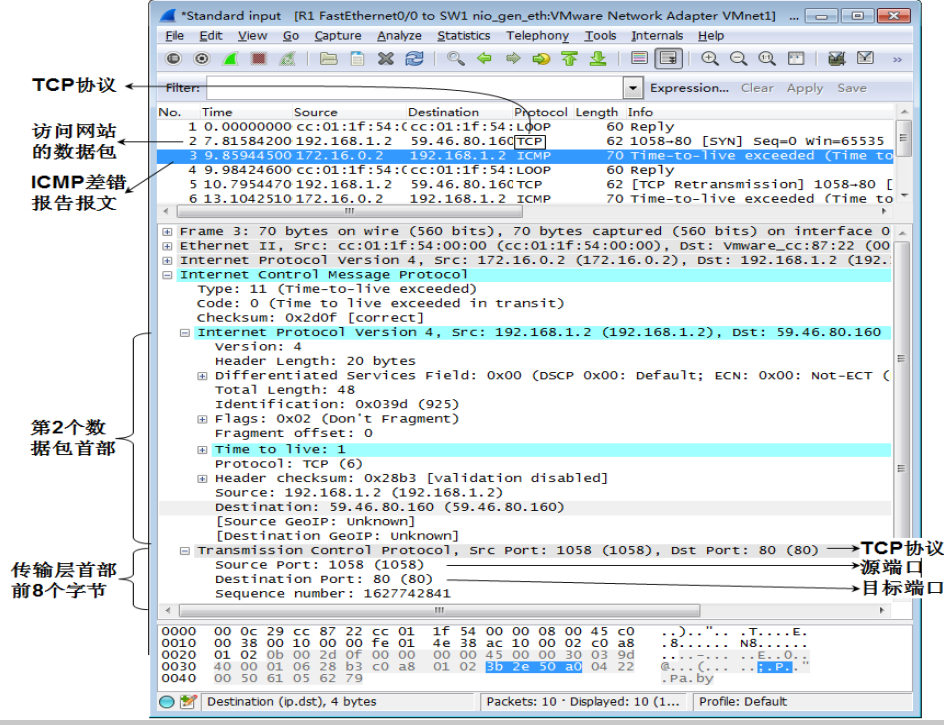






路由重定向的情况

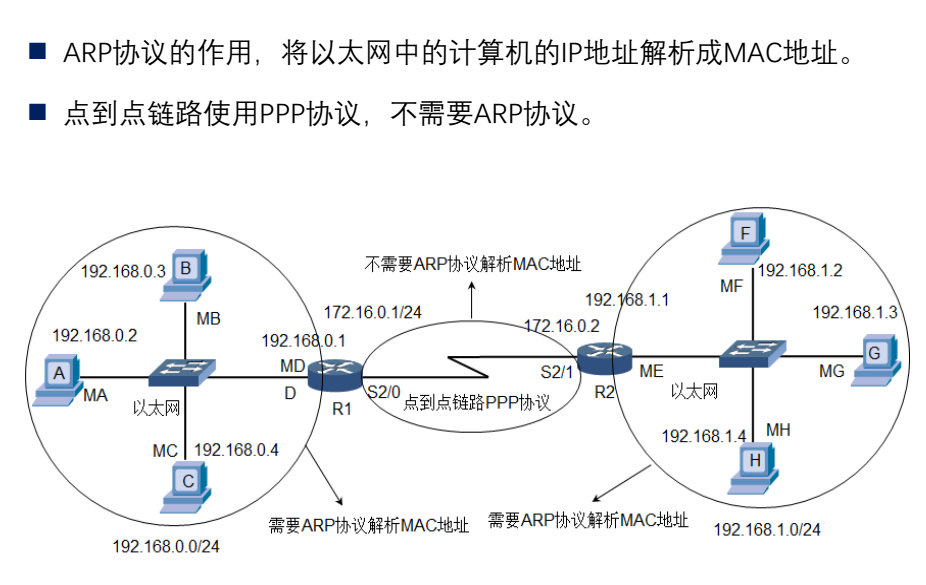


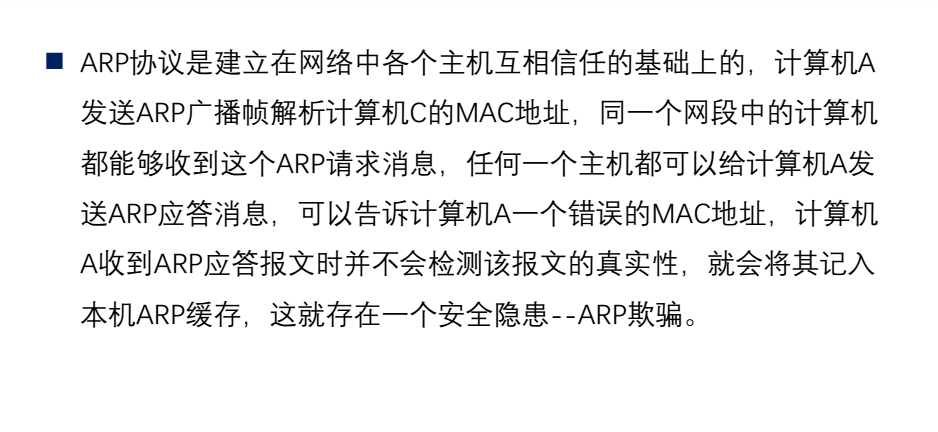


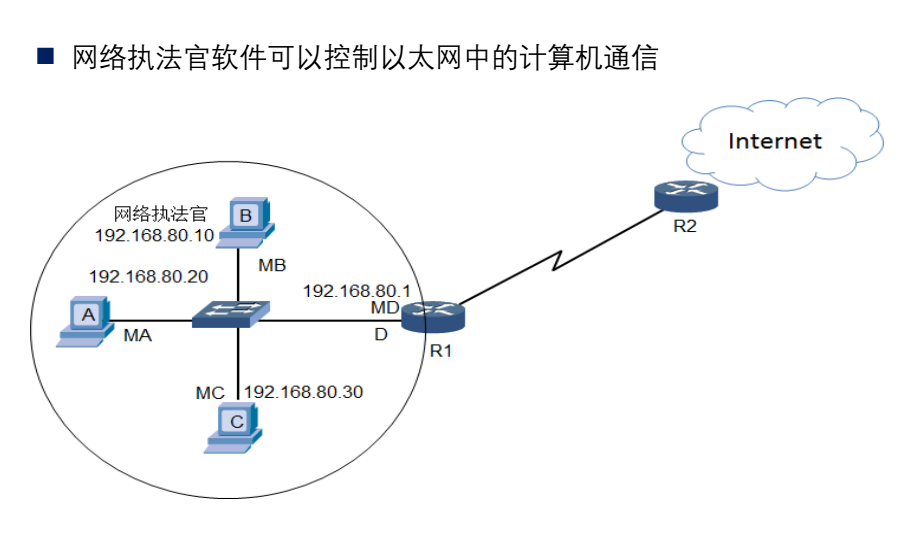
应用程序返回ICMP错误报告的情况

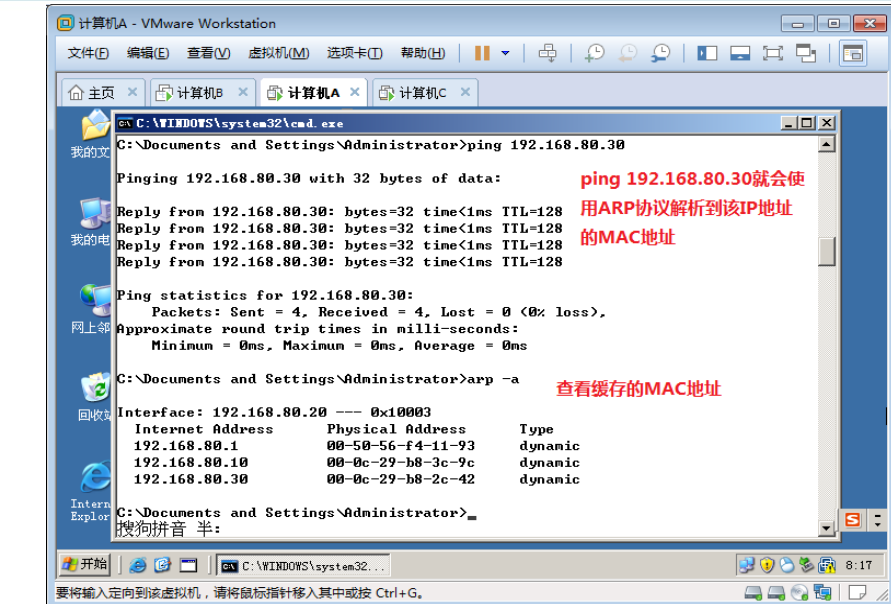
## ARP协议

ARP协议（为IP协议提供帮助，而IP协议又是为了ICMP协议提供帮助）

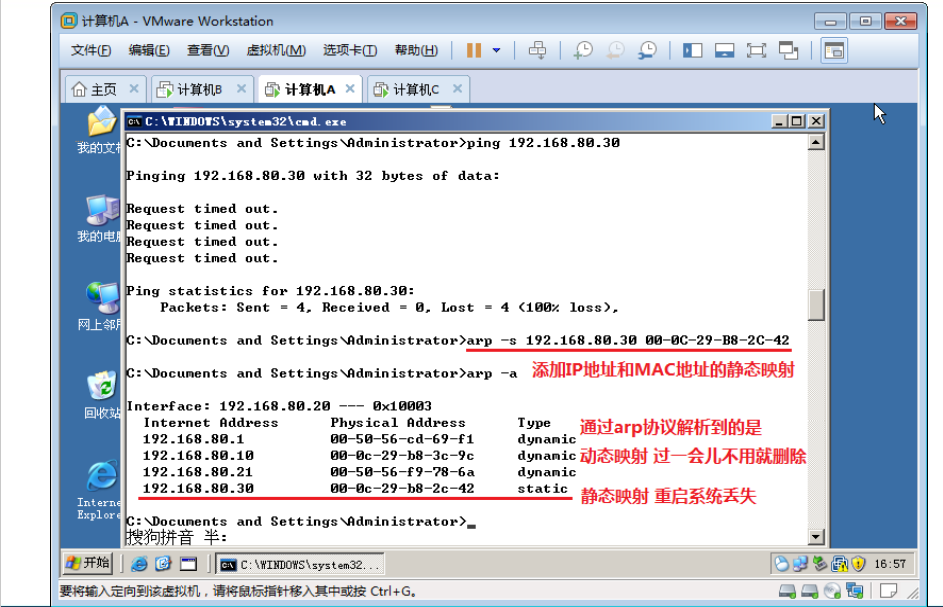








查看解析的MAC地址



判断和防止arp欺骗的方法