**网原HW5**

**计71 张程远 2017011429**

**Chapter 5**

**2、**错误，否则无法给连接建立的分组选择路由。

**3、**比如窗口的大小，超时时间以及数据包大小上限值。

**9、**16\*16不是4800的因子，而15\*16是因子，此时另一项的值为20，即得最小值为51。

**10、**常规方法是家乡代理欺骗路由器以便让路由器确定移动主机响应ARP请求。当路由器得到指向移动主机地址的数据包时，它就广播一次ARP查询，询问拥有这个ip地址的主机的以太网mac地址。当移动主机不在附近时，家乡代理就响应这次ARP查询，所以路由器就可以将移动主机的ip地址与家乡代理的以太网mac地址联系在一起。

**22、**不能，如果加速数据包本身数量过大，那么常规信道的性能可能会更好。

**28、**4096

**34、**安装NAT之后，所有与单个连接有关的数据包需要通过同一个路由器进出公司。如果每个路由器都有自己的IP地址，并且属于给定连接的所有流量都可以发送到同一个路由器，则ping可以生效。

**40、**大概年。

**42、**需要更大的字段。是技术性的，概念上没有变化。

**2.3 IPv4实验**

首先观察几个地址。

PC1的地址：



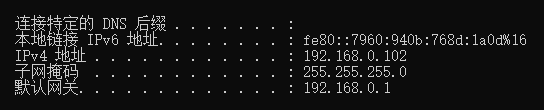
PC2的地址：



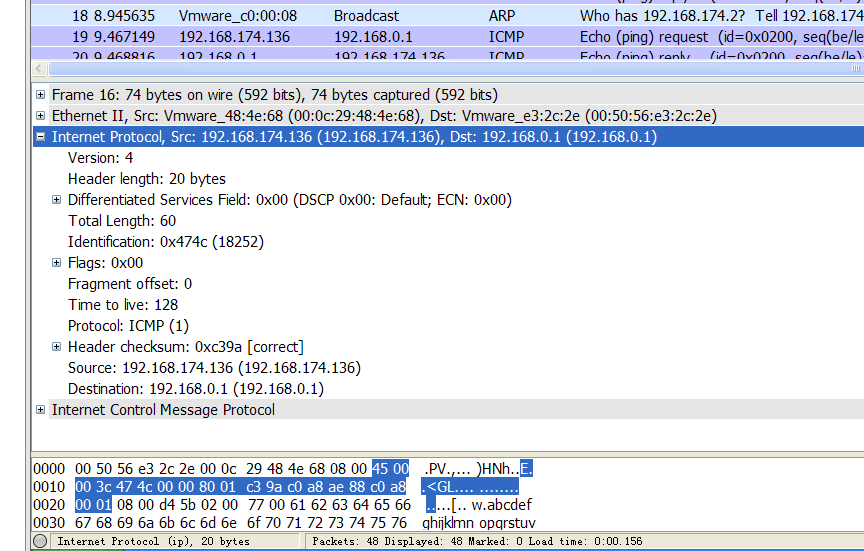
PC3的地址：



R地址：



**2.3.1观察IPv4协议报文**

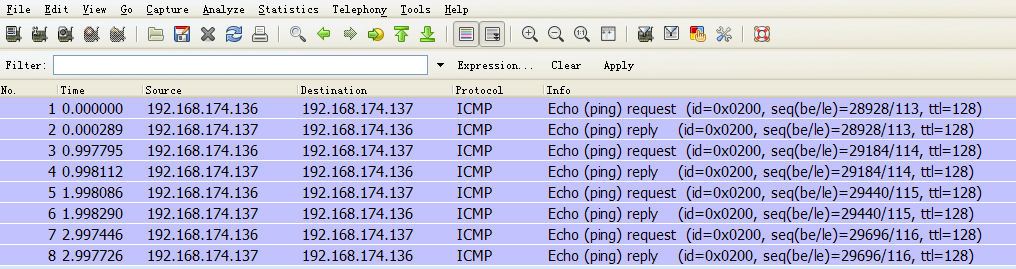


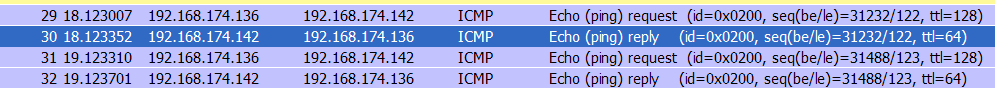
（1）由上图可知，version为4，IHL为5。实际上IHL的值最大可以达到f，但是在这次实验里没有找到这样的数据包。

（2）再观察，可知道Total Length及Header Checksum是正确的，source值为PC1，Destination为默认网关的地址。

（3）是从1开始的

（4）观察下面两张图可知道

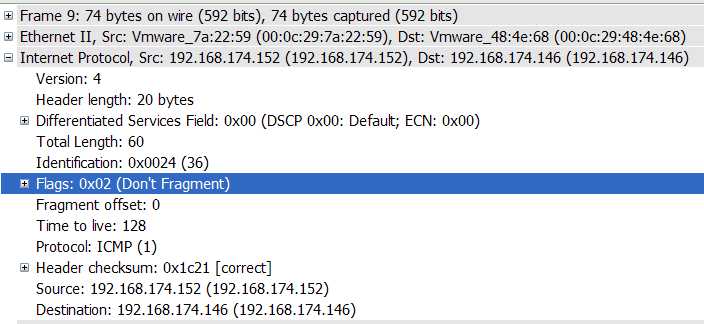




Windows的TTL是128，Linux的TTL是64。

（5）不同分组的identification也不同。

（6）是

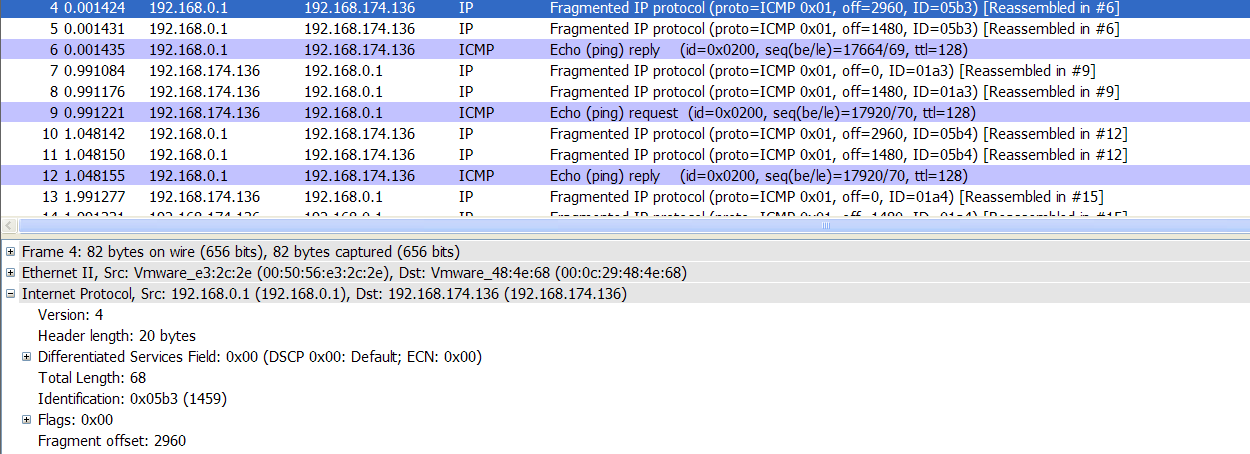


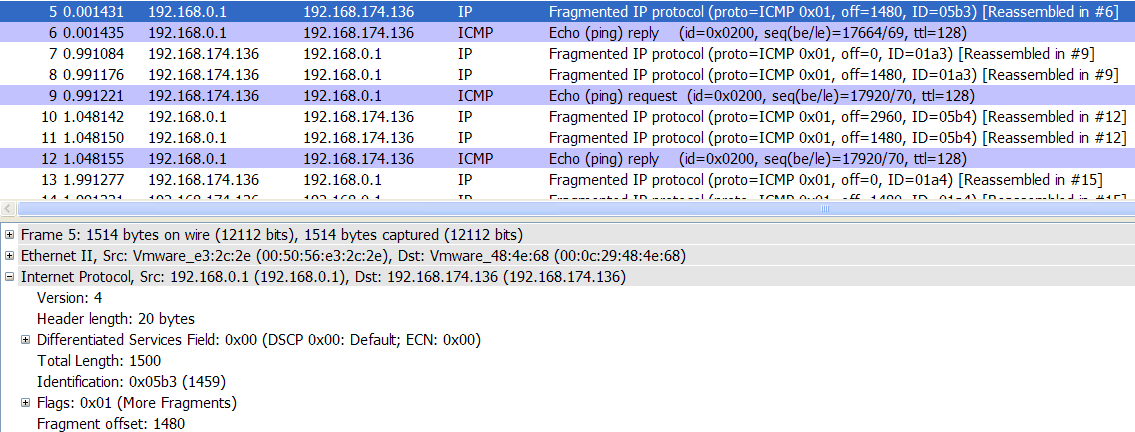
（7）TCP是0x06，UDP是0x11，ICMP是0x01。

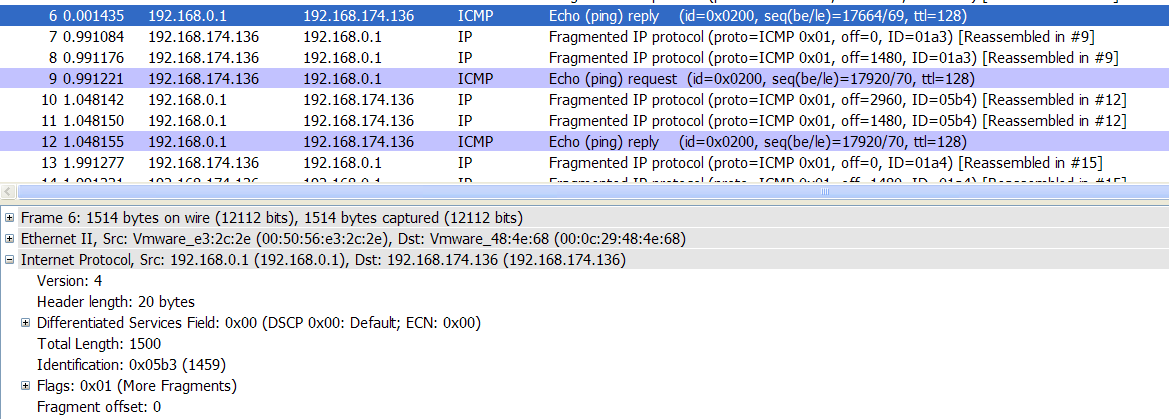
**2.3.2 观察IPv4分段与重组**

（1）IPv4分段

（2）Identification一样的为同一个分组，比如下面这三张图所展示的数据包。







（3）后两张图中的More Fragments为1，证明还可以有分段。第一张图的More Fragment值为0，因此不能有更多分段。

（4）当Flags值为0时表示分段结束。

（5）这里数据包是乱序的，按照offset排序应该为0/1480/2960，这也解释了为什么第一个包的More Fragments是0，因为它实际上是最后一个包。

（6）ICMP头是8字节的

（7）第一个分段的最后一个字符是w，第二个分段第一个字符是a，最后一个字符是h，第三个分段第一个字符是i。

**2.3.3 IP选项的使用**

（1）IPv4选项中code的值为0x07，表示记录路径

（2）len是8条

（3）指针的值指向第9条

**思考题**

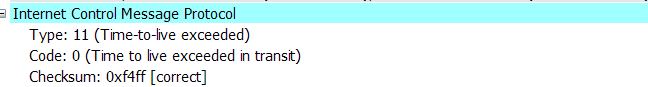
（1）如果网络中的单个数据包过大，数据包就要拆分成小包然后再传输。它在发送端处分段，在接收端处被重新组合成大包。

（2）无操作选项、选项结束项、记录路由选项、严格的源路由选项、不严格的源路由选项，时间戳选项。

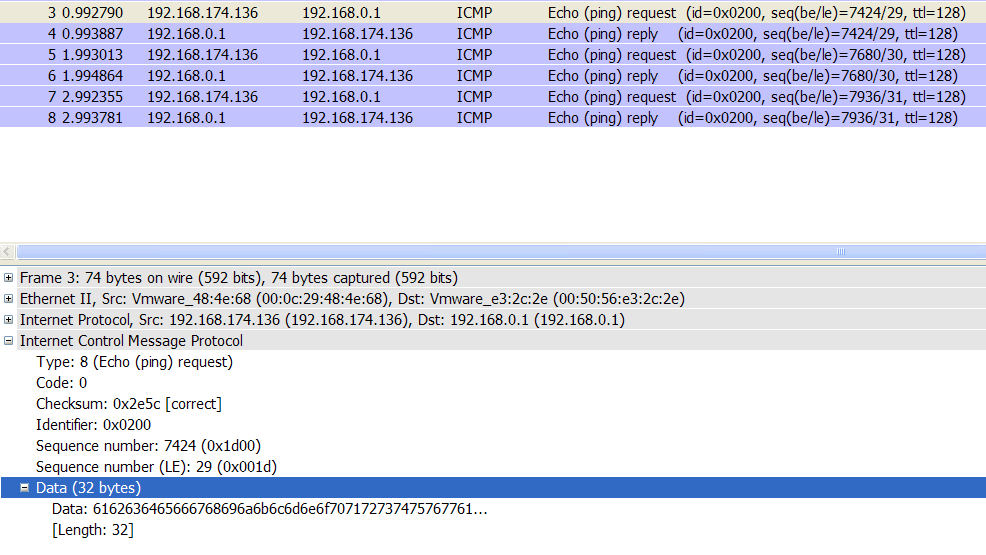
**2.4 ICMPv4协议实验**

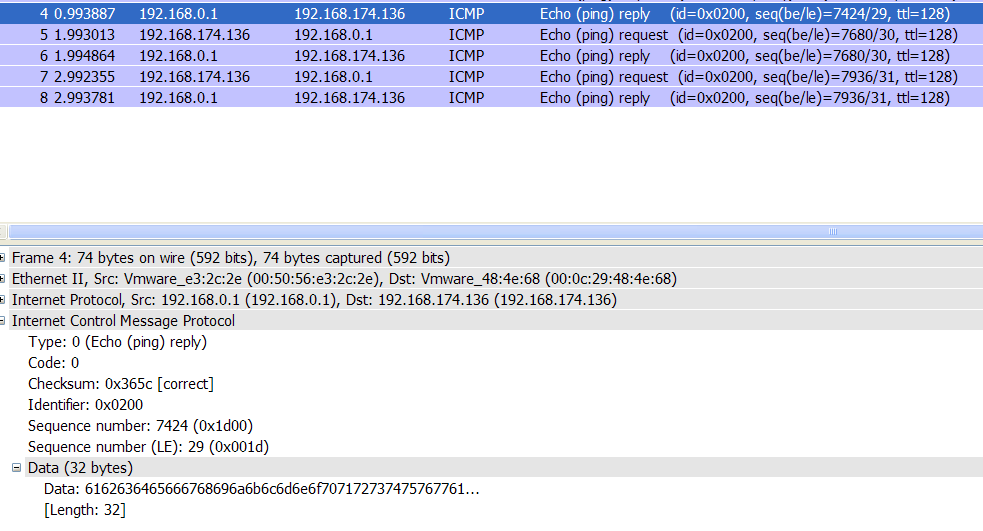
（1）观察可知 Code 10表示目的主机被禁止。

（2）获得的TTL超时信息如下图所示。



（3）观察request和reply的报文，它们符合标准。





**思考题**

1 为了标识ICMP4的错误消息（如不可达消息）和正确的消息。

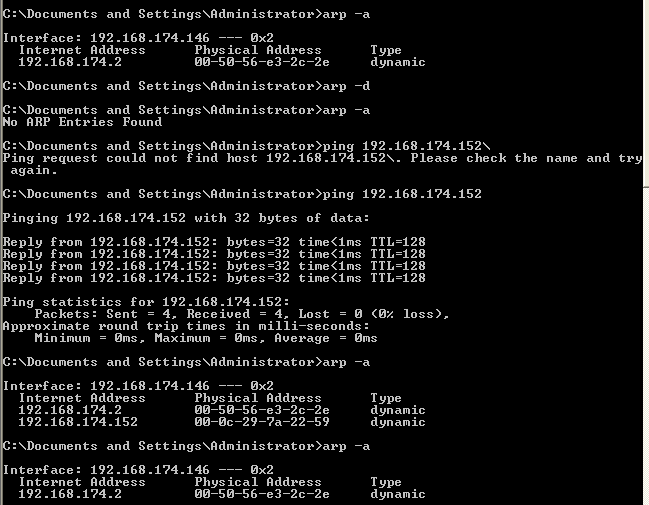
2 上网查阅到下面的资料

ICMP协议被攻击的方法有很多种，比如的“Ping of Death”、使用ICMP数据包发起DDOS攻击、redirect攻击等等。当发送的数据包大小超过64KB（规定最大64KB）后接收信息的主机就会出现内存分配错误，进一步会导致TCP/IP堆栈崩溃，甚至主机死机；DDOS简单来说就是一直不停地发送ICMP数据包从而占满被攻击主机的带宽，当然，更进一步还可以使用一些手段将流量进行放大，比如将源地址设置为被 攻击主机的“echo-request”类型报文广播给很多第三方主机，这时这些接收到报文的主机就会给被攻击目标主机返回“echo-replay”报文，这样流量就被放大了；当路由设备发现某个数据包经过自己不是最优路径时 就会给源地址发一个redirect数据包，告诉对方发的路径不合适，并且指出应该发往的地址。这个功能是很有用的，不过如果被攻击者使用情况就完全不一 样了，他们可以使用这一功能将正常（合理）的路由地址给修改为一个不合理的甚至不存在的地址，这样就会给通讯造成问题，另外，有一些还会将目标地址设置为 他们自己可以控制的主机的地址，这样就可以截获数据了！跟redirect相关的还有router-advertisement、router- solicitation等类型的ICMP数据包。

**2.5 ARP协议实验**

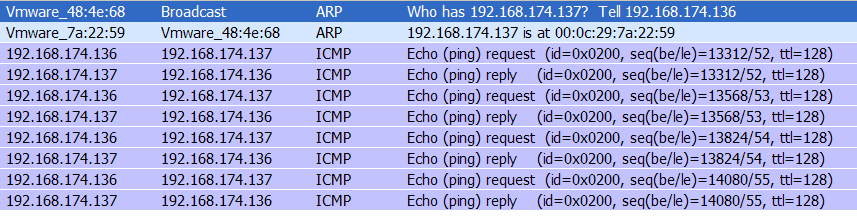
**2.5.1**

ARP缓存的生存时间大概是1-2分钟，如果再次使用则会刷新。



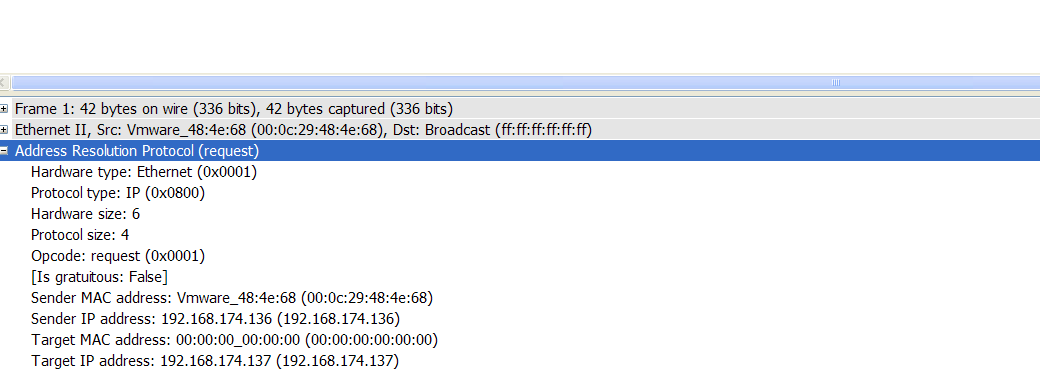
**2.5.2**

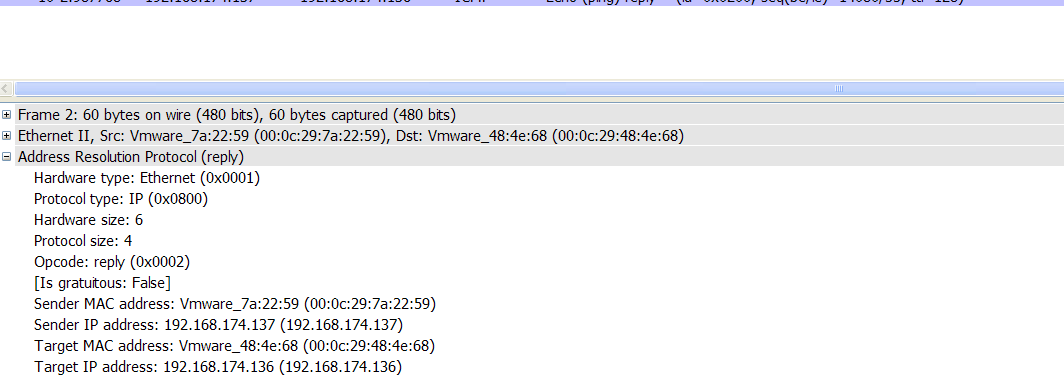
ARP过程图如下所示。



PC1首先检查自己的ARP缓存，如果miss就发送ARP请求，然后PC2应答并告诉PC1自己的MAC地址。（当然如果ARP缓存中有就直接使用）

**2.5.3** ARP分组格式





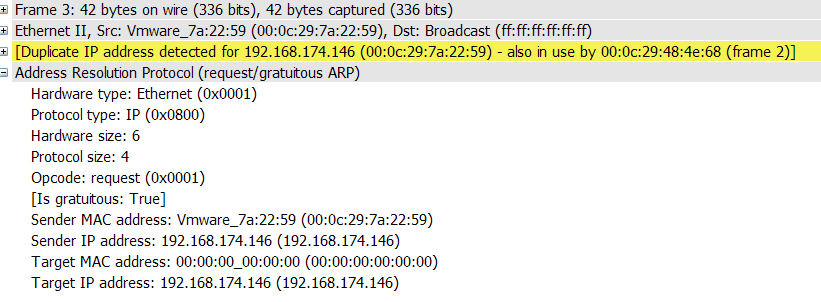
ARP request的目的地址为广播地址，源地址为本机MAC地址；ARP reply的目的地址为请求方MAC地址，源地址为本机的MAC地址，尾部填充了16字节的0。

网口为以太网0x0001，协议为0x0800即IP协议，IP的源地址和目的地址分别为本机地址和目的地址；Request的Opcode为0x0001，Reply的Opcode为0x0002。

**2.5.4观察无偿ARP**

由观察得知，初始化IP地址发送的无偿ARP有3个。首先一台机器会发送一个无偿ARP Request来请求初始化自己的IP地址，另一台机器返回一个Reply并发送一个广播无偿ARP请求，让网络上其他设备获得正确的ARP表。如果ARP应答分组的源和目的一样但MAC不一样，那么源节点收到无偿ARP请求分组后就会产生冲突。

下图是一个无偿ARP。



**思考题**

1、一台主机向另一台主机发送ARP请求报文之后，网关收到报文并代替目的主机向发送者发送响应，之后网关再向目的主机网段发送ARP请求报文，目的主机收到以后再发送ARP响应。

2、arp expire-time命令可以修改动态ARP缓存生存时间

3、arp detect-times 命令可以修改无偿ARP发送的数目。