

lab2.2 利用Wireshark观察链路层报文

lab2.2 利用Wireshark观察链路层报文

&实验步骤

&ARP协议简介

&抓包结果分析

- 1.指定显示过滤器, 只显示"请求指定IP的MAC地址"的arp数据包
- 2.指定显示过滤器, 只显示指定主机(本机)发送的"请求指定IP的MAC地址" 的arp数据包.
- 3.删除本地缓存的某个主机的arp条目, 然后ping该主机, 定义过滤器, 只显示重建该arp条目的数据包.

&实验步骤

(1) 用ipconfig命令获得

本机的mac地址:9C:B6:D0:E1:41:91

本机的ip地址:114.214.240.159

默认网关的IP地址:114.214.240.0

(2) 启动wireshark, ping 114.214.240.0得到抓包结果arp(实验步骤1,2)

(3) 清除arp缓存

(4) 启动wireshark, ping 114.214.240.1得到抓包结果arp(实验步骤3)

备注: arp抓包实验一共两个数据包, 分别对应(实验步骤1,2)和(实验步骤3)

&ARP协议简介

ARP协议的作用是把IP地址解析为MAC地址, 且而 ARP 只为在同一个子 网上的主机和路由器接口解析IP地址

每台主机或路由器在其内存中具有一个 ARP 表 (ARP table), 这张表包含 IP 地址到 MAC 地址的映射关系

一个ARP 分组封装在链路层帧中, 因而在体系结构上位于链路层之上。然而, 一个 ARP 分组具有包含链路层地址的字段, 因而可认为是链路层协议, 但它也包含网络层地址, 因而也可认为是为网络层协议

IP 地址	MAC 地址	TTL
222. 222. 222. 221	88-B2-2F-54-1A-0F	13:45:00
222. 222. 222. 223	5C-66-AB-90-75-B1	13:52:00

&抓包结果分析

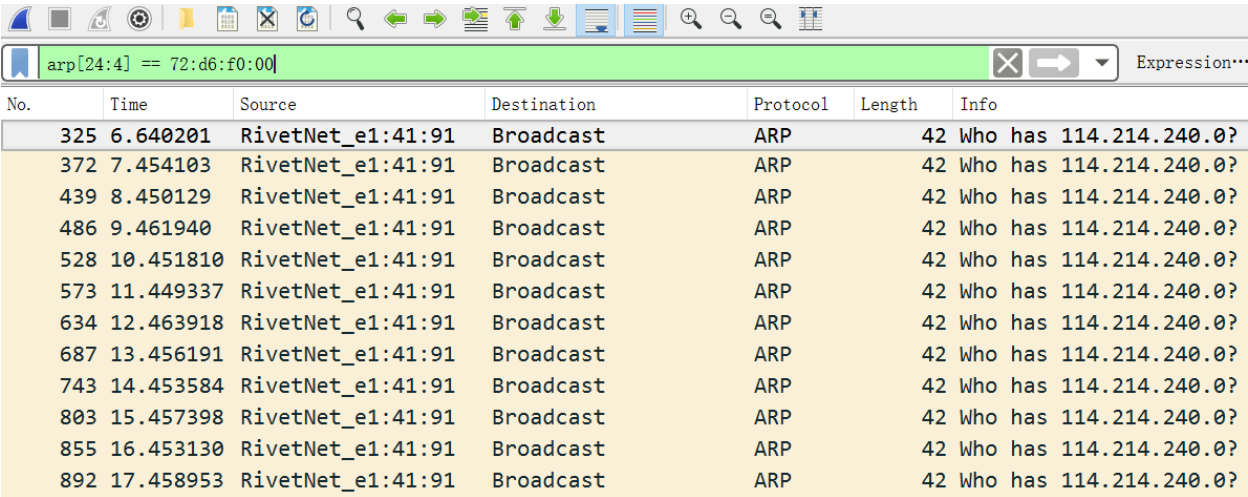
1.指定显示过滤器, 只显示“请求指定IP的MAC地址”的arp数据包

- “请求ip为114.214.240.0的MAC地址”的arp数据包

114.214.240.0的十六进制表示为72:d6:f0:00,

采用报文内容过滤,

显示过滤器: arp[24:4] == 72:d6:f0:00



No.	Time	Source	Destination	Protocol	Length	Info
325	6.640201	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
372	7.454103	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
439	8.450129	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
486	9.461940	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
528	10.451810	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
573	11.449337	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
634	12.463918	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
687	13.456191	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
743	14.453584	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
803	15.457398	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
855	16.453130	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?
892	17.458953	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.240.0?

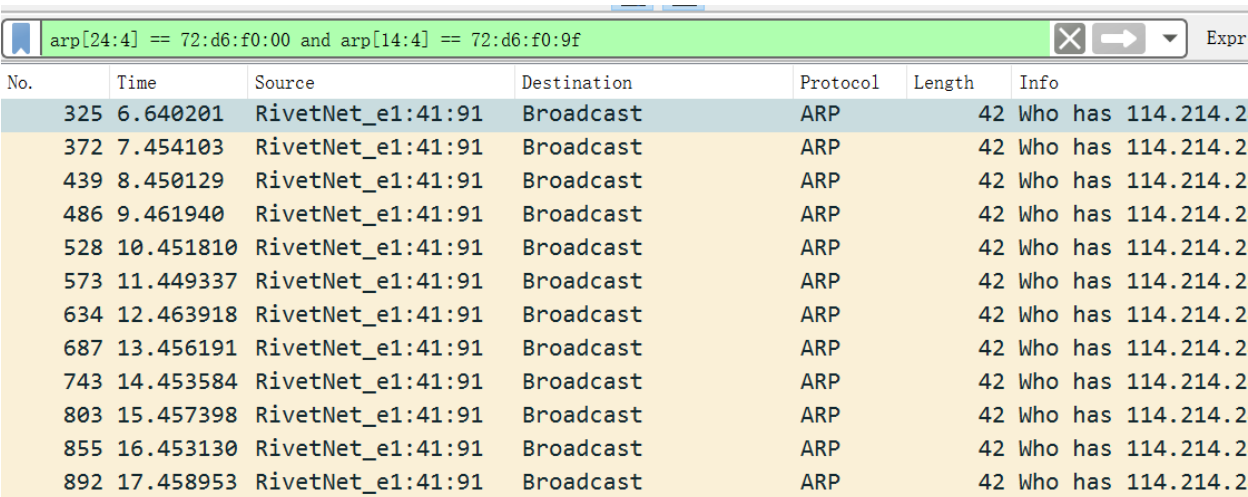
2.指定显示过滤器, 只显示指定主机(本机)发送的“请求指定IP的MAC地址” 的arp数据包.

- 本机发送的“请求ip为114.214.240.0的MAC地址”的arp数据包

本机ip地址为114.214.240.159, 十六进制表示为72:d6:f0:9f

采用报文内容过滤

显示过滤器: arp[24:4] == 72:d6:f0:00 and arp[14:4] == 72:d6:f0:9f



No.	Time	Source	Destination	Protocol	Length	Info
325	6.640201	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
372	7.454103	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
439	8.450129	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
486	9.461940	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
528	10.451810	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
573	11.449337	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
634	12.463918	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
687	13.456191	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
743	14.453584	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
803	15.457398	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
855	16.453130	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2
892	17.458953	RivetNet_e1:41:91	Broadcast	ARP	42	Who has 114.214.2

3.删除本地缓存的某个主机的arp条目, 然后ping该主机, 定义过滤器, 只显示重建该arp条目的数据包.

- 清除arp缓存

命令行输入arp -d 清除arp缓存

命令行输入arp -a 查看arp缓存

```
C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>arp -a

接口: 114.214.240.159 --- 0x6
    Internet 地址      物理地址      类型
    224.0.0.22        01-00-5e-00-00-16 静态

接口: 169.254.143.109 --- 0x9
    Internet 地址      物理地址      类型
    224.0.0.22        01-00-5e-00-00-16 静态

接口: 169.254.222.28 --- 0xa
    Internet 地址      物理地址      类型
    224.0.0.22        01-00-5e-00-00-16 静态
```

- ping 114.214.240.1 重建arp缓存

```
C:\WINDOWS\system32>ping 114.214.240.1

正在 Ping 114.214.240.1 具有 32 字节的数据:
来自 114.214.240.1 的回复: 字节=32 时间=12ms TTL=255
来自 114.214.240.1 的回复: 字节=32 时间=5ms TTL=255
来自 114.214.240.1 的回复: 字节=32 时间=18ms TTL=255
来自 114.214.240.1 的回复: 字节=32 时间=8ms TTL=255

114.214.240.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 5ms, 最长 = 18ms, 平均 = 10ms
```

- 重建后的arp条目

```
C:\WINDOWS\system32>arp -a
```

接口: 114.214.240.159 --- 0x6		
Internet 地址	物理地址	类型
114.214.240.1	5c-dd-70-91-72-e2	动态
224.0.0.22	01-00-5e-00-00-16	静态
接口: 169.254.143.109 --- 0x9		
Internet 地址	物理地址	类型
224.0.0.22	01-00-5e-00-00-16	静态
接口: 169.254.222.28 --- 0xa		
Internet 地址	物理地址	类型
224.0.0.22	01-00-5e-00-00-16	静态

- 重建该arp条目的数据包

重建该arp条目的数据报即为114.214.240.0收到广播arp数据报后，回复本机的数据包。

该数据报包的发送方为114.214.240.0【十六进制表示为72:d6:f0:90】，

接收方为本机ip地址114.214.240.159【十六进制表示为72:d6:f0:9f】。

据此设定显示过滤器:arp[24:4] == 72:d6:f0:9f and arp[14:4] == 72:d6:f0:01

No.	Time	Source	Destination	Protocol	Length	Info
21...	40.891376	Hangzhou_91:72:e2	RivetNet_e1:41:91	ARP	56	114.214.240.1 is at 5c:dd:70:91:72:e2

