



计算机网络实验四

地址解析协议 (ARP)

信息学部 朱婉婷

主要内容

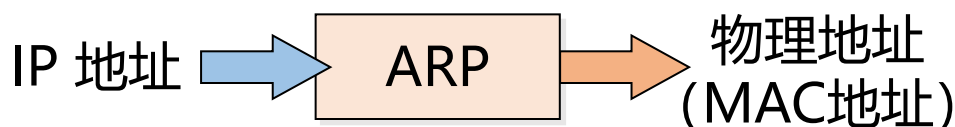
- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

ARP简介

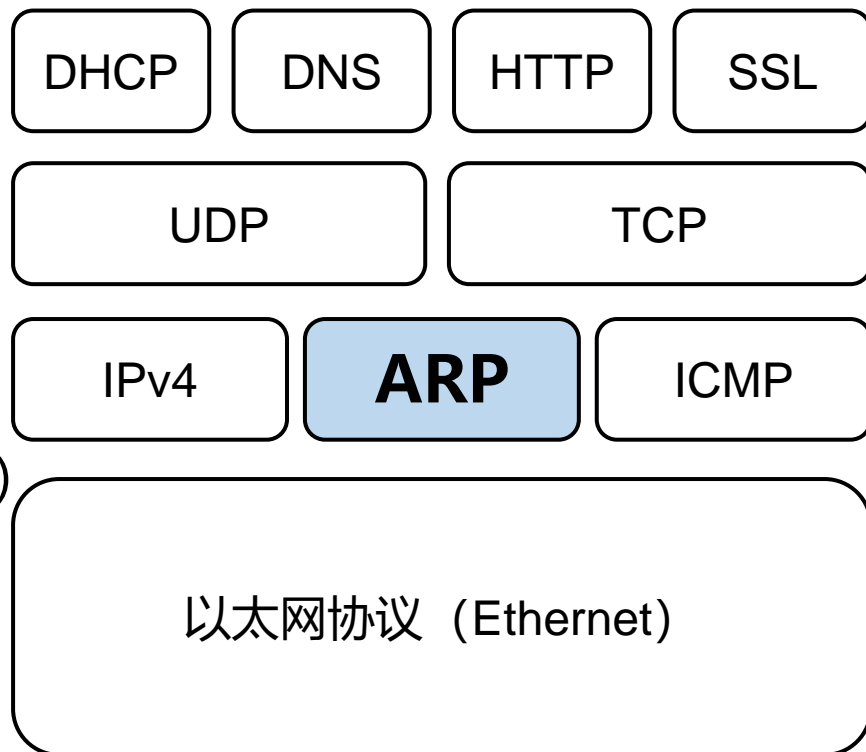
◆地址解析协议 ARP

(Address Resolution Protocol)

- 是根据IP地址获取物理地址的一个网络层协议。



◆逆地址解析协议 RARP



ARP工作过程

◆ARP 高速缓存

- 每个主机都有一个 **ARP 高速缓存**(ARP cache), 里面存储所在的局域网上各节点 (主机、路由器) 的 IP 地址到MAC地址的**映射表**。
- IP/MAC地址映射关系: **< IP地址; MAC地址; TTL >**
- TTL (Time To Live): 经过这个时间以后该映射关系会被遗弃(典型值为20min) 。

ARP工作过程

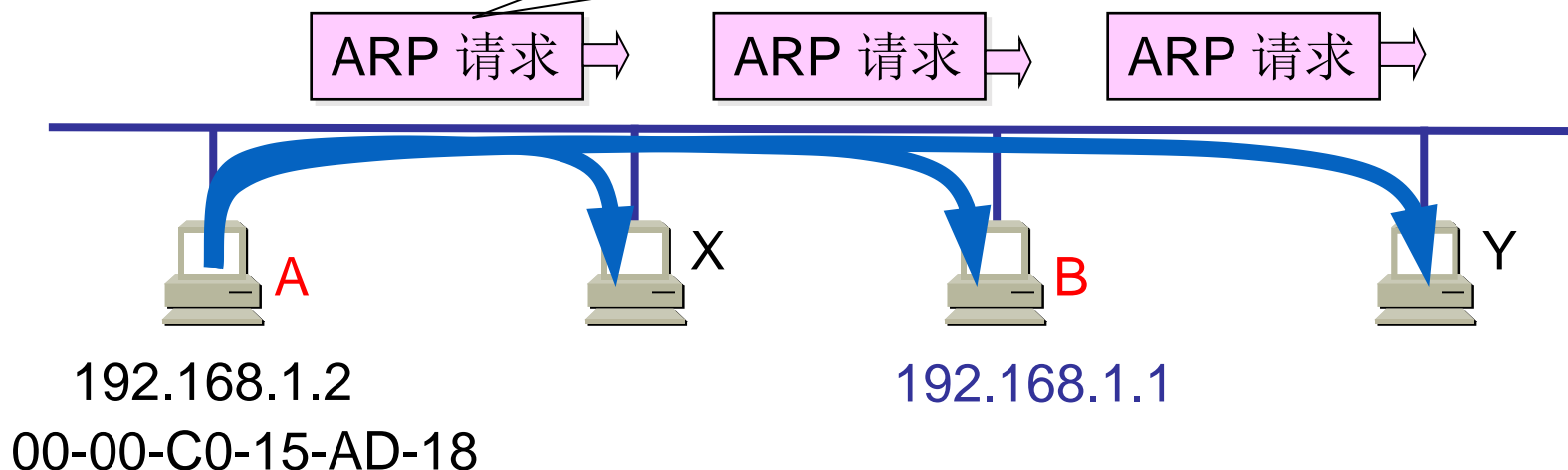
◆ARP 高速缓存

- 为了减少网络上的通信量，主机 A 在发送其 ARP 请求分组时，就将自己的 IP 地址到硬件地址的映射写入 ARP 请求分组。
- 当主机 B 收到 A 的 ARP 请求分组时，就将主机 A 的这一地址映射写入主机 B 自己的 ARP 高速缓存中。主机 B 以后向 A 发送数据包时就更方便了。
- 当主机 A 欲向本局域网上的某个主机 B 发送数据包时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。
- 如有，就可查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址。

ARP 工作过程

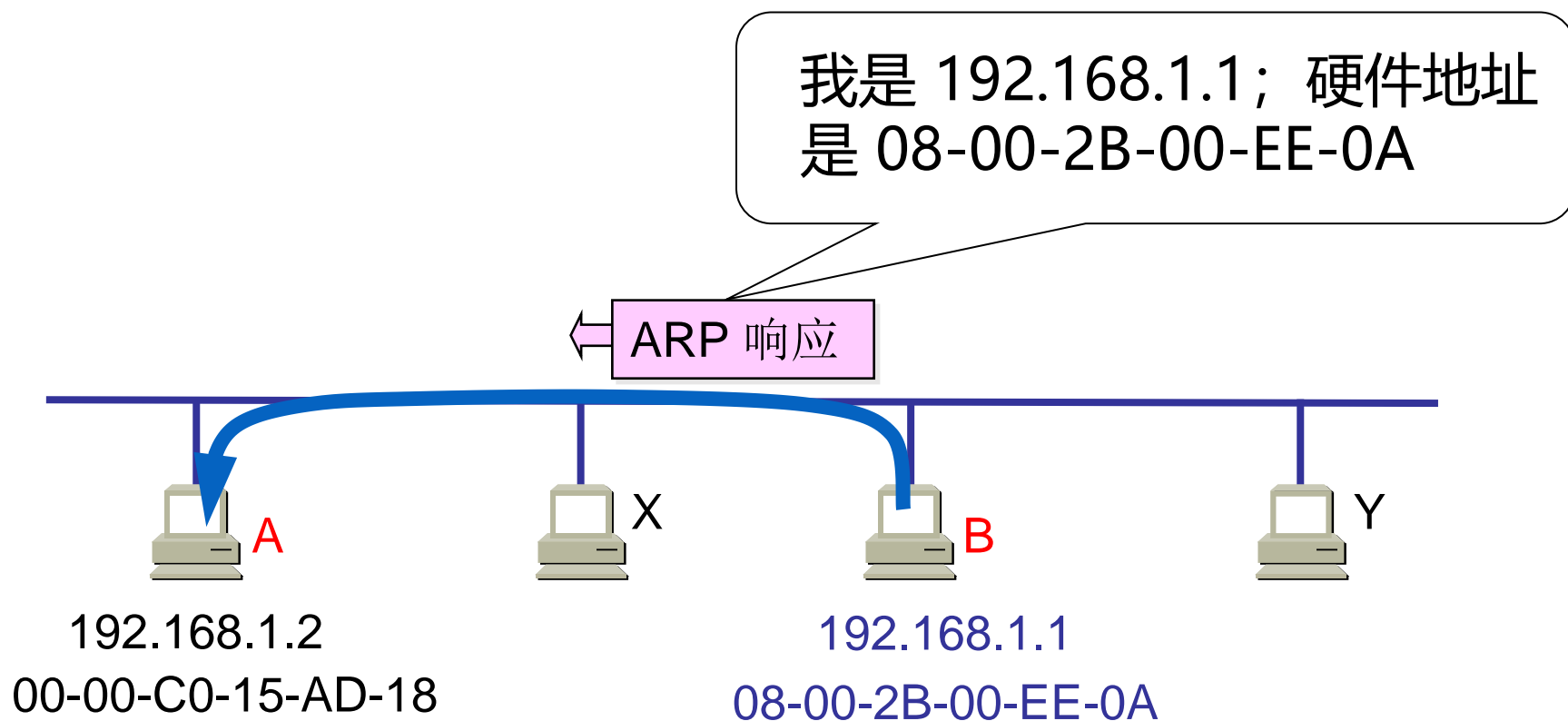
◆ 主机 A 广播发送 ARP 请求分组

我是 192.168.1.2, 硬件地址是 00-00-C0-15-AD-18; 谁有主机 192.168.1.1 的硬件地址?



ARP工作过程

◆主机 B 向 A 发送ARP 响应分组



◆注意：APR请求是**广播**的，但是ARP响应是**单播**的。

ARP分组的格式

2字节 2字节 1字节 1字节 2字节 6字节 4字节 6字节 4字节

硬件 类型	协议 类型	硬件 地址 长度	协议 地址 长度	操作 类型	源 MAC 地址	源IP地 址	目的 MAC 地址	目的IP 地址
----------	----------	----------------	----------------	----------	----------------	-----------	-----------------	------------

- **硬件类型**：表示硬件地址的类型。其值为1即表示以太网地址。
- **协议类型**：表示要映射的协议地址类型。其值为0x0800即表示IPv4协议。
- **硬件地址长度**：表示与硬件类型对应的硬件地址的长度，以字节为单位。如果是以太网，则是6字节（MAC地址长度）。
- **协议地址长度**：表示与协议类型对应的协议地址长度，以字节为单位。如果是IPv4协议，则是4字节（IP地址长度）。

ARP分组的格式

2字节 2字节 1字节 1字节 2字节 6字节 4字节 6字节 4字节

硬件 类型	协议 类型	硬件 地址 长度	协议 地址 长度	操作 类型	源 MAC 地址	源IP地 址	目的 MAC 地址	目的IP 地址
----------	----------	----------------	----------------	----------	----------------	-----------	-----------------	------------

- **操作类型**：四种操作类型。**ARP请求1**，**ARP应答2**，RARP请求3，RARP应答4。
- **发送端硬件地址**：如果是以太网，则是源主机以太网地址。
- **发送端协议地址**：如果是IP协议，则表示源主机的IP地址。
- **目的端硬件地址**：如果是以太网，则是目的主机以太网地址。
- **目的端协议地址**：如果是IP协议，则表示目的主机的IP地址。

特别说明

- ARP 是解决**同一个局域网**上的主机或路由器的 IP 地址和硬件地址的映射问题。
- 如果所要找的主机和源主机不在同一个局域网上，那么就要通过 ARP 找到一个位于本局域网上的某个**路由器**的硬件地址，然后把分组发送给这个路由器，让这个路由器把分组转发给下一个网络。剩下的工作就由这个路由器来做。
- ARP是建立在网络中各个主机**互相信任**的基础上的，网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时**不会检测**该报文的真实性就会将其记入本机ARP缓存。

主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

实验环境搭建

列出本次实验所使用的平台和相关软件，以下为例：

(打开cmd指令窗口，输入指令 “ipconfig /all”查看)

- 1、主机：联想笔记本（Win10系统）；主机IP地址：192.168.1.106；子网掩码：255.255.255.0；主机网卡MAC地址：34-F6-4B-C0-90-40。
- 2、网络连接方式：无线连接；默认网关地址：192.168.1.1。
- 3、抓包工具：Wireshark（v3.6.2）。

实验具体步骤

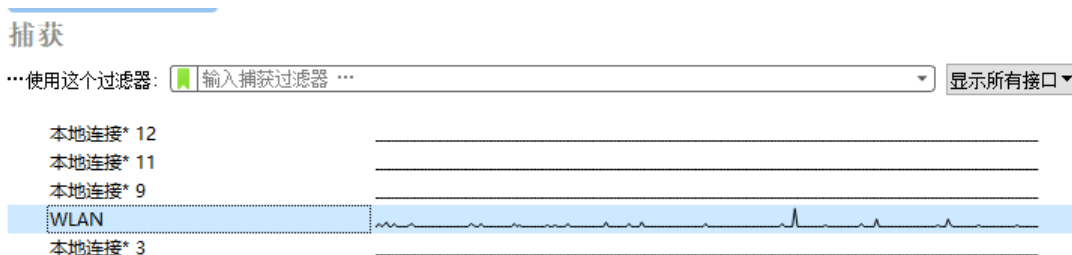
1、在Windows命令模式下利用`arp -a`命令，查看本机的ARP缓存表。观察到默认网关192.168.1.1的MAC地址为F4-2A-7D-57-29-AD。

```
C:\Users\zwt717>arp -a
```

接口: 192.168.1.106 --- 0x14	Internet 地址	物理地址	类型
	192.168.1.1	f4-2a-7d-57-29-ad	动态
	192.168.1.103	58-41-20-ba-a5-ae	动态
	192.168.1.104	b0-41-1d-e2-de-6b	动态
	192.168.1.255	ff-ff-ff-ff-ff-ff	静态
	224.0.0.2	01-00-5e-00-00-02	静态
	224.0.0.22	01-00-5e-00-00-16	静态
	224.0.0.251	01-00-5e-00-00-fb	静态
	224.0.0.252	01-00-5e-00-00-fc	静态
	229.255.255.250	01-00-5e-7f-ff-fa	静态
	239.255.255.250	01-00-5e-7f-ff-fa	静态
	255.255.255.255	ff-ff-ff-ff-ff-ff	静态

实验具体步骤

2、打开Wireshark软件，双击本次实验正在使用的网络接口，开始进行抓包。



3、利用`arp -d *` 命令或`arp -d`命令清空本机的ARP缓存表。

[显示：ARP 项删除失败: 请求的操作需要提升。说明需要用管理员权限运行cmd.exe。]

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

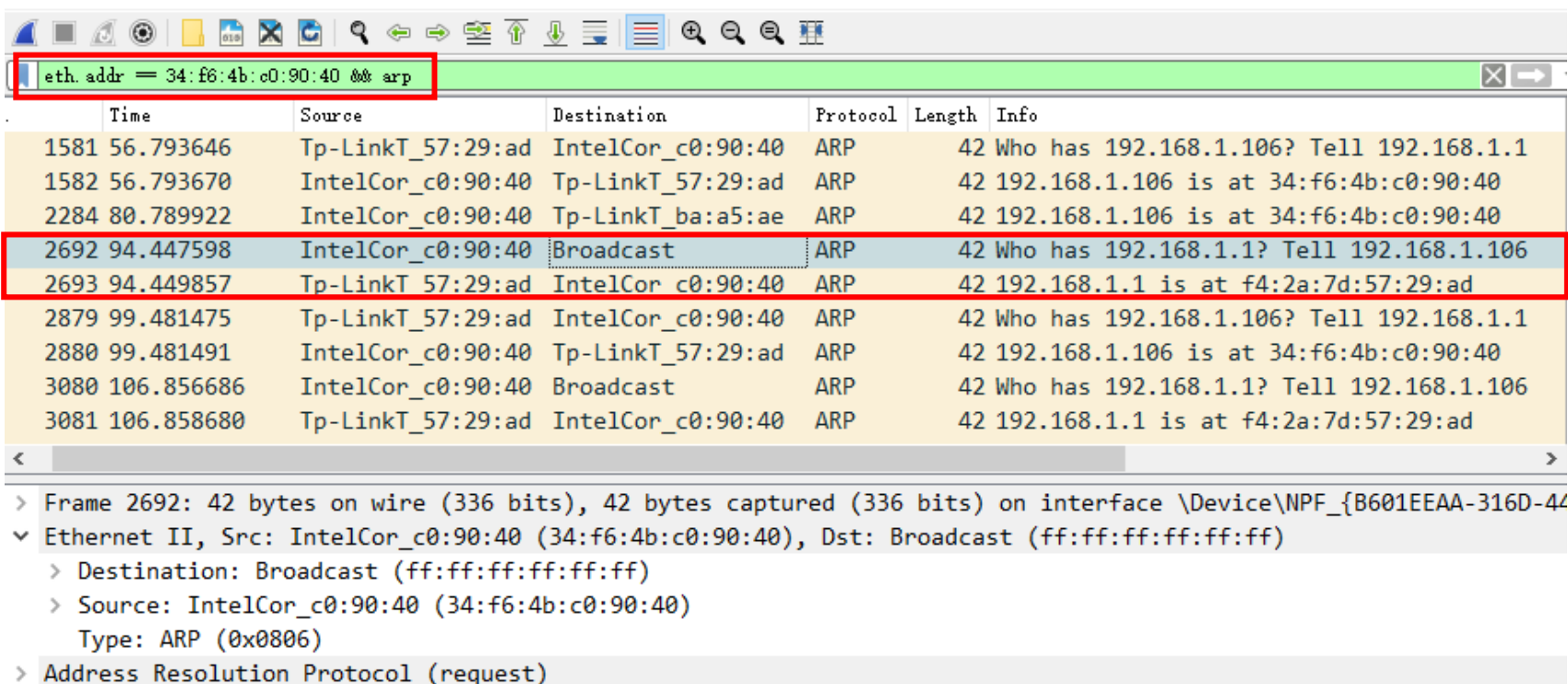
接口: 192.168.1.106 --- 0x14
Internet 地址      物理地址      类型
224.0.0.2          01-00-5e-00-00-02 静态
224.0.0.22         01-00-5e-00-00-16 静态
```

实验具体步骤

4、使用过滤表达式对捕获的数据包进行初步筛选。

eth.addr == 34:f6:4b:c0:90:40 && arp (本机MAC地址)

5、从中选取本机与默认网关交互的一组ARP数据包。



eth.addr == 34:f6:4b:c0:90:40 && arp

Time	Source	Destination	Protocol	Length	Info
1581 56.793646	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	Who has 192.168.1.106? Tell 192.168.1.1
1582 56.793670	IntelCor_c0:90:40	Tp-LinkT_57:29:ad	ARP	42	192.168.1.106 is at 34:f6:4b:c0:90:40
2284 80.789922	IntelCor_c0:90:40	Tp-LinkT_ba:a5:ae	ARP	42	192.168.1.106 is at 34:f6:4b:c0:90:40
2692 94.447598	IntelCor_c0:90:40	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
2693 94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	192.168.1.1 is at f4:2a:7d:57:29:ad
2879 99.481475	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	Who has 192.168.1.106? Tell 192.168.1.1
2880 99.481491	IntelCor_c0:90:40	Tp-LinkT_57:29:ad	ARP	42	192.168.1.106 is at 34:f6:4b:c0:90:40
3080 106.856686	IntelCor_c0:90:40	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
3081 106.858680	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	192.168.1.1 is at f4:2a:7d:57:29:ad

> Frame 2692: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B601EEAA-316D-44...}

✓ Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- > Source: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
Type: ARP (0x0806)
- > Address Resolution Protocol (request)

实验具体步骤

6、观察ARP请求分组格式，并进行分析。

eth. addr = 34:f6:4b:c0:90:40 && arp

	Time	Source	Destination	Protocol	Length	Info
	2692 94.447598	IntelCor_c0:90:40	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
	2693 94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	192.168.1.1 is at f4:2a:7d:57:29:ad

<

> Frame 2692: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B601EEAA-316D-
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40) Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1) ←
 Sender MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
 Sender IP address: 192.168.1.106
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.1.1

<

0000	ff ff ff ff ff ff 34 f6 4b c0 90 40 08 06 00 014. K..@...
0010	08 00 06 04 00 01 34 f6 4b c0 90 40 c0 a8 01 6a4. K..@...j
0020	00 00 00 00 00 00 c0 a8 01 01

实验具体步骤

7、观察ARP响应分组格式，并进行分析。

eth. addr = 34:f6:4b:c0:90:40 00 arp

	Time	Source	Destination	Protocol	Length	Info
	2692 94.447598	IntelCor_c0:90:40	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
	2693 94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	192.168.1.1 is at f4:2a:7d:57:29:ad

<

> Frame 2693: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF {B601EEAA-316D-
> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad) Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2) ←
Sender MAC address: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
Sender IP address: 192.168.1.1
Target MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
Target IP address: 192.168.1.106

<

0000	34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 06 00 01	4-K-@.* }W).....
0010	08 00 06 04 00 02 f4 2a 7d 57 29 ad c0 a8 01 01* }W).....
0020	34 f6 4b c0 90 40 c0 a8 01 6a	4-K-@... ·j

主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

实验结果与分析

请求

eth.addr == 34:f6:4b:c0:90:40 && arp				
Time	Source	Destination	Protocol	
2692 94.447598	IntelCor_c0:90:40	Broadcast	ARP	
2693 94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	
<				
> Frame 2692: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0				
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Broadcast (ff:ff:ff:ff:ff:ff)				
v Address Resolution Protocol (request)				
Hardware type: Ethernet (1)				
Protocol type: IPv4 (0x0800)				
Hardware size: 6				
Protocol size: 4				
Opcode: request (1)				
Sender MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)				
Sender IP address: 192.168.1.106				
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)				
Target IP address: 192.168.1.1				
<				
0000	ff ff ff ff ff ff 34 f6 4b c0 90 40 08 06 00 012		
0010	08 00 06 04 00 01 34 f6 4b c0 90 40 c0 a8 01 6a2		
0020	00 00 00 00 00 00 c0 a8 01 01		

响应

eth.addr == 34:f6:4b:c0:90:40 && arp				
Time	Source	Destination	Protocol	
2692 94.447598	IntelCor_c0:90:40	Broadcast	ARP	
2693 94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	
<				
> Frame 2693: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0				
> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)				
v Address Resolution Protocol (reply)				
Hardware type: Ethernet (1)				
Protocol type: IPv4 (0x0800)				
Hardware size: 6				
Protocol size: 4				
Opcode: reply (2)				
Sender MAC address: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)				
Sender IP address: 192.168.1.1				
Target MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)				
Target IP address: 192.168.1.106				
<				
0000	34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 06 00 01	4-K..@		
0010	08 00 06 04 00 02 f4 2a 7d 57 29 ad c0 a8 01 01		
0020	34 f6 4b c0 90 40 c0 a8 01 01	4-K..@		

ARP请求分组

实验结果:

eth. addr = 34:f6:4b:c0:90:40 arp

	Time	Source	Destination	Protocol	Length	Info
	2692 94.447598	IntelCor_c0:90:40	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
	2693 94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	192.168.1.1 is at f4:2a:7d:57:29:ad

<

> Frame 2692: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B601EEAA-316D-
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
- Sender IP address: 192.168.1.106
- Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.1

<

0000	ff ff ff ff ff ff 34 f6 4b c0 90 40 08 06 00 014. K..@...
0010	08 00 06 04 00 01 34 f6 4b c0 90 40 c0 a8 01 6a4. K..@...j
0020	00 00 00 00 00 00 c0 a8 01 01

实验结果与分析

实验分析：

- Hardware type: Ethernet (1) #硬件类型 (16位) : 类型为1, 所以是以太网硬件类型
- Protocol type: IPv4 (0x0800) #协议类型 (16位) : IPv4 协议, 字段值为0x0800
- Hardware size: 6 #硬件长度 (8位) : 使用48位以太网 MAC地址
- Protocol size: 4 #协议长度 (8位) : 使用32位IPv4地址
- Opcode: request (1) #操作 (16位) : 值为1表示此分组是ARP请求分组

实验结果与分析

实验分析：

- Sender MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
#发送方硬件地址： 34:f6:4b:c0:90:40 （主机MAC地址）
- Sender IP address: 192.168.1.106 #发送方IP地址：
192.168.1.106 （主机IP地址）
- Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
#目标MAC地址： 由于主机的ARP缓存已经清空， 因此主机已经不知道目标的MAC地址， 所以为全0的地址。
- Target IP address: 192.168.1.1 #目标IP地址： 192.168.1.1
（网关IP地址）

实验结果与分析

绘制ARP请求分组格式（包括以太网帧首部）：

← 以太网帧首部 → ← ARP请求分组 →

目的 MA C地 址	源 MA C地 址	上层 协议 类型	硬件 类型	协议 类型	硬件 地址 长度	协议 地址 长度	操作 类型	源 MA C地 址	源IP 地址	目的 MA C地 址	目的 IP地 址
ff:ff: ff:ff: ff:ff	34:f 6:4b :c0:9 0:40	ARP (0x0 806)	Ethe rnet 1	IPv4 0x0 800	6	4	requ est 1	34:f 6:4b :c0:9 0:40	192. 168. 1.10 6	00:0 0:00: 00:0 0:00	192. 168. 1.1

ARP响应分组

实验结果:

eth. addr = 34:f6:4b:c0:90:40 arp

	Time	Source	Destination	Protocol	Length	Info
2692	94.447598	IntelCor_c0:90:40	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
2693	94.449857	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	192.168.1.1 is at f4:2a:7d:57:29:ad

<

> Frame 2693: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B601EEAA-316D-...}

> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
Sender IP address: 192.168.1.1
Target MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
Target IP address: 192.168.1.106

<

0000	34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 06 00 01	4-K..@.* }W).....
0010	08 00 06 04 00 02 f4 2a 7d 57 29 ad c0 a8 01 01* }W).....
0020	34 f6 4b c0 90 40 c0 a8 01 6a	4-K..@.. .j

实验结果与分析

实验分析：

- Hardware type: Ethernet (1) #硬件类型 (16位) : 类型为1, 所以是以太网硬件类型
- Protocol type: IPv4 (0x0800) #协议类型 (16位) : IPv4 协议, 字段值为0x0800
- Hardware size: 6 #硬件长度 (8位) : 使用48位以太网 MAC地址
- Protocol size: 4 #协议长度 (8位) : 使用32位IPv4地址
- Opcode: reply (2) #操作 (16位) : 值为2表示此分组是 ARP响应分组

实验结果与分析

实验分析：

- Sender MAC address: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
#发送方硬件地址： f4:2a:7d:57:29:ad （网关MAC地址）
- Sender IP address: 192.168.1.1 #发送方IP地址： 192.168.1.1
（网关IP地址）
- Target MAC address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
#目标MAC地址： 34:f6:4b:c0:90:40 （主机MAC地址）。
- Target IP address: 192.168.1.1 06 #目标IP地址：
192.168.1.106 （主机IP地址）

实验结果与分析

绘制ARP响应分组格式（包括以太网帧首部）：

← 以太网帧首部 → ← ARP响应分组 →

目的 MA C地 址	源 MA C地 址	上层 协议 类型	硬件 类型	协议 类型	硬件 地址 长度	协议 地址 长度	操作 类型	源 MA C地 址	源IP 地址	目的 MA C地 址	目的 IP地 址
34:f 6:4b :c0:9 0:40	f4:2 a:7d: 57:2 9:ad	ARP (0x0 806)	Ethe rnet 1	IPv4 0x0 800	6	4	repl y 2	f4:2 a:7d: 57:2 9:ad	192. 168. 1.1	34:f 6:4b :c0:9 0:40	192. 168. 1.10 6

思考题

思考题：主机的ARP缓存中已存储了目标主机的MAC地址，在维护阶段，ARP请求分组的发送内容有何异同。

