

暨南大学本科实验报告专用纸

课程名称 《计算机网络实验》 成绩评定
实验项目名称 计算机网络协议分析 指导教师 雷小林、魏林锋
实验项目编号 实验项目类型 综合 实验地点 N117
学生姓名 陈宇 学号 2020101642
学院 信息科学技术学院 系 计算机系 专业 软件工程
实验时间 2022 年 9 月 27 日 上午~9 月 27 日 上午 温度 °C 湿度

实验目的

1. 掌握 ARP 协议的报文格式
2. 掌握 ARP 协议的工作原理
3. 理解 ARP 高速缓存的作用
4. 掌握 ARP 请求和应答的实现方法
5. 掌握 ARP 缓存表的维护过程

实验原理

● 物理地址与逻辑地址

1. 物理地址：物理地址是节点的地址，由它所在的局域网或广域网定义。物理地址包含在数据链路层的帧中。物理地址是最低一级的地址。物理地址的长度和格式是可变的，取决于具体的网络。以太网使用写在网络接口卡（NIC）上的 6 字节的标识作为物理地址。物理地址可以是单播地址（一个接收者）、多播地址（一组接收者）或

暨南大学本科实验报告专用纸(附页)

广播地址（由网络中的所有主机接收）。有些网络不支持多播或广播地址，当需要把帧发送给一组主机或所有主机时，多播地址或广播地址就需要用单播地址来模拟。

2. 逻辑地址：在互联网的环境中仅使用物理地址是不合适的，因为不同网络可以使用不同的地址格式。因此，需要一种通用的编址系统，用来惟一地标识每一台主机，而不管底层使用什么样的物理网络。逻辑地址就是为此目的而设计的。目前 Internet 上的逻辑地址是 32 位地址，通常称为 IP 地址，可以用来标识连接在 Internet 上的每一台主机。在 Internet 上没有两个主机具有同样的 IP 地址。逻辑地址可以是单播地址、多播地址和广播地址。其中广播地址有一些局限性。在实验三中 将详细介绍这三种类型的地址。

● ARP 协议介绍

ARP 是地址解析协议（Reverse Address Resolution Protocol）的缩写，负责实现从 IP 地址到物理地址（如以太网 MAC 地址）的映射。在实际通信中，物理网络使用硬件地址进行报文传输。IP 报文在封装为数据链路层帧进行传送时，就有必要把 IP 地址转换为对应的硬件地址，ARP 正是动态地完成这一功能的。

（1） ARP 报文格式

暨南大学本科实验报告专用纸(附页)

0	8	16	31
硬件类型		协议类型	
硬件地址长度	协议地址长度	操作	
源站物理地址（前 4 字节）			
源站物理地址（后 2 字节）		源站 IP 地址（前 2 字节）	
源站 IP 地址（后 2 字节）		目的站物理地址（前 2 字节）	
目的站物理地址（后 4 字节）			
目的站 IP 地址（4 字节）			

图 26 ARP 报文格式

ARP 协议报文是定长的，其格式如图 26 所示，报文中每一字段的含义如下：

- * 硬件类型：表示物理网络的类型，“0X0001”表示以太网；
- * 协议类型：表示网络网络协议类型，“0X0800”表示 IP 协议；
- * 硬件地址长度：指定源/ 目的站物理地址的长度，单位为字节；
- * 协议地址长度：指定源/ 目的站 IP 地址的长度，单位为字节；
- * 操作：指定该报文的类型，“1”为 ARP 请求报文，“2”为 ARP 响应报文；
- * 源端硬件/IP 地址：由 ARP 请求者填充；
- * 目的站物理地址：在请求报文中为 0，在响应报文中，由由发送响应报文的主机填写 接收该报文的目的是主机的物理地址；
- * 目的站 IP 地址：由 ARP 请求者填充，指源端想要知道的主机的 IP 地址。只有 IP 地址等于该 IP 地址的主机才向源主机发送相应报文。

(2) ARP 的工作方式

在以太网中，每台使用 ARP 协议实现地址解析的主机都在自己的高速缓存中维护着一个地址映射表，这个 ARP 表中存放着最近和它通信的同网络中的计算机 IP 地址和对应的 MAC 地址。具体运行过程如下：

- 发送端知道目的端的 IP 地址。
- IP 要求 ARP 创建一个 ARP 请求报文，其中包含了发送方的物理地址、发送方的 IP 地址和目的端的 IP 地址。目的端的物理地址用 0 填充。
- 将报文传递到数据链路层，并在该层中用发送方的物理地址作为源地址，用物理广播地址作为目的地址，将其封装在一个帧中。
- 因为该帧中包含了一个广播目的地址，所以同一链路中的每个主机或路由器都接收到这个帧。所有接收到该帧的主机都将其传递到 ARP 层进行处理。除了目的端主机以外的所有主机都丢弃该报文。
- 目的端主机用一个包含其物理地址的 ARP 应答报文做出响应，并对该报文进行单播。发送方接收到这个应答报文，这样它就知道了目标主机的物理地址。

ARP 地址解析过程 如下图所示。

暨南大学本科实验报告专用纸(附页)

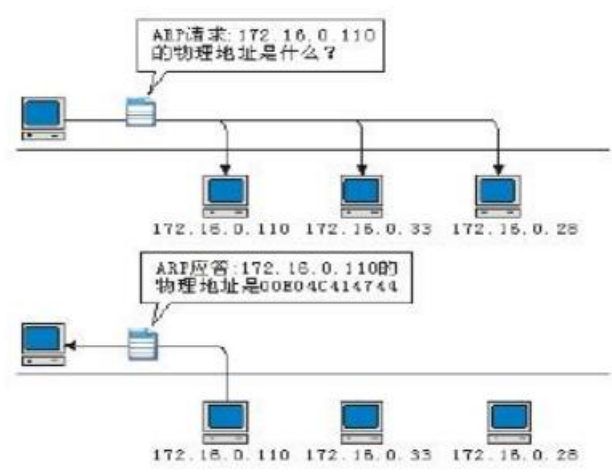


图 4-4 ARP 地址解析过程

注意：不同网络中的 IP 地址将对应网关。当两台计算机通信时，源主机首先查看自己的 ARP 表中是否有目的主机的 IP 地址项，若有则使用对应的 MAC 地址直接向目的主机发送信息；否则就向网络中广播一个 ARP 请求 报文，当网络中的主机收到该 ARP 请求报文时，首先查看报文中的目的 IP 地址是否与自己 的 IP 地址相符，若相符则将请求报文中的源 IP 地址和 MAC 地址写入自己的 ARP 表中；然 后，创建一个 ARP 响应报文，将自己的 MAC 地址填入该响应报文中，发送给原主机。ARP 高 速缓存表如下：

Internet 地址	物理地址	类型
192.168.3.1	44-5e-56-07	动态
192.168.3.255	ff-ff-ff-ff-ff-ff	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
239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态

发送 IP 数据报前先对 ARP 缓存表进行查找，查看目的 MAC 地址是否存在于缓存表 中，如果存在，则不需要发送 ARP 请求报文而直接使用此地址进行 IP 数据包的发送。如 果不存在，则发送 ARP 请求报文，在收到 ARP 应答报文之后，使用应答报文中的目的 MAC 地址发送 IP 数据包，并将目的 MAC 地址存于 ARP 缓存表中供以后使用。另外，ARP 缓存表采用老化机制，在一段时间内如果表中的某一项没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。 注意：ARP 响应报文不再广播，而是直接发送给请求者。

暨南大学本科实验报告专用纸(附页)

● Arp 命令简介

本次实验使用的 Windows 自带的 Arp 命令提供了显示和修改地址解析协议所使用的地址映射表的功能。

Arp 命令的格式要求如下：

ARP -s inet_addr eth_addr [if_addr]

ARP -d inet_addr [if_addr]

ARP -a [inet_addr] [-N if_addr]

其中：

* -s: 在 ARP 缓存中添加表项：将 IP 地址 inet_addr 和物理地址 ether_addr 关联，物理地址由以连字符分隔的 6 个十六进制数给定，使用点分十进制标记指定 IP 地址，添加项是永久性的；

* -d: 删除由 inet_addr 指定的表项；

* -a: 显示当前 ARP 表，如果指定了 inet_addr 则只显示指定计算机的 IP 和物理地址；

* inet_addr: 以点分十进制标记指定 IP 地址；

* -N: 显示由 if_addr 指定的 ARP 表项；

* if_addr: 指定需要选择或修改其地址映射表接口的 IP 地址；

* ether_addr: 指定物理地址；

实验环境

实验设备和连接图如图 27 所示，一台 S2126G 交换机连接了 2 台 PC 机，分别命名为 主机 A、主机 B，交换机命名为 Switch。图 27ARP 协议分析实验连接图

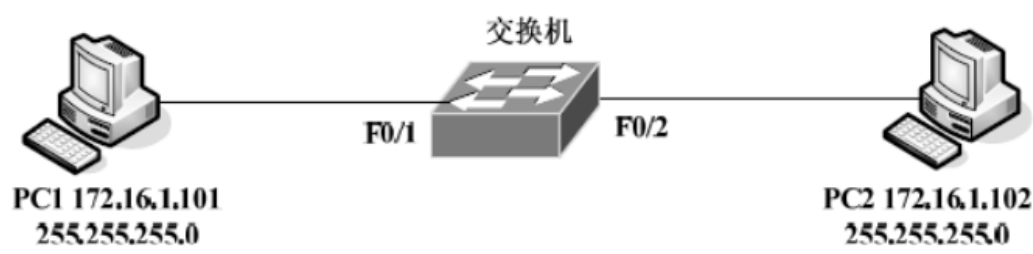


图 27ARP 协议分析实验连接图

实验内容

练习一：领略真实的 ARP

步骤 1：在主机 A、主机 B 两台计算机上执行如下命令，清除 ARP 缓存： ARP -d

步骤 2：在主机 A、主机 B 两台计算机上执行如下命令，查看高速缓存中的 ARP 地址映射表的内容： ARP -a

```
C:\Users\Administrator>ARP -d
C:\Users\Administrator>arp -a
接口: 172.23.65.91 --- 0xb
Internet 地址      物理地址      类型
224.0.0.22        01-00-5e-00-00-16 静态
224.0.2.32        01-00-5e-00-02-20 静态
229.111.112.12    01-00-5e-6f-70-0c 静态
255.255.255.255   ff-ff-ff-ff-ff-ff 静态
C:\Users\Administrator>
```

步骤 3：在主机 A 和主机 B 上运行 Wireshark 截获报文，为了

暨南大学本科实验报告专用纸(附页)

截获和实验内容有关的报文，Wireshark 的 Capture Filter 设置为默认方式；

步骤 4：在主机 A 上执行“Ping 主机 B IP 地址”命令向主机 B 发送数据报；（注查看 IP 的命令是 ipconfig/all）；

步骤 5：执行完毕，在 Wireshark 中输入“arp || icmp”过滤数据报，保存截获的报文并命名为 arp-1-学号；

步骤 6：在主机 A、主机 B 两台计算机上再次执行 ARP -a 命令，查看高速缓存中的 ARP 地址映射表的内容：

```
C:\Users\Administrator>ARP -a

接口: 172.23.65.91 --- 0xb
Internet 地址      物理地址      类型
172.23.65.92      3c-52-82-7a-d1-58 动态
172.23.65.255     ff-ff-ff-ff-ff-ff 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
224.0.2.32        01-00-5e-00-02-20 静态
229.111.112.12    01-00-5e-6f-70-0c 静态
255.255.255.255   ff-ff-ff-ff-ff-ff 静态

C:\Users\Administrator>
```

- 这次看到的内容和步骤 3 的内容相同吗？结合两次看到的结果，理解 ARP 高速缓存的作用。

答：不相同，ARP 高速缓存里存放了之前进行 ARP 请求和 ARP 应答中的 IP 地址和 MAC 地址对应列表。

作用：下次再次访问 ARP 中已缓存的 IP 地址时，不需要再次发送 ARP 请求去获取 MAC 地址。可以提高链路的效率。

暨南大学本科实验报告专用纸(附页)

- 把这次看到的高速缓存中的 ARP 地址映射表写出来。

```
C:\Users\Administrator>ARP -a

接口: 172.23.65.91 --- 0xb
Internet 地址      物理地址      类型
172.23.65.92      3c-52-82-7a-d1-58      动态
172.23.65.255      ff-ff-ff-ff-ff-ff      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
224.0.2.32         01-00-5e-00-02-20      静态
229.111.112.12     01-00-5e-6f-70-0c      静态
255.255.255.255    ff-ff-ff-ff-ff-ff      静态

C:\Users\Administrator>
```

步骤 8：重复步骤： 4—6，将此结果保存为 arp-2-学号；

步骤 9：打开 arp-1-学号，完成以下各题：

- 在截获的报文中由几个 ARP 报文？在以太网帧中，ARP 协议类型的代码值是什么？

12696 5.057575	HewlettP_73:69:df	Broadcast	ARP	60 Who has 172.23.65.46? Tell 172.23.65.45
12697 5.057576	HewlettP_7d:05:95	HewlettP_7a:d1:58	ARP	60 172.23.65.93 is at 18:60:24:7d:05:95

答：有两类 ARP 报文，一类是广播请求获取目的 IP 地址的 MAC 地址，一类是来自目的 IP 地址的响应，ARP 协议类型的代码值是 0806

- 打开 arp-2-学号，比较两次截获的报文有何区别？分析其原因。

答：第二次的报文不需要进行广播 ARP 了，因为已经缓存对应 IP 的 MAC 的地址了。

暨南大学本科实验报告专用纸(附页)

- 分析 arp-1 中 ARP 报文的结构，完成表 11。

ARP 请求报文		ARP 应答报文	
字段	报文信息及参数	字段	报文信息及参数
硬件类型	00 01	硬件类型	00 01
协议类型	08 00	协议类型	08 00
硬件地址长度	06	硬件地址长度	06
协议地址长度	04	协议地址长度	04
操作	00 01	操作	00 02
源站物理地址	18 60 24 7d 05 9c	源站物理地址	3c 52 82 7a d1 58
源站 IP 地址	172.23.65.91	源站 IP 地址	172.23.65.92
目的站物理地址	00 00 00 00 00 00	目的站物理地址	18 60 24 7d 05 9c
目的站 IP 地址	172.23.65.92	目的站 IP 地址	172.23.65.91

练习二、编辑并发送 ARP 报文

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

步骤 1：在主机 E 上启动协议编辑器，并编辑一个 ARP 请求报文。
其中。

MAC 层：

目的 MAC 地址：设置为 FFFFFFFF-FFFFFF

暨南大学本科实验报告专用纸(附页)

源 MAC 地址：设置为主机 E 的 MAC 地址 (注查看 MAC 地址的命令是 ipconfig/all)

协议类型或数据长度：0806

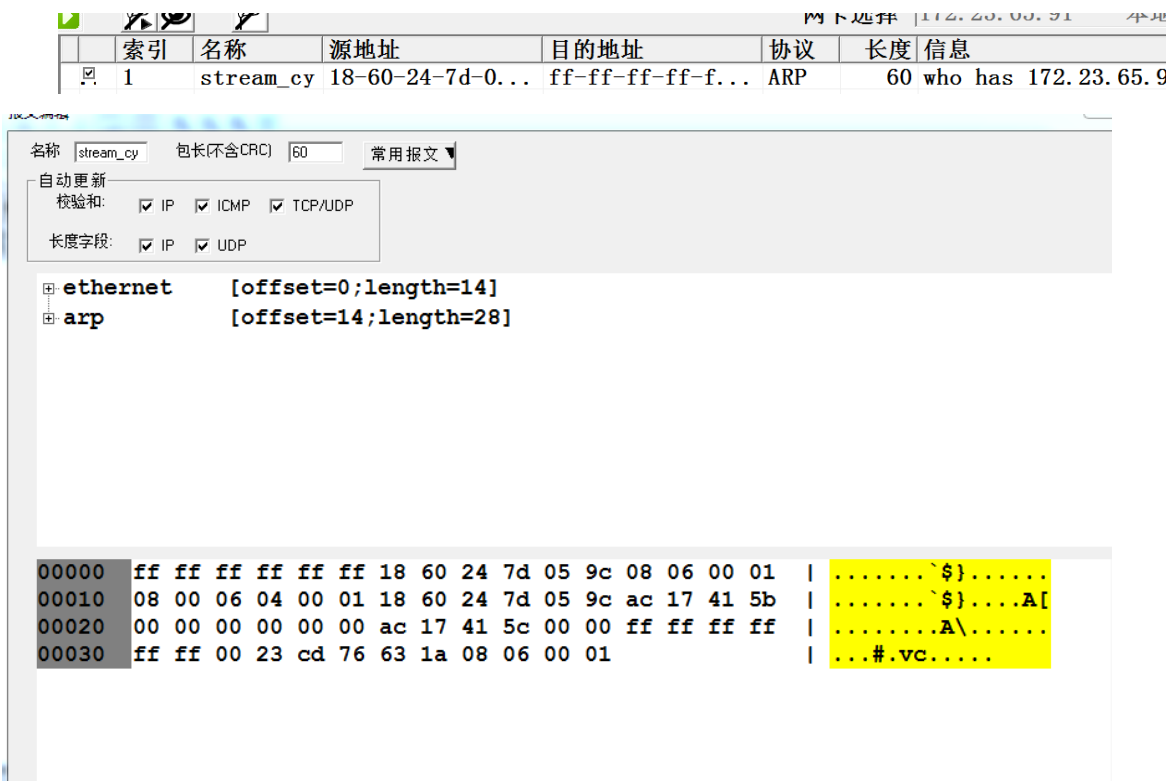
ARP 层：

发送端硬件地址：设置为主机 E 的 MAC 地址

发送端逻辑地址：设置为主机 E 的 IP 地址

目的端硬件地址：设置为 000000-000000

目的端逻辑地址：设置为主机 F 的 IP 地址



步骤 2: 主机 A、B、C、D、F 启动 Wireshark, 打开捕获窗口进行数据捕获并设置过滤条件 (提取 ARP 协议)。

暨南大学本科实验报告专用纸(附页)

步骤 3: 主机 B、E、F 在命令行下运行 “arp -d” 命令，清空 ARP 高速缓存。主机 E 发送 已编辑好的 ARP 报文。

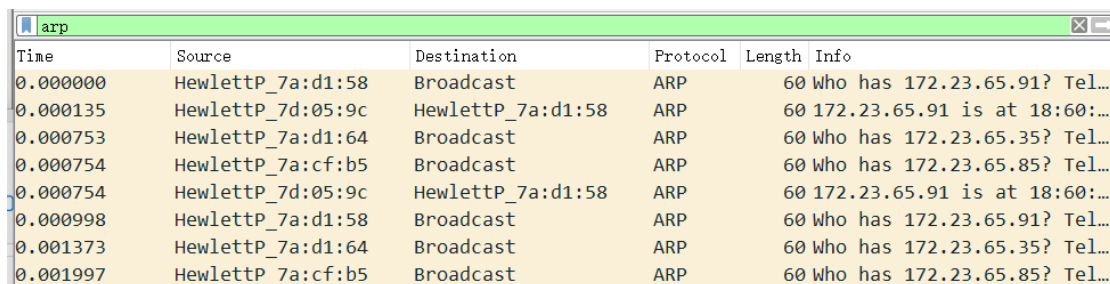
步骤 4: 主机 A、B、C、D、F 停止捕获数据，分析捕获到的数据，进一步体会 ARP 报文 交互过程。

实验思考

思考问题：

哪些主机收到了 ARP 请求包，哪个主机给出了 ARP 响应包？为什么？

答：主机 A、B、C、D、F 都收到了 ARP 请求包，只有主机 F 给出了 ARP 响应包。



The image shows a Wireshark packet capture window titled 'arp'. It displays a list of captured packets with columns for Time, Source, Destination, Protocol, Length, and Info. The packets are ARP requests and responses. The first packet is a broadcast request from HewlettP_7a:d1:58. The second packet is a response from HewlettP_7d:05:9c to HewlettP_7a:d1:58. The third packet is a broadcast request from HewlettP_7a:d1:64. The fourth packet is a broadcast request from HewlettP_7a:cf:b5. The fifth packet is a response from HewlettP_7d:05:9c to HewlettP_7a:d1:58. The sixth packet is a broadcast request from HewlettP_7a:d1:58. The seventh packet is a broadcast request from HewlettP_7a:d1:64. The eighth packet is a broadcast request from HewlettP_7a:cf:b5.

Time	Source	Destination	Protocol	Length	Info
0.000000	HewlettP_7a:d1:58	Broadcast	ARP	60	Who has 172.23.65.91? Tel...
0.000135	HewlettP_7d:05:9c	HewlettP_7a:d1:58	ARP	60	172.23.65.91 is at 18:60:...
0.000753	HewlettP_7a:d1:64	Broadcast	ARP	60	Who has 172.23.65.35? Tel...
0.000754	HewlettP_7a:cf:b5	Broadcast	ARP	60	Who has 172.23.65.85? Tel...
0.000754	HewlettP_7d:05:9c	HewlettP_7a:d1:58	ARP	60	172.23.65.91 is at 18:60:...
0.000998	HewlettP_7a:d1:58	Broadcast	ARP	60	Who has 172.23.65.91? Tel...
0.001373	HewlettP_7a:d1:64	Broadcast	ARP	60	Who has 172.23.65.35? Tel...
0.001997	HewlettP_7a:cf:b5	Broadcast	ARP	60	Who has 172.23.65.85? Tel...

因为只有和收到 ARP 请求包中的目的 IP 地址相同的主机才会给出 ARP 响应包，其余主机则会将其抛弃，但其会记录发送请求包主机的 IP 地址及其 MAC 地址，并将其存入 ARP 高速缓存中。

暨南大学本科实验报告专用纸(附页)
