网络协议分析实验

计算机学院 谢牧航 2022211363

目录

第一章 实验内容和实验环境描述

第二章 实验步骤和协议分析

2.1 IP 协议分析

2.1.1 捕获短 IP 分组

输入命令 `ping 10.3.9.161`，将 Wireshark 过滤器设置为 `icmp`，捕获到数个 ICMP 数据包，其中一个由 `10.3.9.161` 发回的数据包的 IP 包头如下：

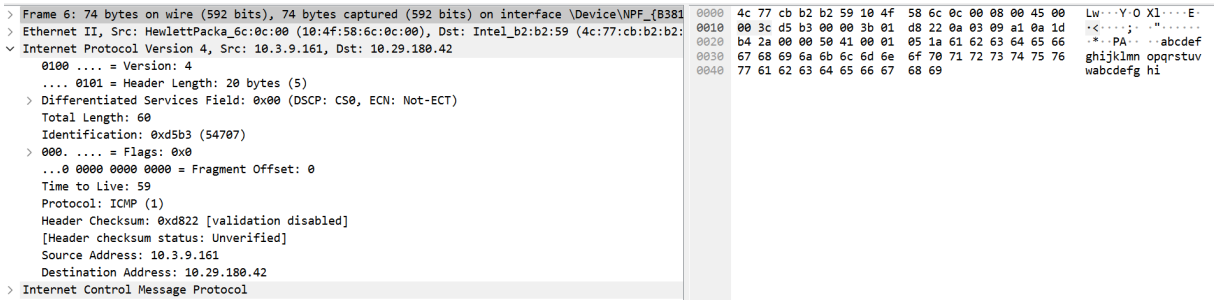


图 1　捕获到的短 IP 协议数据包头

2.1.2 捕获长 IP 分组

输入命令 `ping 10.3.9.161 -l 8000 -n 1`，向目的主机发送一个长度为 8000 字节的 ICMP 数据包。Wireshark 过滤器设置为 `ip.dst == 10.29.180.42`，捕获到一组六个 ICMP 数据包如下。

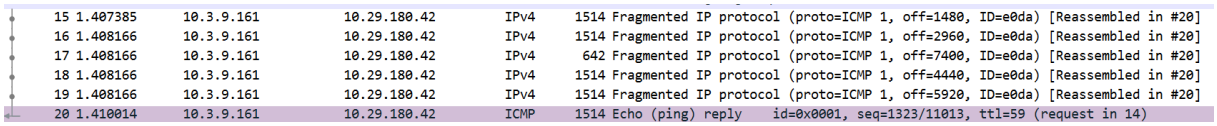


图 2　捕获到的长 IP 协议数据分片

以下展示第一个分片的 IP 包头内容和最后一个分片的 IP 包头内容：

(a) 第一个分片的 IP 包头内容　　(b) 最后一个分片的 IP 包头内容

图 3　长 IP 数据包头详细信息

2.1.3IP 包头内容分析

短 IP 分组：

字段 (字节数)	内容（16 进制）	解释
Version & HL(1)	45	版本：IPv4，头长度：20 字节
DSCP (1)	00	服务类型：正常时延，正常吞吐量，正常可靠性
Total Length (2)	00 3c	总长度：60 字节

字段 (字节数)	内容（16 进制）	解释
Identification (2)	d5 b3	分组标识：0×d5b3
Flags (1)	00	标志：MF = 0, DF = 0，允许分片，此片为最后一片
Fragment Offset (1)	00	片偏移：偏移量为 0
TTL (1)	3b	生存周期：每跳生存时间为 59 秒
Protocol (1)	01	协议：ICMP 协议
Header CheckSum (4)	d8 22	头部校验和：0×d822
Source IP Address (4)	0a 03 09 a1	源地址：10.3.9.161
Destimation IP Address (4)	0a 1d b4 2a	目标地址：10.29.180.42

长 IP 分组（第一个分片）:

字段 (字节数)	内容（16 进制）	解释
Version & HL(1)	45	版本：IPv4，头长度：20 字节
DSCP (1)	00	服务类型：正常时延，正常吞吐量，正常可靠性
Total Length (2)	05 dc	总长度：1500 字节
Identification (2)	e0 da	分组标识：0×e0da
Flags (1)	20	标志：MF = 0, DF = 1，允许分片，此片不是最后一片
Fragment Offset (1)	00	片偏移：偏移量为 0
TTL (1)	3b	生存周期：每跳生存时间为 59 秒
Protocol (1)	01	协议：ICMP 协议
Header CheckSum (4)	a7 5b	头部校验和：0×a75b
Source IP Address (4)	0a 03 09 a1	源地址：10.3.9.161
Destimation IP Address (4)	0a 1d b4 2a	目标地址：10.29.180.42

六个分组的区别分别为 MF 标志位和 Fragment Offset 字段。

分组序号	MF 标志位	分段偏移量	数据长度
14	1	0	1480
15	1	1480	1480
16	1	2960	1480
17	1	4440	1480
18	1	5920	1480
19	0	7400	608

2.1.4IP 包头问题解答

1. **包头校验和验证（以短 IP 分组为例）**

IP 首部的检验和不采用复杂的 CRC 检验码而采用下面的简单计算方法：

在发送方，先把 IP 数据报首部划分为许多 16 位字的序列，并把检验和字段置零。用反码算术运算把所有 16 位字相加后，将得到的和的反码写入检验和字段。

接收方收到数据报后，将首部的所有 16 位字再使用反码算术运算相加一次。将得到的和取反码，即得出接收方检验和的计算结果。

若首部未发生任何变化，则此结果必为 0，于是就保留这个数据报。否则即认为出差错。

以短 IP 分组为例，其头部校验和为 `0×d822`，计算过程如下：

```
ffff - (4500 + 003c + d5b3 + 0000 + 3b01 + 0a03 + 09a1 + 0a1d + b42a) = d822
```

2. **分片的 MF 标志位和分段偏移量**

IP 数据报分片时，每个分片的标志字段中的 MF（More Fragment）位和 DF（Don’t Fragment）位用于指示分片的情况。MF 位为 1 表示后面还有分片，为 0 表示这是最后一个分片；DF 位为 1 表示不允许分片，为 0 表示允许分片。

分段偏移量字段指示了当前分片在原始数据报中的位置。第一个分片的偏移量为 0，后续分片的偏移量为前一个分片的偏移量加上前一个分片的数据长度。

以长 IP 分组为例，其分片的 MF 标志位和分段偏移量如下：

- 第一个分片：MF = 1，分段偏移量 = 0
- 第二个分片：MF = 1，分段偏移量 = 1480
- 第三个分片：MF = 1，分段偏移量 = 2960
- 第四个分片：MF = 1，分段偏移量 = 4440
- 第五个分片：MF = 1，分段偏移量 = 5920
- 第六个分片：MF = 0，分段偏移量 = 7400

从分段偏移量可以看出，每个分片的数据长度为 1480 字节，这是因为原始数据包的长度为 8000 字节（实际上是 8008 字节，因为 ICMP 协议的规定，报文会包含产生 ICMP 差错报文的 IP 数据包的前 8 个字节），超过了以太网的最大传输单元（MTU），因此需要分片传输。而以太网数据链路层的最大传输单元为 1500 字节，去除 IP 首部的 20 字节，剩下 1480 字节。而最后一段的数据长度为 608 字节，因为原始数据包的长度为 8000 字节，减去前五个分片的总长度（$1480 \times 5 = 7400$），剩下的就是 608 字节。

2.2 ICMP 协议分析

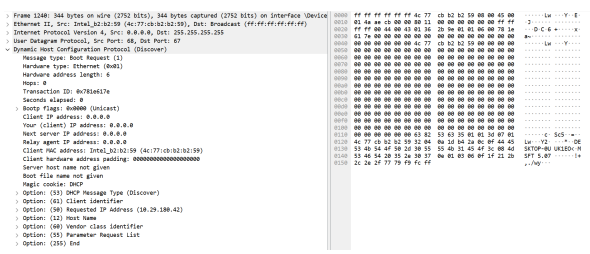
2.3 DHCP 协议分析

2.3.1 捕获 DHCP 协议数据包

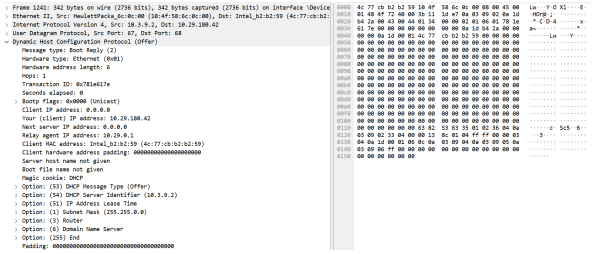
在 Wireshark 软件中输入过滤器 `udp port 67`，在终端执行 `ipconfig -release` 和 `ipconfig -renew`，过滤出四个 DHCP 协议数据包如图。

1240 43.973997	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover - Transaction ID 0x781e617e
1241 43.987473	10.3.9.2	10.29.180.42	DHCP	342 DHCP Offer - Transaction ID 0x781e617e
1242 43.994791	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0x781e617e
1243 44.003438	10.3.9.2	10.29.180.42	DHCP	342 DHCP ACK - Transaction ID 0x781e617e

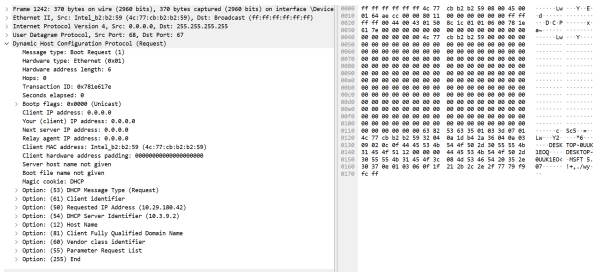
图 4　捕获到的 DHCP 协议数据包



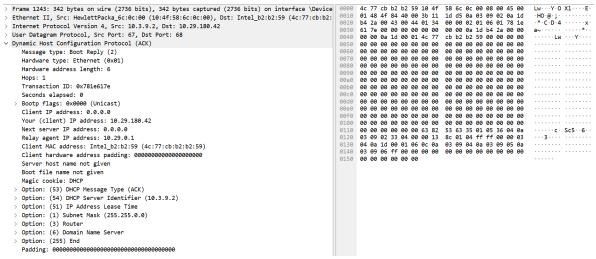
(a) DHCP Discover



(b) DHCP Offer



(c) DHCP Request



(d) DHCP Ack

图 5　DHCP 协议数据包详细信息

2.3.2DHCP 数据包内容分析

DHCP Discover:

字段 (字节数)	内容（16 进制）	解释
OP (1)	`01`	消息类型：引导请求
HTYPE (1)	`01`	硬件地址类型：以太网
HLEN (1)	`06`	硬件地址长度：6
HOPS (1)	`00`	经过的 DHCP 中继的数目：0
XID (4)	`78 1e 61 7e`	处理 ID，标记一次 IP 地址请求过程：`0×781e617e`，后面 ID 相同的数据包属于同一次 DHCP 请求
SECS (2)	`00 00`	从获取到 IP 地址或者续约过程开始到现在所消耗的时间：0 秒
FLAGS (2)	`00 00`	标记：第一位为 0，表示单播

字段 (字节数)	内容（16 进制）	解释
CIADDR (4)	00 00 00 00	客户端 IP 地址
YIADDR (4)	00 00 00 00	服务器给你分配的 IP 地址
SIADDR (4)	00 00 00 00	在 bootstrap 过程中下一台服务器的地址
GIADDR (4)	00 00 00 00	客户端发出请求（没有经过中继）
CHADDR (16)	4c 77 cb b2 b2 59	客户端的 MAC 地址
CHADDR Padding (10)	00 00 00 00 00 00 00 00 00 00	MAC 地址填充
SNAME (64)	00 00 ...	为客户端分配 IP 地址的服务器域名：未给出
FILE (128)	00 00 ...	为启动客户端指定的配置文件路径：未给出
Magic Cookie(4)	63 82 53 63	可选字段的格式：DHCP
OPTION (3)	35 01 01	DHCP 消息类型：Discover
OPTION (9)	3d 07 01 4c 77 cb b2 b2 59	客户端标识符：以太网，MAC 地址 4c:77:cb:b2:b2:59
OPTION (6)	32 04 0a 1d b4 2a	请求的 IP 地址：10.29.180.42
OPTION (17)	0c 0f ...	主机名，长度为 15
OPTION (8)	3c 08 ...	供应商标识符，长度为 8
OPTION (16)	37 0e ...	参数需求列表，长度为 14
OPTION (1)	ff	选项字段结束

以下忽略重复部分，展示各数据包不同的部分：

DHCP Offer:

字段 (字节数)	内容（16 进制）	解释
OP (1)	02	消息类型：引导回复
HOPS (1)	01	经过的中继的数目：1
YIADDR (4)	0a 1d b4 2a	服务器分配的地址：10.29.180.42
GIADDR (4)	0a 1d 00 01	客户端发出请求分组后经过的第一个中继的地址：10.29.0.1
OPTION (3)	35 01 02	DHCP 消息类型：Offer
OPTION (6)	36 04 0a 03 09 02	DHCP 服务器标识符：10.3.9.2
OPTION (6)	33 04 00 00 13 8c	IP 地址释放时间：5004 秒
OPTION (6)	01 04 ff ff 00 00	子网掩码：255.255.0.0
OPTION (6)	03 04 0a 1d 00 01	路由器：10.29.0.1

字段 (字节数)	内容（16 进制）	解释
OPTION (10)	06 0c 0a 03 09 04 0a 03 09 05 0a 03 09 06	域名服务器：10.3.9.4、10.3.9.5、10.3.9.6
OPTION (1)	ff	选项字段结束

DHCP Request:

字段 (字节数)	内容（16 进制）	解释
OPTION (3)	35 01 03	DHCP 消息类型：Request
OPTION (9)	3d 07 01 4c 77 cb b2 b2 59	客户端标识符：以太网，MAC 地址 4c:77:cb:b2:b2:59
OPTION (6)	32 04 0a 1d b4 2a	请求的 IP 地址：10.29.180.42
OPTION (6)	36 04 0a 03 09 02	DHCP 服务器标识符：10.3.9.2
…		
OPTION (1)	ff	选项字段结束

DHCP ACK:

字段 (字节数)	内容（16 进制）	解释
OP (1)	02	消息类型：引导回复
HOPS (1)	00	经过的 DHCP 中继的数目：1
YIADDR (4)	0a 1d b4 2a	服务器分配的地址：10.29.180.42
GIADDR (4)	0a 1d 00 01	客户端发出请求分组后经过的第一个中继的地址：10.29.0.1
OPTION (3)	35 01 05	DHCP 消息类型：ACK
…		
OPTION (1)	ff	选项字段结束

2.3.3DHCP 分配过程和问题解答

DHCP（动态主机配置协议）是用于在网络上自动分配 IP 地址和其他相关配置信息的通信协议。这个过程通常包括四个主要步骤：Discover、Offer、Request、和 ACK，具体如下：

1. **DHCP Discover**

   客户端连接到网络后，如果需要动态 IP 地址，它会广播一个 DHCP Discover 消息。这个消息是客户端寻求可用的 DHCP 服务器来获取 IP 配置的请求。此消息中包含客户端的硬件（MAC）地址和其他识别信息。

2. **DHCP Offer**

   网络上的 DHCP 服务器接收到 Discover 消息后，会对该请求做出响应，发送一个 DHCP Offer 消息。这个消息包括一个服务器提供给客户端的 IP 地址，同时还包括其他网络配置信

息，如子网掩码、默认网关、DNS 服务器地址等。如果网络上有多个 DHCP 服务器，客户端可能会收到多个 Offer。

3. **DHCP Request**

   客户端从一个或多个 Offer 中选择一个，并通过广播发送一个 DHCP Request 消息来请求这些网络参数。这个消息不仅重新请求先前 Offer 中提供的 IP 地址，还确认了客户端将接受哪个 DHCP 服务器的配置（通常是第一个收到的 Offer）。

4. **DHCP ACK**

   最后，DHCP 服务器接收到 Request 后，会发送一个 DHCP ACK 消息给客户端。这个 ACK 消息确认了 IP 地址和其他配置的分配，并可能包含其他详细信息，如租约的持续时间，即客户端可以保持这个 IP 地址的时间。成功接收到 ACK 消息后，客户端会配置其网络接口使用这些参数，并可以开始网络通信。

从数据包中可以推断出关于 DHCP 服务器和 DHCP 中继（Relay）的使用情况：

1. 是否有 DHCP Relay?

是的，存在 DHCP Relay 的使用。这可以从 DHCP Offer 和 DHCP ACK 消息中 GIADDR 字段的值判断。GIADDR（Gateway IP Address）字段在 DHCP Relay 环境中用来标识客户端请求消息首次经过的 DHCP Relay 代理的 IP 地址。在这些消息中，GIADDR 被设置为 `0a 1d 00 01`（即 `10.29.0.1`），且 HOPS 字段为 1，表明请求在到达 DHCP 服务器前经过了恰好一个 DHCP Relay。

1. DHCP Server 是否由路由器充当?

由服务器标识符（DHCP Server Identifier）选项看出，DHCP 服务器的 IP 地址是 `10.3.9.2`。这个地址不是我的网关地址（`10.29.0.1`），因此 DHCP 服务器不是由我的路由器充当的。查询可知，这个地址是北京邮电大学的 DHCP 服务器地址。

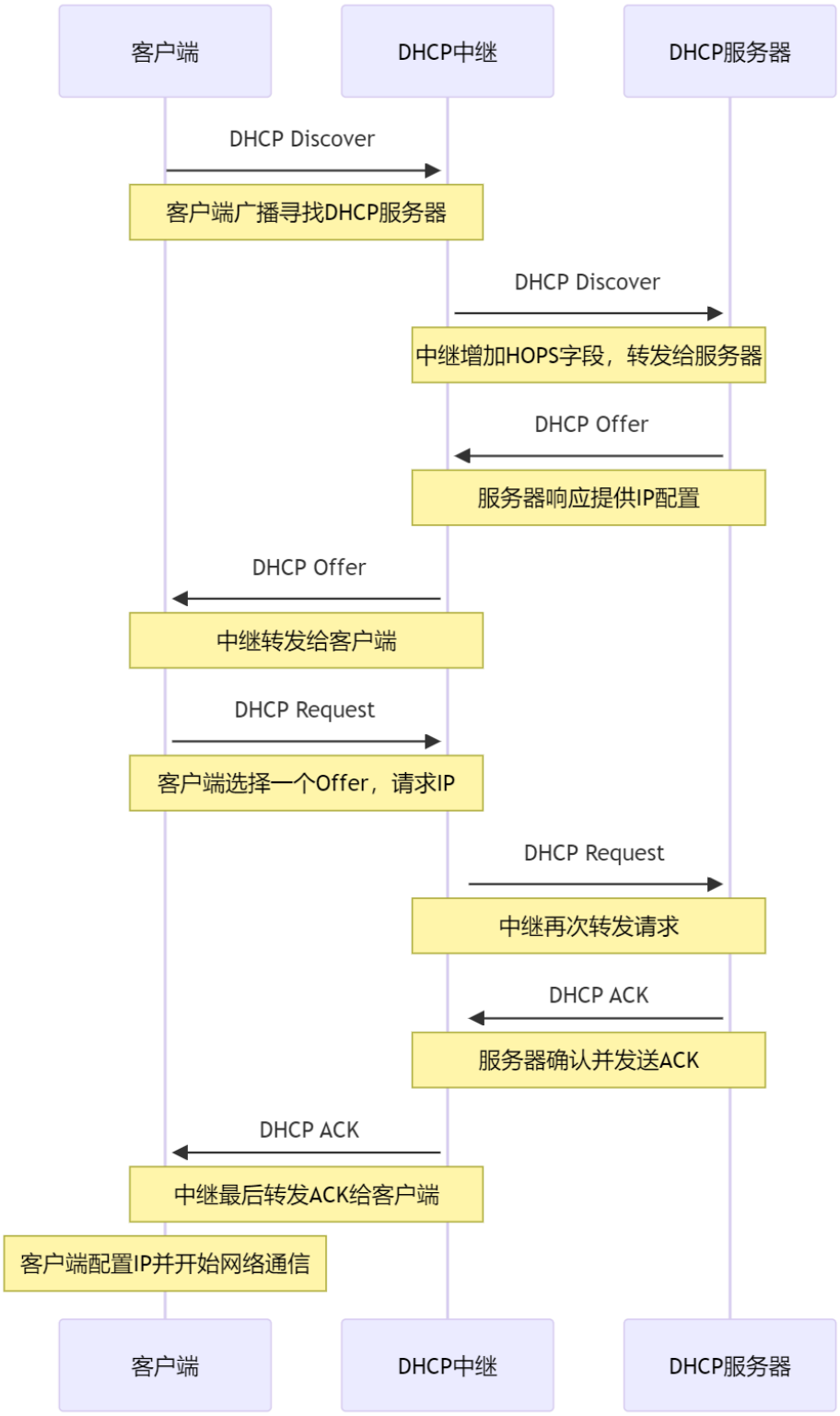
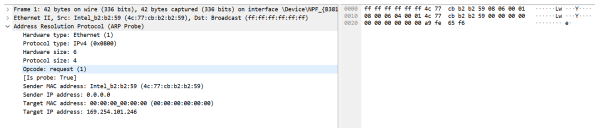


图 6　DHCP 地址分配过程的消息序列图

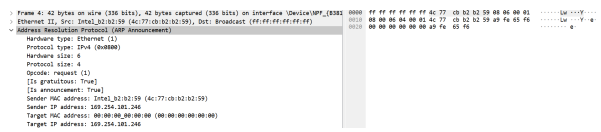
2.4 ARP 协议分析

2.4.1 捕获 ARP 协议数据包

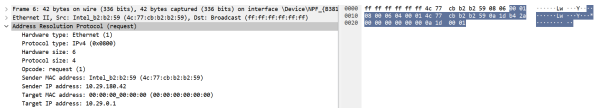
执行 `ipconfig -release` 和 `ipconfig -renew` 释放和续约 IP 地址，Wireshark 过滤器输入 `arp`，捕获到四种 ARP 协议数据包如下：



(a) ARP Probe



(b) ARP Announcement



(c) ARP Request

(d) ARP Reply

图 7　ARP 协议数据包详细信息

查询可知，还有一种免费 ARP 包（Gratuitous ARP）,免费 ARP 数据包是主机发送 ARP 查找自己的 IP 地址。通常，它发生在系统引导期间进行接口配置的时候。通过以太网线与另一台主机相连，重启另一台主机后捕获到 Gratuitous ARP 数据包如下：

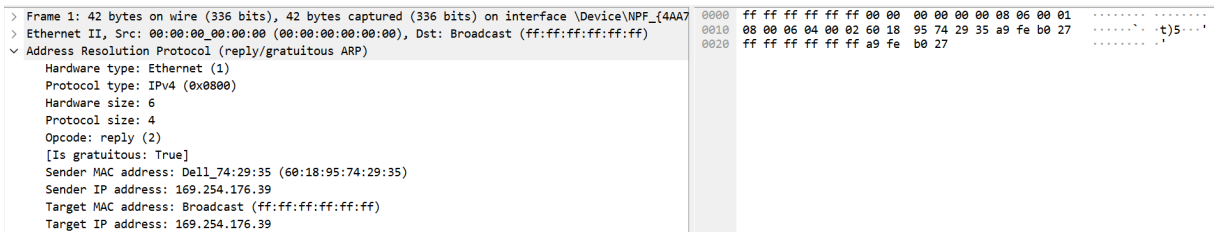
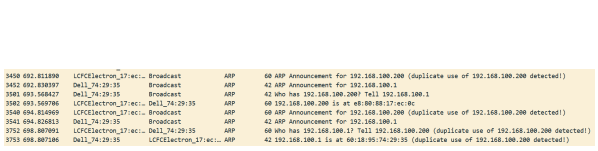
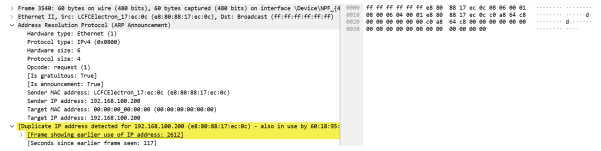


图 8　捕获到的 Gratuitous ARP 数据包

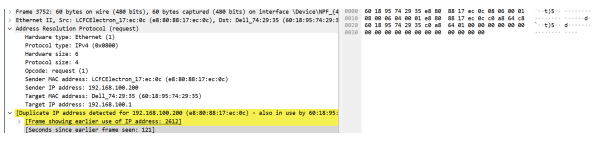
通过以太网线和另一台主机相连，并手动将两者的 IP 地址设置为同一地址，可以捕获到 IP 地址冲突时的 ARP 数据包：



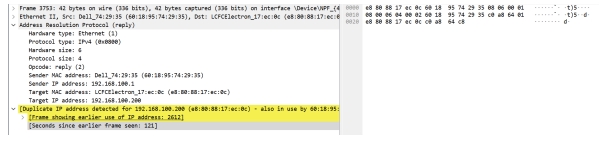
(a) ARP 冲突时的现象



(b) ARP Announcement（主机 1）



(c) ARP Request（主机 1）



(d) ARP Reply（主机 2）

图 9　ARP 冲突时的协议数据包详细信息

2.4.2ARP 数据包内容分析

分析 ARP 数据包组成如下。一开始未分配 IP，IP 地址询问经过了 `169.254.101.246` -> `10.29.180.42` 的分配过程。以下展示了分配 `10.29.180.42` 后的 ARP 数据包内容：

ARP Probe:

字段 (字节数)	内容（16 进制）	解释
HTYPE (2)	`00 01`	硬件类型：以太网
PTYPE (2)	`08 00`	协议类型：IPv4
HLEN (1)	`06`	硬件地址长度：6
PLEN (1)	`04`	协议地址长度：4
OPER (2)	`00 01`	ARP 消息类型：request
SHA (6)	`4c 77 cb b2 b2 59`	发送方 MAC 地址：`4c:77:cb:b2:b2:59`
SPA (4)	`00 00 00 00`	发送方 IP 地址：`0.0.0.0`（未分配状态）
THA (6)	`00 00 00 00 00 00`	接收方 MAC 地址（未知）
TPA (6)	`a9 fe 65 f6`	接收方 IP 地址：`10.29.180.42`，查询是否被分配

分配后，本机会宣布 ARP Announcement:

ARP Announcement:

字段 (字节数)	内容（16 进制）	解释
SHA (6)	`4c 77 cb b2 b2 59`	发送方 MAC 地址：`4c:77:cb:b2:b2:59`
SPA (4)	`a9 fe 65 f6`	发送方 IP 地址：`10.29.180.42`
THA (6)	`00 00 00 00 00 00`	接收方 MAC 地址（未知）
TPA (6)	`a9 fe 65 f6`	接收方 IP 地址：`10.29.180.42`

此时询问 `10.29.0.1` 的地址:

ARP Request:

字段 (字节数)	内容（16 进制）	解释
SHA (6)	`4c 77 cb b2 b2 59`	发送方 MAC 地址：`4c:77:cb:b2:b2:59`
SPA (4)	`a9 fe 65 f6`	发送方 IP 地址：`10.29.180.42`
THA (6)	`00 00 00 00 00 00`	接收方 MAC 地址（未知）
TPA (6)	`a9 1d 00 01`	接收方 IP 地址：`10.29.0.1`

最后，收到 `10.29.0.1` 的回复:

ARP Reply:

字段 (字节数)	内容（16 进制）	解释
SHA (6)	`10 4f 58 6c 0c 00`	发送方 MAC 地址：`10:4f:58:6c:0c:00`
SPA (4)	`a9 1d 00 01`	发送方 IP 地址：`10.29.0.1`
THA (6)	`4c 77 cb b2 b2 59`	接收方 MAC 地址：`4c:77:cb:b2:b2:59`
TPA (6)	`a9 1d 00 01`	接收方 IP 地址：`10.29.0.1`

2.4.3ARP 工作流程

ARP 协议（地址解析协议）是网络通信中用于将网络层的 IP 地址转换为数据链路层的 MAC 地址的关键协议。以下是 ARP 协议的基本工作流程：

1. **冲突检测**：
   - ARP Probe 和 ARP Announcement 用于检测 IP 地址冲突。ARP Probe 用于查询是否有其他设备使用了自己的 IP 地址，而 ARP Announcement 用于通知其他设备自己的 IP 地址。
2. **发起 ARP 请求**：
   - 当一个设备（例如，计算机 A）需要将数据包发送到另一个设备（例如，计算机 B），但只知道目标设备的 IP 地址时，它需要先获得目标设备的 MAC 地址。
   - 设备 A 会在本地 ARP 缓存中查找是否已经有 IP 地址到 MAC 地址的映射。如果找到了，直接使用这个映射发送数据。
   - 如果没有找到，设备 A 会构建一个 ARP Request 包，其中包含自己的 IP 地址和 MAC 地址，以及目标设备的 IP 地址。目标 MAC 地址字段填充为广播地址。
3. **广播 ARP 请求**：
   - 设备 A 将这个 ARP Request 包通过网络广播给同一局域网（LAN）上的所有设备。每个接收到请求的设备都会检查 ARP 包中的“目标 IP 地址”，以确定是否为自己的 IP 地址。
4. **接收和响应 ARP 请求**：
   - 如果一个设备（例如，计算机 B）发现 ARP 请求中的目标 IP 地址与自己的 IP 地址匹配，它将构建一个 ARP Reply 包。在这个响应包中，它会填充自己的 IP 地址和 MAC 地址，并将发送者的 IP 和 MAC 地址设置为原 ARP 请求中的值。
   - 然后计算机 B 将这个 ARP 响应包直接发送给原请求的发送者（计算机 A），而不是广播。
5. **更新 ARP 缓存**：
   - 一旦计算机 A 接收到来自计算机 B 的 ARP 响应，它将解析出 B 的 MAC 地址，并将这个 IP 地址到 MAC 地址的映射存储在本地 ARP 缓存中。这样，未来发送到同一 IP 地址的数据可以直接使用这个映射，无需再次发送 ARP 请求。
   - 这个映射通常会在 ARP 缓存中保留一段时间，然后过期删除，以应对网络配置的可能变更。
   - 这个功能通常通过 Gratuitous ARP 包来实现，即设备定期发送 ARP 响应包来更新网络中其他设备的 ARP 缓存。
6. **数据传输**：
   - 有了目标 MAC 地址后，计算机 A 可以将数据包封装在以太网帧中，并设置正确的目标 MAC 地址，通过物理网络发送给计算机 B。

这个过程确保了即使在只知道目标 IP 地址的情况下，数据也能被正确地发送到目标设备。ARP 协议是局域网通信中不可或缺的一部分，它使得 IP 层和 MAC 层的转换成为可能。

2.5 TCP 协议分析

第三章 实验结论和实验心得