计算机网络通信协议分析

58121124 张博彦

2023 年 5 月 25 日

1 ARP

1.1 生成并捕获 ARP 数据包

在 wireshark 软件中选择 WLAN 进行捕获，之后在管理员运行的 cmd 中输入 arp -d，然后使用过滤器选择 ARP 进行过滤，即可得到 ARP 的数据包。

实际实验操作结果如图 1

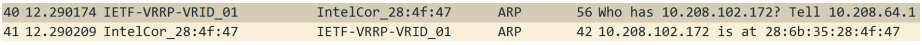


图 1: ARP 数据包捕获结果

1.2 ARP 数据包分析

1.2.1 ARP 请求数据包

1. 具体结构如图 2

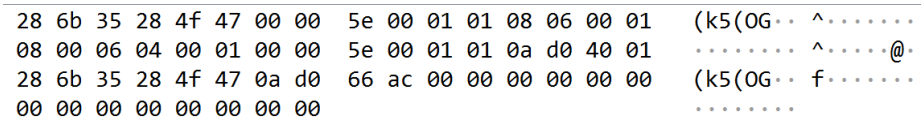


图 2: ARP 请求数据包结构

2. 字段及其含义

(a) 28 6b 35 28 4f 47 为目的地址

(b) 00 00 5e 00 01 01 为源 MAC 地址

(c) 08 06 为 ARP 协议

(d) 00 01 为以太网

(e) 08 00 为 ARP 的协议类型为 IPV4

(f) 06 为硬件地址位数

(g) 04 为协议地址位数

(h) 00 01 为 ARP 请求报文类型

(i) 00 00 5e 00 01 01 为源 MAC 地址

(j) 0a d0 40 01 为源 IP 地址

(k) 28 6b 35 28 4f 47 为目的 MAC

(l) 0a d0 66 ac 为目的 IP

(m) 00 00 00 00 00 00 00 00 00 00 00 00 00 00 为全 0 的 MAC 地址

1.2.2 ARP 应答数据包

1. 具体结构如图 3

```
00 00 5e 00 01 01 28 6b  35 28 4f 47 08 06 00 01   ··^···(k 5(OG····
08 00 06 04 00 02 28 6b  35 28 4f 47 0a d0 66 ac   ······(k 5(OG··f·
00 00 5e 00 01 01 0a d0  40 01                     ··^····· @·
```

图 3: ARP 应答数据包结构

2. 字段及其含义

(a) 00 00 5e 00 01 01 为目的地址

(b) 28 6b 35 28 4f 47 为源 MAC 地址

(c) 08 06 为 ARP 协议

(d) 00 01 为以太网

(e) 08 00 为 ARP 的协议类型为 IPV4

(f) 06 为硬件地址位数

(g) 04 为协议地址位数

(h) 00 02 为 ARP 应答报文类型

(i) 28 6b 35 28 4f 47 为源 MAC 地址

(j) 0a d0 66 ac 为源 IP 地址

(k) 00 00 5e 00 01 01 为目的 MAC

(l) 0a d0 40 01 为目的 IP

1.3 ARP 协议的工作流程

考虑两台主机 A 和 B，A 要向 B 发送信息

1. 当 A 和 B 在同一个网段，A 首先查看自己的 ARP 缓存表，确定其中是否包含有 B 对应的 ARP 表项。如果有对应的 MAC 地址，则 A 直接利用该地址，对 IP 数据包进行帧封装，并将数据包发送给 B。如果 A 在 ARP 表中没有对应的 MAC 地址，则将缓存该数据报文，然后以广播方式发送一个 ARP 请求报文。ARP 请求报文中的发送端 IP 地址和发送端 MAC 地址为 A 的 IP 地址和 MAC 地址，目标 IP 地址和目标 MAC 地址为 B 的 IP 地址和全 0 的 MAC 地址。而之后，B 会对该请求进行处理。B 比较自己的 IP 地址和 ARP 请求报文中的目标 IP 地址，当两者相同时进行如下处理：将 ARP 请求报文中 A 的 IP 地址和 MAC 地址存入自己的 ARP 表中。之后再发送 ARP 响应报文给 A，该报文包含 B 自己的 MAC 地址。A 收到 ARP 响应报文后，将 B 的 MAC 地址加入到自己的 ARP 表中，同时将 IP 数据包进行封装后发送出去。

2. 当 A 和 B 不在同一网段时，A 就会先向网关发出 ARP 请求，ARP 请求报文中的目标 IP 地址为网关的 IP 地址。当 A 从收到的响应报文中获得网关的 MAC 地址后，将报文封装并发给网关。如果网关没有 B 的 ARP 表项，网关会广播 ARP 请求，目标 IP 地址为 B 的 IP 地址，当网关从收到的响应报文中获得 B 的 MAC 地址后，就可以将报文发给 B；如果网关已经有 B 的 ARP 表项，网关直接把报文发给 B。

1.4 ARP 协议的功能

ARP 协议的功能是将 IP 地址解析为 MAC 地址，从而通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

2 ICMP

2.1 生成并捕获 ICMP 数据包

此处以百度为例，首先在 wireshark 软件中选择 WLAN 进行捕获，之后在 cmd 中输入 ping www.baidu.com，然后使用过滤器选择 ICMP 进行过滤，即可得到 ICMP 的数据包。

实际实验操作结果如图 4、5

图 4: cmd 输入结果

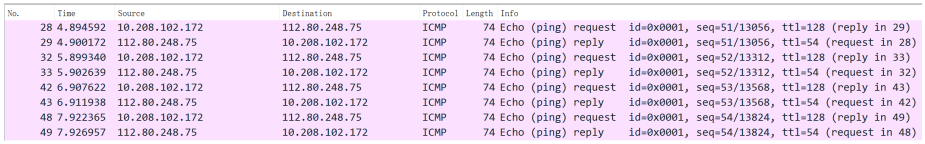


图 5: ICMP 数据包捕获结果

2.2 ICMP 数据包分析

1. 具体结构如图 6

```
00 00 5e 00 01 01 28 6b  35 28 4f 47 08 00 45 00
00 3c 05 75 00 00 80 01  00 00 0a d0 66 ac 70 50
f8 4b 08 00 4d 28 00 01  00 33 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67  68 69
```

图 6: ICMP 数据包结构

2. 字段及其含义

   (a) 00 00 5e 00 01 01 为目的 MAC 地址

   (b) 28 6b 35 28 4f 47 为源 MAC 地址

   (c) 08 00 为 ICMP 类型为 IPv4

   (d) 80 为该报文的生存时间

   (e) 01 为 ICMP 类型

   (f) 0a d0 66 ac 为源 IP 地址

   (g) 70 50 f8 4b 为目的 IP 地址

   (h) 08 为请求 ICMP 类型

   (i) 4d 28 为校验码

   (j) 00 01 为匹配请求的标识符

   (k) 00 33 为匹配请求的序列号

   (l) 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 为所要传递的数据

2.3 ICMP 的工作流程 (此处为使用 ping 命令)

1. 向目的服务器发送回显请求

2. 目的服务器发送回显应答

3. 源服务器显示相关数据

2.4 ICMP 的功能

1. 侦测远端主机是否存在
2. 确认 IP 包是否成功到达目标地址
3. 若不可达，则通知在发送过程中 IP 包被丢弃的原因
4. 建立及维护路由资料
5. 重导数据传送路径

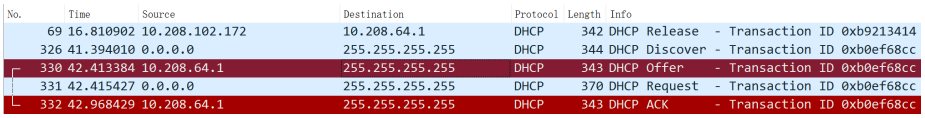
3 DHCP

3.1 生成并捕获 DHCP 数据包

首先在 wireshark 软件中选择 WLAN 进行捕获，之后在管理员运行的 cmd 中依次输入以下命令：

```
ipconfig /release
ipconfig /renew
```

然后使用过滤器选择 DHCP 进行过滤，即可得到 DHCP 的数据包。实际实验操作结果如图 7



No.	Time	Source	Destination	Protocol	Length	Info
69	16.810902	10.208.102.172	10.208.64.1	DHCP	342	DHCP Release - Transaction ID 0xb9213414
326	41.394010	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb0ef68cc
330	42.413384	10.208.64.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0xb0ef68cc
331	42.415427	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb0ef68cc
332	42.968429	10.208.64.1	255.255.255.255	DHCP	343	DHCP ACK - Transaction ID 0xb0ef68cc

图 7: DHCP 数据包捕获结果

3.2 DHCP 数据包分析 (以 DHCP 释放数据包为例)

1. 具体结构如图 8
2. 字段及其含义
   (a) 00 00 5e 00 01 01 为目的 MAC 地址
   (b) 28 6b 35 28 4f 47 为源 MAC 地址

```
00 00 5e 00 01 01 28 6b  35 28 4f 47 08 00 45 00
01 48 1c 57 00 00 80 11  00 00 0a d0 66 ac 0a d0
40 01 00 44 00 43 01 34  bd 92 01 01 06 00 b9 21
34 14 00 00 00 00 0a d0  66 ac 00 00 00 00 00 00
00 00 00 00 00 00 28 6b  35 28 4f 47 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 63 82  53 63 35 01 07 36 04 0a
d0 40 01 3d 07 01 28 6b  35 28 4f 47 ff 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00
```

图 8: DHCP 释放数据包结构

(c) 08 00 为 DHCP 类型为 IPv4

(d) 80 为生存时间

(e) 11 为 UDP 协议类型

(f) 0a d0 66 ac 为源 IP 地址

(g) 0a d0 40 01 为目的 IP 地址

(h) 01 为请求操作

(i) 0a d0 66 ac 为客户端 IP 地址

(j) 第五行至第十八行的 00 数据为服务器名称和启动文件名未给出

(k) 63 82 53 63 为确定之后的内容为选择字段 (optional field)

3.3 DHCP 的工作流程

DHCP 的工作流程分为 4 给阶段：

1. 发现阶段：DHCP 客户端以广播方式发送 DHCP Discover 报文。所有收到该报文的 DHCP 服务器发送回应报文，DHCP 客户端据此可以知道网络中存在的 DHCP 服务器的位置。

2. 提供阶段：接收到 DHCP Discover 报文的 DHCP 服务器，将从 IP 地址池中选择一个合适的 IP 地址，连同 IP 地址租约期限及其他配置信息，一同通过 DHCP Offer 报文发送给 DHCP 客户端。

3. 选择阶段：若有多台 DHCP 服务器向 DHCP 客户端回应 DHCP Offer 报文，则 DHCP 客户端只接受第一个收到的 DHCP Offer 报文。然后以广播方式发送 DHCP Request 请求报文，通知所有的 DHCP 服务器，将选择 Option 54 中标识的 DHCP 服务器提供的 IP 地址，其他 DHCP 服务器可以重新使用曾提供的 IP 地址。

4. 确认阶段：当 DHCP 服务器收到 DHCP 客户端发送的 DHCP Request 报文后，DHCP 服务器根据 DHCP Request 报文中携带的 MAC 地址来查找有没有相应的租约记录。

   (a) 若有，则发送 DHCP ACK 报文作为应答，通知 DHCP 客户端使用分配的 IP 地址。DHCP 客户端收到 DHCP 服务器返回的 DHCP ACK 报文后，会以广播的方式发送免费 ARP 报文，探测是否有主机使用服务器分配的 IP 地址，如果在规定的时间内没有收到回应，客户端才使用此地址。否则，客户端会发送 DHCP Decline 报文给 DHCP 服务器，通知 DHCP 服务器该地址不可用，并重新申请 IP 地址。

   (b) 若没有或因部分原因无法正常分配 IP 地址，则发送 DHCP NAK 报文作为应答，通知 DHCP 客户端无法分配合适 IP 地址。DHCP 客户端需要重新发送 DHCP Discover 报文请求新的 IP 地址。

3.4 DHCP 的功能

用于管理分配 IP 地址，为大量的主机分配 IP 地址并进行集中管理

4 DNS

4.1 生成并捕获 DHCP 数据包

在 wireshark 软件中选择 WLAN 进行捕获，然后使用过滤器选择 DNS 进行过滤，即可得到 DNS 的数据包。

实际实验操作结果如图 9

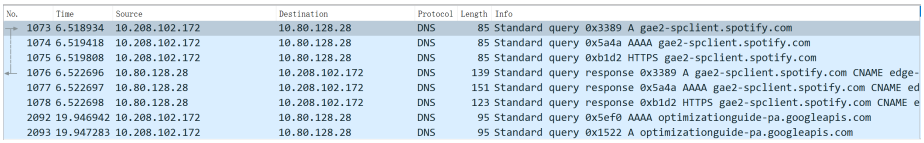


图 9: DNS 数据包捕获结果

4.2 DNS 数据包分析

1. 具体结构如图 10

```
00 00 5e 00 01 01 28 6b  35 28 4f 47 08 00 45 00
00 47 f1 27 00 00 80 11  00 00 0a d0 66 ac 0a 50
80 1c dd 09 00 35 00 33  fc 2c 33 89 01 00 00 01
00 00 00 00 00 00 0d 67  61 65 32 2d 73 70 63 6c
69 65 6e 74 07 73 70 6f  74 69 66 79 03 63 6f 6d
00 00 01 00 01
```

图 10: DNS 数据包结构

2. 字段及其含义

   (a) 00 00 5e 00 01 01 为目的 MAC 地址

   (b) 28 6b 35 28 4f 47 为源 MAC 地址

   (c) 08 00 为 DNS 类型为 IPv4

   (d) 80 为生存时间

   (e) 11 为 UDP 协议类型

   (f) 0a d0 66 ac 为源 IP 地址

(g) 0a d0 40 01 为目的 IP 地址

(h) dd 09 为源端口

(i) 00 35 为目的端口

(j) 00 01 为问题记录数为 1

(k) 00 00 为回答记录数

(l) 00 00 为授权记录数

(m) 00 00 为附加信息记录数

(n) 0d 67 至报文尾为问题查询内容

4.3 DNS 的工作流程

1. 客户机提出域名解析请求，并将该请求发送给本地的域名服务器。
2. 当本地的域名服务器收到请求后，查询本地的缓存
   (a) 若有该纪录项，则本地的域名服务返回查询的结果。
   (b) 若没有该记录项，则本地域名服务器将把请求发送至根域名服务器，之后根域名服务器再返回给本地域名服务器一个所查询域的主域名服务器的地址。本地服务器再向上一步返回的域名服务器发送请求，然后接受请求的服务器查询自己的缓存，若没有该纪录项，则返回相关的下级的域名服务器的地址。不断重复查询操作，直至找到正确的记录。本地域名服务器把返回的结果保存至缓存，以备下一次使用，同时还将结果返回给客户机。

4.4 DNS 的功能

通过主机名，将域名解析为 IP 地址，从而使用户无需记住 IP 数串便能方便的地访问互联网。

5 UDP、TCP

5.1 TCP 连接建立过程

1. 服务器进程先创建传输控制块 TCB，并处于监听状态，等待客户端的连接请求

2. 客户端创建传输控制块 TCB，并向服务器发出连接请求报文段

3. 服务器收到连接请求报文段后，如同意建立连接，则发送确认报文段

4. 客户端进程收到服务器的确认报文段后，立即回复确认报文段，并进入已建立连接状态

5. 服务器收到确认报文段之后，也进入已建立连接状态

5.2 生成并捕获 HTTP 数据包

在 wireshark 软件中选择 WLAN 进行捕获,然后使用过滤器选择 HTTP 进行过滤，即可得到 HTTP 的数据包。

实际实验操作结果如图 11

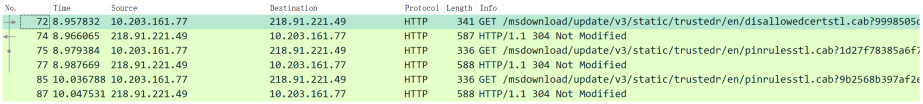


图 11: HTTP 数据包捕获结果

5.3 HTTP 数据包分析

1. 具体结构如图 12

2. 字段及其含义

   (a) 00 00 5e 00 01 01 为目的 MAC 地址

   (b) 28 6b 35 28 4f 47 为源 MAC 地址

   (c) 08 00 为 HTTP 类型为 IPv4

   (d) 80 为生存时间

   (e) 06 为 TCP 协议类型

   (f) 0a d0 66 ac 为源 IP 地址

   (g) 0a d0 40 01 为目的 IP 地址

   (h) e2 4b 为源端口

   (i) 00 50 为目的端口

```
00 00 5e 00 01 65 28 6b  35 28 4f 47 08 00 45 00
01 47 2b ff 40 00 80 06  00 00 0a cb a1 4d da 5b
dd 31 e2 4b 00 50 10 47  8d 1c d6 45 25 b9 50 18
02 01 64 df 00 00 47 45  54 20 2f 6d 73 64 6f 77
6e 6c 6f 61 64 2f 75 70  64 61 74 65 2f 76 33 2f
73 74 61 74 69 63 2f 74  72 75 73 74 65 64 72 2f
65 6e 2f 64 69 73 61 6c  6c 6f 77 65 64 63 65 72
74 73 74 6c 2e 63 61 62  3f 39 39 39 38 35 30 35
64 65 35 31 32 35 39 34  66 20 48 54 54 50 2f 31
2e 31 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20
4b 65 65 70 2d 41 6c 69  76 65 0d 0a 41 63 63 65
70 74 3a 20 2a 2f 2a 0d  0a 49 66 2d 4d 6f 64 69
66 69 65 64 2d 53 69 6e  63 65 3a 20 54 75 65 2c
20 31 36 20 4d 61 72 20  32 30 32 31 20 30 37 3a
33 33 3a 34 32 20 47 4d  54 0d 0a 49 66 2d 4e 6f
6e 65 2d 4d 61 74 63 68  3a 20 22 30 38 66 35 61
62 30 33 36 31 61 64 37  31 3a 30 22 0d 0a 55 73
65 72 2d 41 67 65 6e 74  3a 20 4d 69 63 72 6f 73
6f 66 74 2d 43 72 79 70  74 6f 41 50 49 2f 31 30
2e 30 0d 0a 48 6f 73 74  3a 20 63 74 6c 64 6c 2e
77 69 6e 64 6f 77 73 75  70 64 61 74 65 2e 63 6f
6d 0d 0a 0d 0a
```

图 12: HTTP 数据包结构

(j) 第四行 47 至第十行 0a 为请求方式为 GET

(k) 第十行 43 至第十一行为 0a 为客户端与服务端指定的请求

(l) 第十七行 55 至第二十行 0a 为发送请求的操作系统及浏览器信息

(m) 第二十行 48 至第 22 行 0a 为请求的主机名

5.4 HTTP 网页内容获得方式

1. 一般情况下为逐条获取。当访问网页时，浏览器会向服务器发送 HTTP 请求，并按照请求的顺序逐条获取网页中的资源，如 HTML 文件、CSS 样式表、JavaScript 代码和图像等。这些资源通常被分成多个请求，浏

览器会逐个请求并加载这些资源，然后将它们组合在一起以呈现完整的网页。

2. 少数情况下使用成批获取，从而在部分场景下获得更好的性能和加载速度。

5.5 基于用户代理的服务和 web 邮件服务的区别

1. 功能和目的方面：基于用户代理的服务是一种代理服务器的应用，其主要目的是为了改善网络连接和性能，提供缓存、安全性、过滤和其他增强功能。它通常用于代理 HTTP 请求和响应，以提供更好的网络体验。Web 邮件服务则专注于电子邮件的管理和传输，使用户能够通过 Web 界面发送、接收和管理电子邮件。

2. 协议方面：基于用户代理的服务主要基于 HTTP 协议，因为它通常用于代理 HTTP 请求和响应。Web 邮件服务则使用专门的电子邮件协议。

3. 功能范围方面：基于用户代理的服务可以提供多种功能，如缓存、内容过滤等，还可以通过代理服务器减少带宽消耗，提高响应时间，并提供安全性和隐私保护。Web 邮件服务则专注于电子邮件的功能，如发送、接收、组织邮件等。

4. 用户界面方面：基于用户代理的服务通常没有用户可见的界面，因为它是在网络层次上工作的。它可能会对网络连接进行透明的优化和增强，而用户不需要直接与它进行交互。Web 邮件服务则提供一个 Web 界面，使用户可以直接通过浏览器访问和管理电子邮件。