DHCP

一 实验目的

1. 掌握 DHCP 协议的作用。
2. 了解 DHCP 报文的格式。
3. 了解 DHCP 的工作原理。

二 预备知识

1. DHCP 简介

DHCP(Dynamic Host Configuration Protocol)，动态主机配置协议，是一个应用层协议。当我们将客户主机 ip 地址设置为动态获取方式时，DHCP 服务器就会根据 DHCP 协议给客户端分配 IP，使得客户机能够利用这个 IP 上网。DHCP 的前身是 BOOTP 协议(Bootstrap Protocol)，后来被 DHCP 取代了，DHCP 比 BOOTP 更加复杂，功能更强大。在用 Wireshark 过滤显示 DHCP 包，需要输入过滤条件 BOOTP，而不是 DHCP。DHCP 报文种类及功能如表 1 所示。

表 1 DHCP 报文种类

报文类型	主要功能
DHCP-DISCOVER	客户端广播发送，用来查找网络中可用的 DHCP 服务器
DHCP-OFFER	服务器用来响应客户端的 DHCP-DISCOVER 请求，并为客户端指定相应配置参数
DHCP-REQUEST	客户端广播发送 DHCP 服务器，用来请求配置参数或者续借租用
DHCP-ACK	服务器通知客户端可以使用分配的 IP 地址和配置参数
DHCP-NAK	服务器通知客户端地址请求不正确或者租期已过期，续租失败
DHCP-RELEASE	客户端主动向 DHCP 服务器发送，告知服务器该客户端不再需要分配的 IP 地址
DHCP-DECLINE	客户端发现地址冲突或者由于其它原因导致地址不能使用，则发送 DHCP-DECLINE 报文，通知服务器所分配的 IP 地址不可用
DHCP-INFORM	客户端已有 IP 地址，用它来向服务器请求其它配置参数

2. DHCP 报文格式

DHCP 报文格式如图 1 所示，部分字段含义如下：

字段	含义
OP	表示报文的类型：1 表示请求报文；2 表示响应报文
htype	表示硬件地址的类型。对于以太网，该类型的值为“1”。
xid	事务 ID，由客户端选择的一个随机数，被服务器和客户端用来在它们之间交流请求和响应，客户端用它对请求和应答进行匹配。该 ID 由客户端设置并由服务器返回，为 32 位整数。
Options	选项字段，格式为"代码+长度+数据"。DHCP 通过此字段包含了服务器分配给终端的配置信息，如网关 IP 地址，DNS 服务器的 IP 地址，客户端可以使用 IP 地址的有效租期等信息。

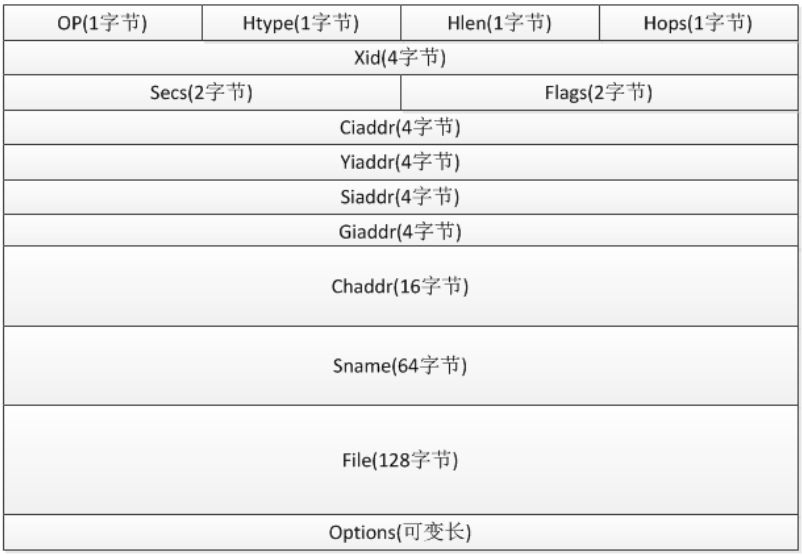


图 1 DHCP 报文格式

3. Options 常用字段

表 2 Options

代码	长度(字节)	说明
1	4	子网掩码
3	N*4	默认网关（可以是一个路由器 IP 地址列表）
6	N*4	DNS 服务器（可以是一个 DNS 服务器 IP 地址列表）
15	可变	域名称（主 DNS 服务器名称）
44	N*4	WINS 服务器（可以是一个 WINS 服务器 IP 列表）
51	4	有效租约期（以秒为单位）
53	1	报文类型
58	4	续约时间

三 实验环境

本实验可以在自己的电脑(需要联网)上进行，设备环境如下：

1. Windows 操作系统
2. 安装有 Wireshark 抓包工具
3. 开启 DHCP 服务

默认情况下，Windows 系统的 DHCP 服务是默认开启的，如果你之前已将自己设备的 IP 地址设置为了静态 IP，请暂时更改回自动获取 IP 后再进行实验。如果打开 Wireshark 后显示找不到网卡接口的提示信息，解决方法为：管理员身份运行命令提示符，执行命令 net start npf 之后重新打开 wires hark 即可。本实验中所用设备的原始 IP 地址为 192.168.1.160 。

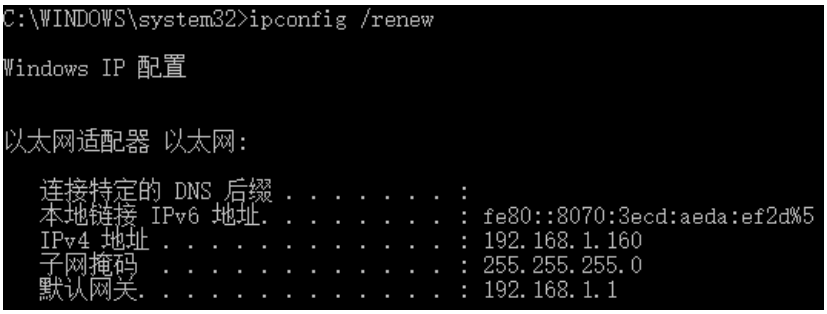
四 实验内容

1. 抓包

打开 wires hark，过滤栏中输入 **bootp** 过滤 DHCP 数据包，点击开始进行抓包。

打开命令提示符，输入 **ipconfig /release** 释放当前 IP 地址（执行后会断网）：

继续输入 **ipconfig /renew** 重新获取 IP 地址，主机成功连入网络：



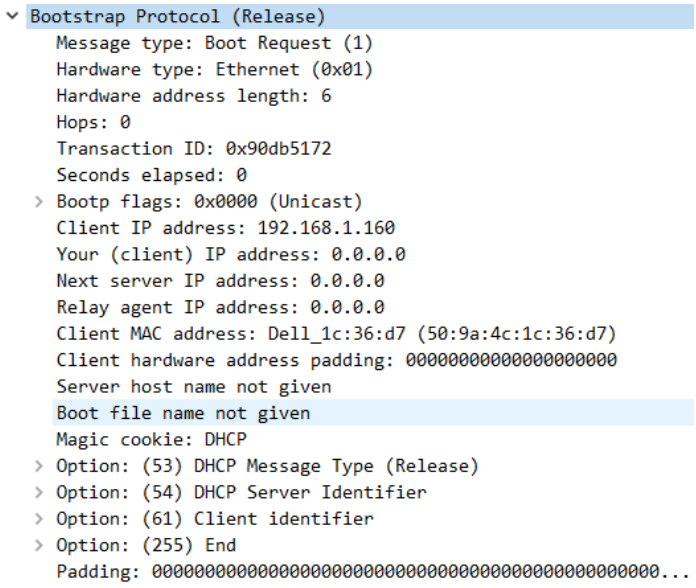
抓获的 DHCP 数据包:

No.	Time	Source	Destination	Protocol	Length	Info
27178	420.995559	192.168.1.160	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x90db5172
28368	650.068695	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5ccbe4f1
28369	650.069340	192.168.1.1	192.168.1.160	DHCP	342	DHCP Offer - Transaction ID 0x5ccbe4f1
28370	650.069601	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x5ccbe4f1
28371	650.070469	192.168.1.1	192.168.1.160	DHCP	350	DHCP ACK - Transaction ID 0x5ccbe4f1

2. 流程分析

(1) DHCP Release

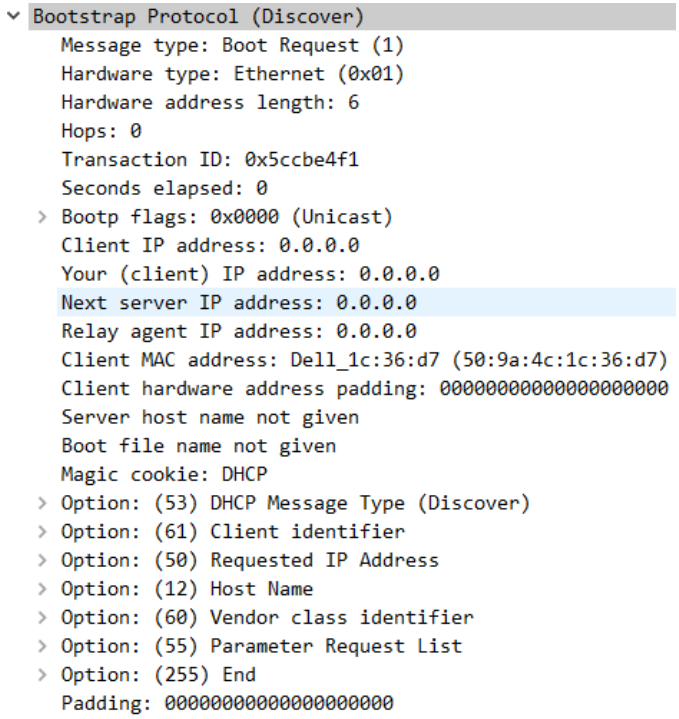
当执行 ipconfig /release 命令时，客户端主动向 DHCP 服务器发送一条 DHCP Release 报文，告知服务器该客户端不再需要分配的 IP 地址。



DHCP Release(No=27178)

(2) DHCP Discover

当一台没有 IP 地址的计算机申请 IP 地址时将发送该报文。DHCP Discovery 报文被发送给特殊的广播地址：255.255.255.255，该地址将到达某个限定广播范围内所有在线的主机。理论上，255.255.255.255 能够广播到整个因特网上，但实际上并不能实现，因为路由器为了阻止大量的请求淹没因特网，不会将这样的广播发送到本地网之外。



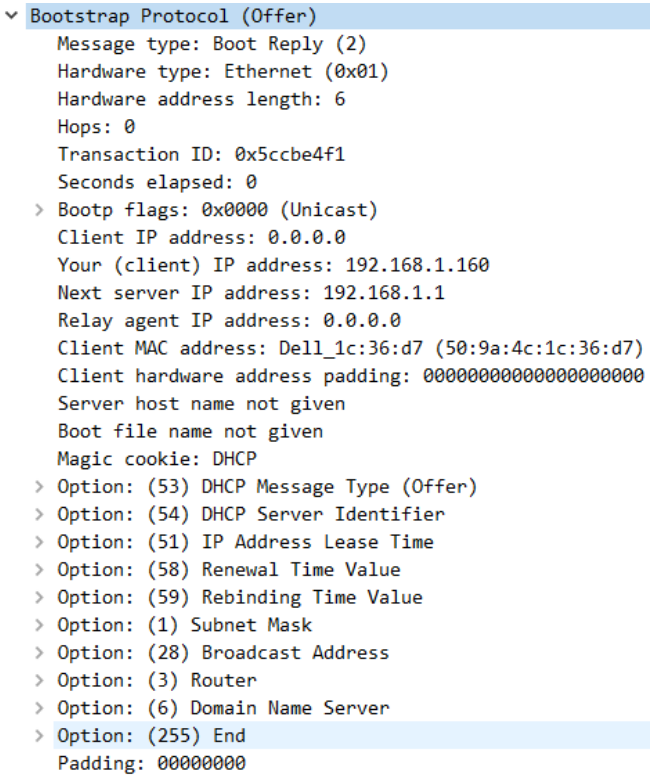
DHCP Discover(No=28368)

在 DHCP Discover 报文中，客户端包括了自身的信息。特别是，它提供了自己的主机名和其以太网接口的物理地址。这些信息可以被 DHCP 服务器用来标识一个已知的客户端。DHCP 服务器可以使用这些信息实现一系列的策略，比如，分配与上次相同的 IP 地址，分配一个与上次不同的 IP 地址，或要求客户端注册其物理层地址来获取 IP 地址。

此外，客户端还详细列出了它希望从 DHCP 服务器接收到的信息。在 **Option** 字段中的 **Parameter Request List** 包含了除客户端希望得到的本地网络的 IP 地址之外的其他数据项。这些数据项中许多都是一台即将连入因特网的计算机所需要的数据。例如，客户端必须知道的本地路由器的标识。任何目的地址不在本地网的数据报都将发送到这台路由器上。也就是说，这是发向外网的数据报在通向目的端的路径上遇到的第一台中间路由器。

(3) DHCP Offer

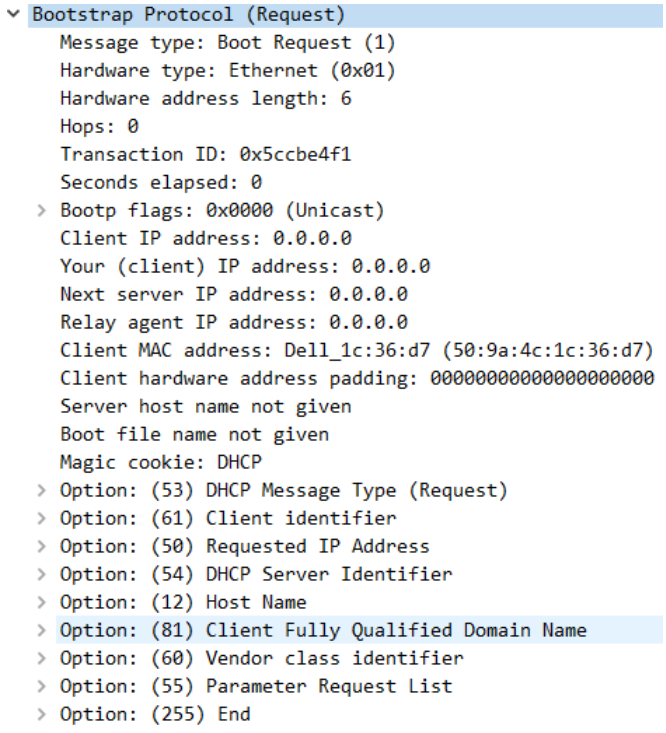
IP 地址为 192.168.1.1 的 DHCP 服务器收到 DHCP Discover 报文后，向客户端发送了一个 Offer 报文，其中 **Your(Client) IP Address** 字段提供了一个可用的 IP，除此之外，Option 字段还发送了子网掩码、路由器、DNS、域名、IP 地址租用期等信息。注意此时 DHCP 服务器知识告诉客户端自己本身可以提供服务，并没有开始 IP 地址的分配。



DHCP Offer(No=28369)

(4) DHCP Request

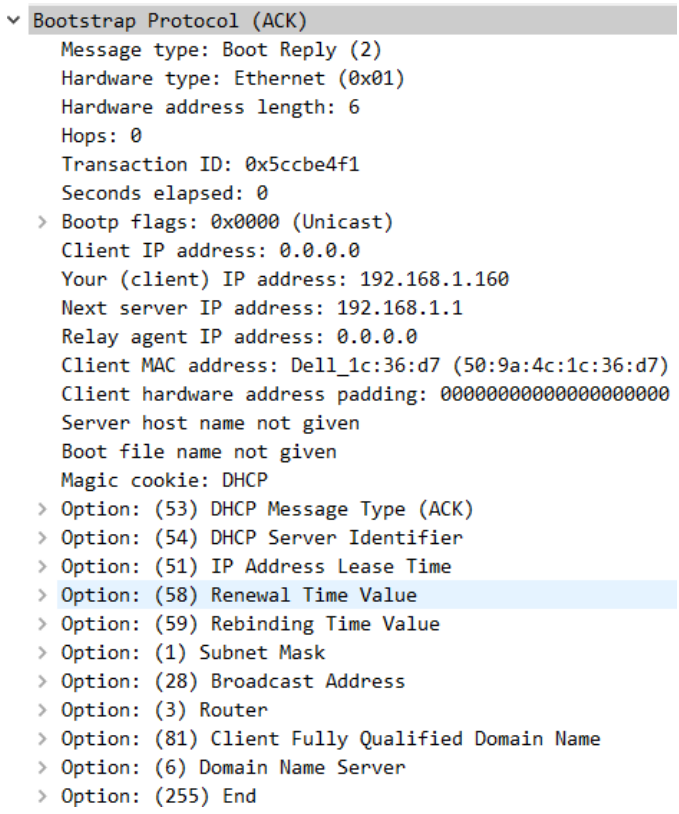
当 Client 收到了 DHCP Offer 包以后（如果有多个可用的 DHCP 服务器，那么可能会收到多个 DHCP Offer 包），确认有可以和它交互的 DHCP 服务器存在，于是 Client 发送 Request 数据包，请求分配 IP。该报文依然通过广播发送。



DHCP Request(No=28370)

(5) DHCP ACK

DHCP 服务器通过 DHCP ACK 对 DHCP Request 进行响应。



DHCP ACK(No=28371)

数据包中的 Your(client) IP address 表示将该 IP 地址分配给客户端使用，option 选项中的前两项给出了 DHCP 服务器发送的消息类型(ACK)和服务器的身份标识，同时还给出了客户端分配到的 IP 的子网掩码、默认网关、DNS 服务器等等信息。

3. 思考

根据以上实验内容完成以下问题：

1. 客户端执行 ipconfig /release 命令后，ip 地址变为什么？
2. DHCP 所使用的传输层协议是？使用的端口号是？
3. 客户端通过 DHCP 申请到的动态 IP 的租期是多长？
4. 客户端在申请动态 IP 的过程中，其早期的 IP 地址 192.168.1.160 已经被客户端释放，而 Offer 报文和 ACK 报文却可以使用该 ip 地址通过单播通讯直接向客户端发送报文而不是使用广播，试分析原因。
5. 在以上实验的基础上，再次执行 ipconfig /renew 命令会发生什么？