DHCP

DHCP 服务概述

1. 给内部网络自动分配 IP 地址，主机名，DNS 服务器，域名
2. 约束特定的计算机使用特定的 IP 地址（MAC/IP 绑定）

DHCP 服务运行原理

1．DHCP 客户端发现阶段（discover）

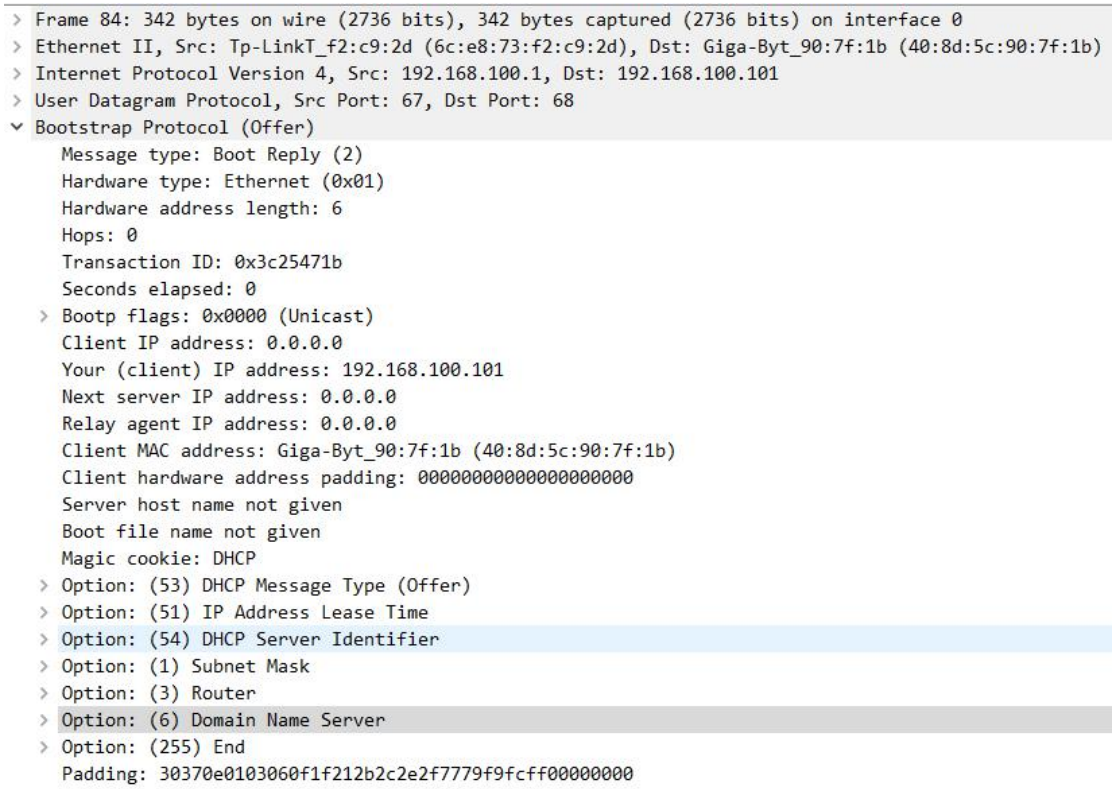
客户端广播一个 discover 报文，Discovery 报文是广播包，源地址为 0.0.0.0 目的地址为 255.255.255.255。只有 DHCP server 才会对 discover 报文做出响应。

```
> Frame 71: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Giga-Byt_90:7f:1b (40:8d:5c:90:7f:1b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3c25471b
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Giga-Byt_90:7f:1b (40:8d:5c:90:7f:1b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 00000000
```

2．DHCP 服务提供阶段（offer）

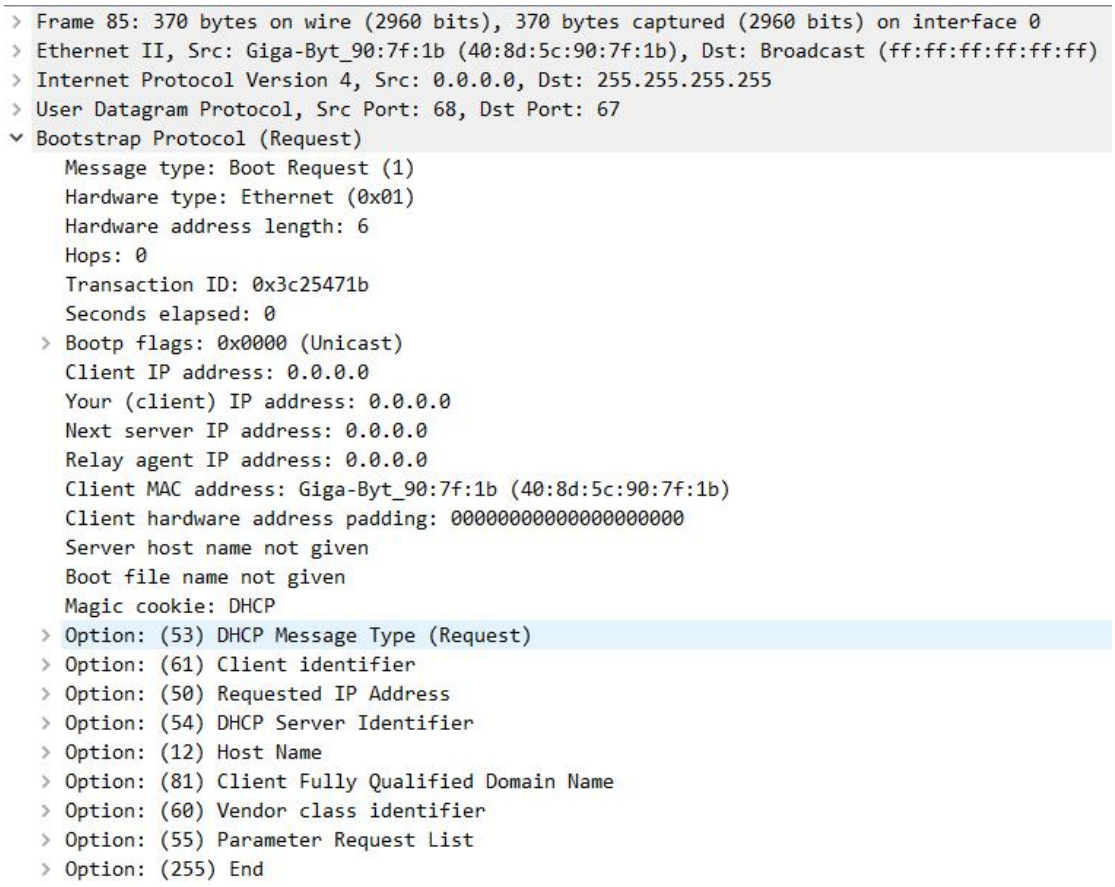
DHCP Server 提供阶段，即为 DHCP Server 响应 DHCP Discovery 所发的 DHCP Offer 阶段，即 DHCP 服务器提供 IP 地址的阶段。在网络中接收到 DHCP discover 信息的 DHCP 服务器都

会做出响应，它从尚未出租的 IP 地址中挑选一个分配给 DHCP 客户机，向 DHCP 客户机发送一个包含出租的 IP 地址和其他设置的 DHCP offer 提供信息（此过程可单播，也可以广播。主要保证发出的信息客户端能正常接收就行，mercku 使用的是单播）



3．DHCP 客户端确认阶段（request）

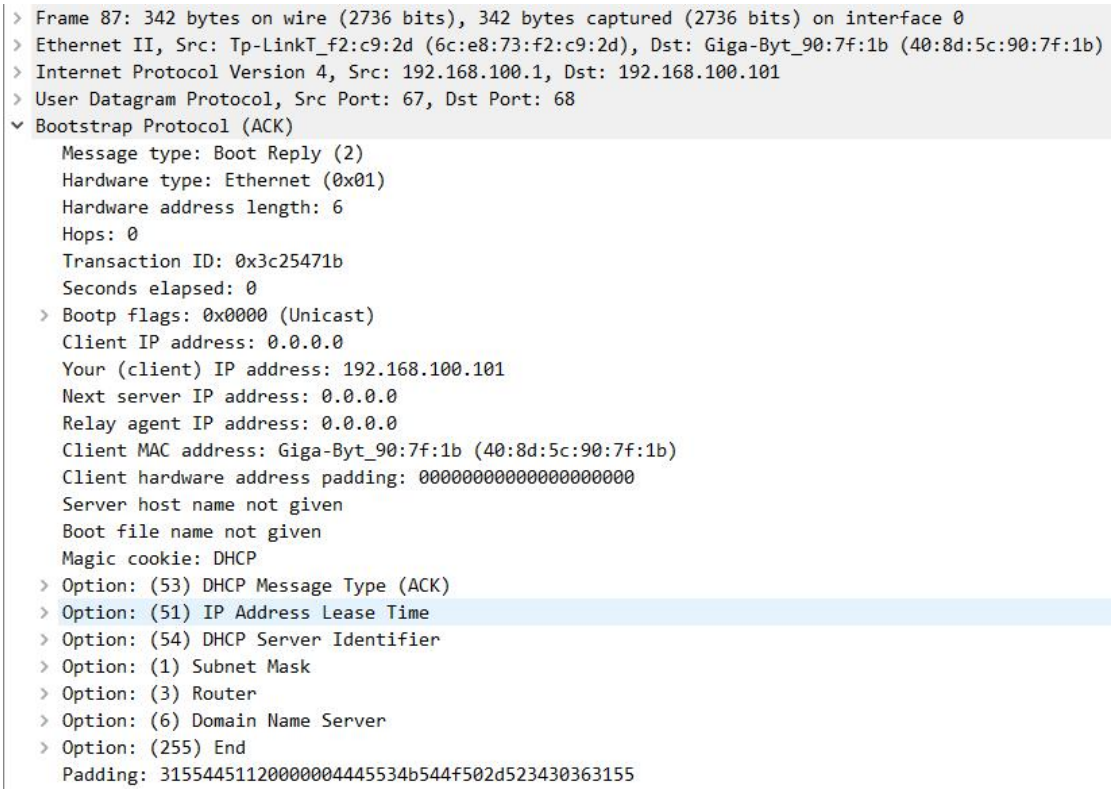
如果客户端收到了多个 DHCP 服务端发出的 offer 报文，客户端只会接受第一个达到的 offer 提供信息，然后它就以广播方式回答一个 DHCP request 请求信息，该信息中包含向它所选定的 DHCP 服务器请求 IP 地址的内容。之所以要以广播方式回答，是为了通知所有的 DHCP 服务器，他将选择某台 DHCP 服务器所提供的 IP 地址



4. DHCP 服务确认阶段（ACK）

当 DHCP 服务器收到 DHCP 客户机回答的 DHCP request 请求信息之后，它便向 DHCP 客户机发送一个包含它所提供的 IP 地址和其他设置的 DHC Pack 确认信息，告诉 DHCP 客户机可以使用它所提供的 IP 地址。然后 DHCP 客户机便将其 TCP/IP 协议与网卡绑定，另外，除 DHCP 客户机选中的服务器外，其他的 DHCP 服务器都将收回曾提供的 IP 地址（广播方式同

offer 阶段）



5．DHCP 客户端重新登录网络

客户端之前从服务端获取到过 IP 地址，将执行此操作。客户端重新登录不会再发送 discover 报文，而是直接发送包含前一次所分配的 IP 地址的 DHCP request 请求信息。如果次 IP 任然可用，服务端则返回 ack 报文，如果 IP 无法使用，服务端则返回 nak 报文。客户端收到 nak 报文后就必须重新发送 discover 报文

注：当客户端从一个 DHCP 服务器到另一个服务器时，就会收到 NAK 报文。如电脑拔掉网线，接入到另一台 DHCP 服务器上

6．DHCP 客户端更新租约

DHCP 服务获取的 IP 地址都有一个租约时间，租约过期后服务端将会收回该 IP 地址。续租方式，当租约时间过去一半客户端都会发送 renew 报文来续租（如果没有续租成功，服务端任然会保留该 IP 地址，在后期还会继续接受客户端发送的 renew 报文）。简单说就是到了续租时间，客户端将重新发送 request 报文，等待服务端的 ACK 报文的确认（发送 request 请求的时间分别为 1/2，7/8 的租约时间）

7．报文参数解析

（1）字段分析

Type：1 为请求，2 为回复

Ciddr：获取 IP 是都为 0.0.0.0，续租或者重新 renew 时，此处为客户端想继续使用的 IP

Yiaddr：服务端分配给路由器的 IP 地址

Options:可选参数域，格式为"代码+长度+数据"（一般为网关，DNS 服务器地址，DNS 域名，子网掩码之类的）

（2）常用 options 解析

1-子网掩码
3-网关
6-DNS 服务器地址
15-域名
51-租约时间（总共的时间）
53-DHCP 报文类型
54-DHCP 服务器地址
58-租约时间（租约时间的一半）
59-租约时间（租约时间的 7/8）

8．DHCP 配置文件参数说明

配置文件说明：

作用域：可以分配 IP 的范围 subnet
地址池：可以分配给客户端的 IP，range 包括的 IP
保留地址：指定某个客户端使用一个特定 IP，通过 host 配置的
租约(时间)：客户端可以使用这个 IP 地址的时间

注：DHCP 服务安装完成会自动生成 DHCP 配置文件，配置文件中一般包含了 IP 地址池，子网掩码，网关，域名，DNS 服务器地址，IP 地址租约时间

续租数据库文件

租约数据库文件用于保存一系列的租约声明，其中包含客户端的主机名、MAC 地址、分配到的 IP 地址，以及 IP 地址的有效期等相关信息

9．MAC/IP 绑定

基本原理：在 DHCP 服务中插入一条对应的 mac 和 IP，在 DHCP 客户端获取 DHCP 服务端的 IP 地址时，优先匹配绑定的关系。