9.1.2 DHCP 续租过程

DHCP 的主要任务就是在续租过程中向客户端分配 IP 地址。续租过程在一个客户端和 DHCP 服务器之间进行，如文件 dhcp_nolease_renewal.pcap 中所示。DHCP 的续租过程通常被称为 DORA 过程，因为它使用了 4 种类型的 DHCP 数据包：发现（Discover）、提供（Offer）、请求（Request）和确认（Acknowledgement），如图 9-2 所示。在这里，我们将对 DORA 数据包的每种类型进行逐一介绍。

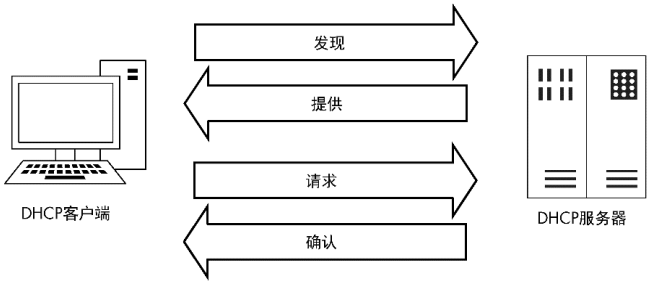

图 9-2　DHCP 的 DORA 过程

1．发现数据包

正如在引用的捕获文件中看到的那样，第一个数据包从 0.0.0.0 的 68 端口发往 255.255.255.255 的 67 端口。客户端使用 0.0.0.0，是因为它目前还没有 IP 地址。数据包被发往 255.255.255.255，是因为这是一个独立于网络的广播地址，从而确保这个数据包会被发往网络上的每台设备。因为这台设备并不知道 DHCP 服务器的地址，所以它的第一个数据包是为了寻找正在监听的 DHCP 服务器。

在 Packet Details 面板中，我们第一眼就可以看到 DHCP 是基于 UDP 作为传输层协议的。DHCP 对于客户端得到其所请求信息的速度有很高的要求。由于 DHCP 有其内置的保证可靠性的方法，因此也就意味着 UDP 是比较适合的协议。你可以在第一个数据包的 Packet Details 面板的 DHCP 部分，查看发现过程的细节，如图 9-3 所示。

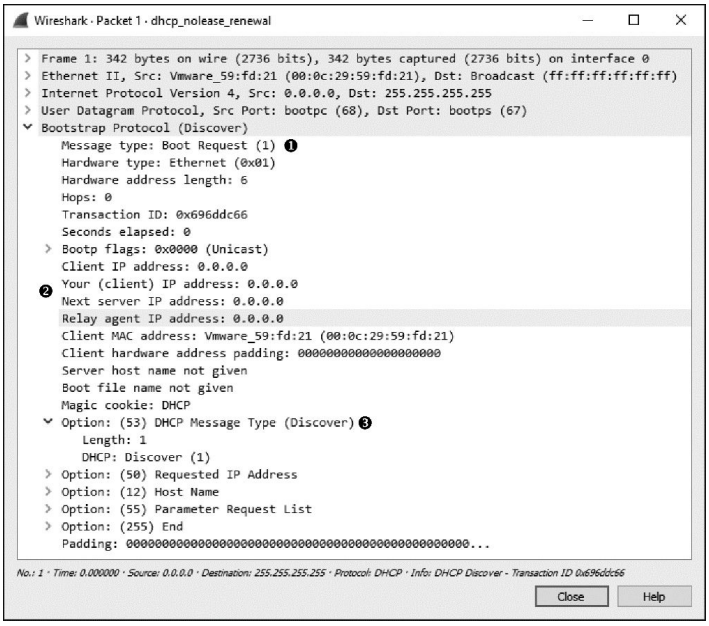

图 9-3　DHCP 发现数据包

> 注意
>
> 由于 Wireshark 在处理 DHCP 时，仍然会引用 BOOTP，因此你会在 Packets Detail 面板中看到 BOOTP 协议，而不是 DHCP。但无论如何，我在这本书中仍会将其叫作数据包的 DHCP 部分。

这是一个请求数据包，在消息类型域中标识为 1。发现数据包中的大多数字段或者为空（就像是 IP 地址域）；或者根据上一节所列出的 DHCP 字段，就已经解释的很清楚了。这个数据包的主要内容是这 4 个字段。

DHCP 消息类型：这里的选项类型为 53（t=53），长度为 1，它的值为 1。这些值表明这是一个 DHCP 发现数据包。

客户端标识符：这里提供了客户端请求 IP 地址的额外信息。

所请求 IP 地址：这里提供了客户端希望得到的 IP 地址（通常是之前用过的 IP 地址）。

请求参数列表：这里列出了客户端希望从 DHCP 服务器接收到的不同配置项（其他重要网络设备的 IP 地址）。

2．提供数据包

这个文件的第二个数据包在 IP 头中列出了可用的 IP 地址，显示这个数据包从 192.168.0.1 发往 192.168.0.10，如图 9-4 所示。因为客户端实际上还没有 192.168.0.10 这个地址，所以服务器会首先尝试使用由 ARP 提供的客户端硬件地址与之通信。如果通信失败，那么它将会直接将提供（Offer）广播出去，进行通信。

第二个数据包的 DHCP 部分，称为提供数据包，表明这是一个响应的消息类型。这个数据包包含了和前一个数据包相同的事务 ID，也就是告诉我们这个响应与我们原先的请求相对应。

该提供数据包由 DHCP 服务器发出，用以向客户端提供其服务。它提供了关于其自身的信息，以及它想要给客户端提供的地址。图 9-4 中，在「你的」（客户端）IP 地址字段中的 IP 地址 192.168.0.10 就是要提供给客户端的。下一个服务器 IP 地址（Next Server IP Address）域中的值 192.168.0.1 表明我们的 DHCP 服务器与默认网关共享一个 IP 地址。

列出的第一个选项指明这个数据包是一台 DHCP 服务器提供的。服务器所提供的接下来的这些选项和客户端的 IP 地址，一起给出了它所能提供的额外信息。你可以看到它给出了如下信息。

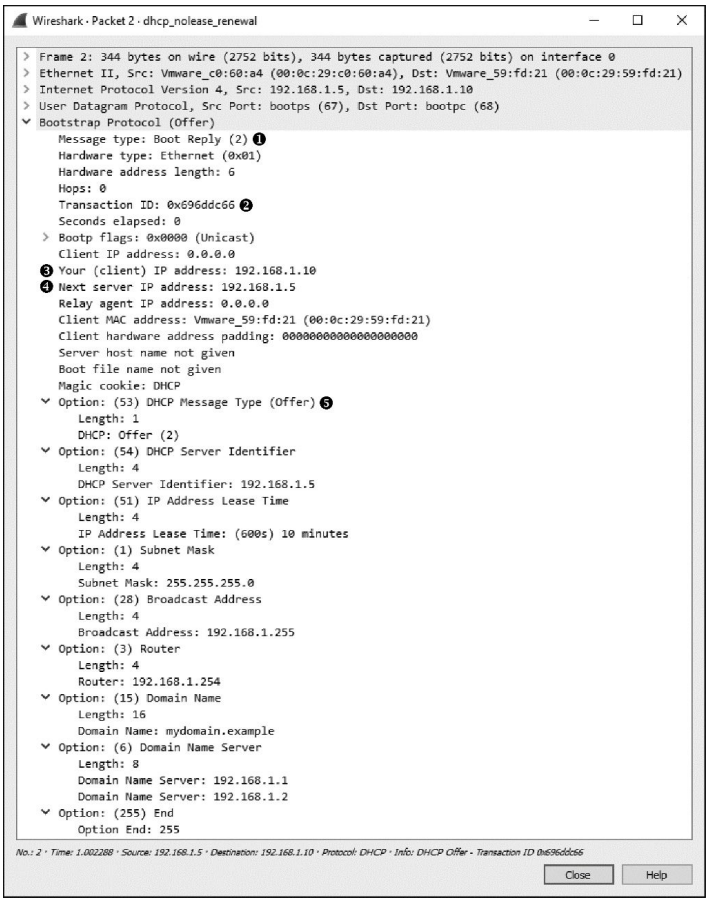

图 9-4　DHCP 提供数据包

- 子网掩码是 255.255.255.0。
- 续租时间是 30min。
- 重新绑定时间的值是 52min30s。
- IP 地址的租期是 1h。
- DHCP 服务器的标识符是 192.168.0.1。

3．请求数据包

在客户端接收到 DHCP 服务器的提供数据包之后，它将以一个 DHCP 请求数据包作为接收确认，如图 9-5 所示。

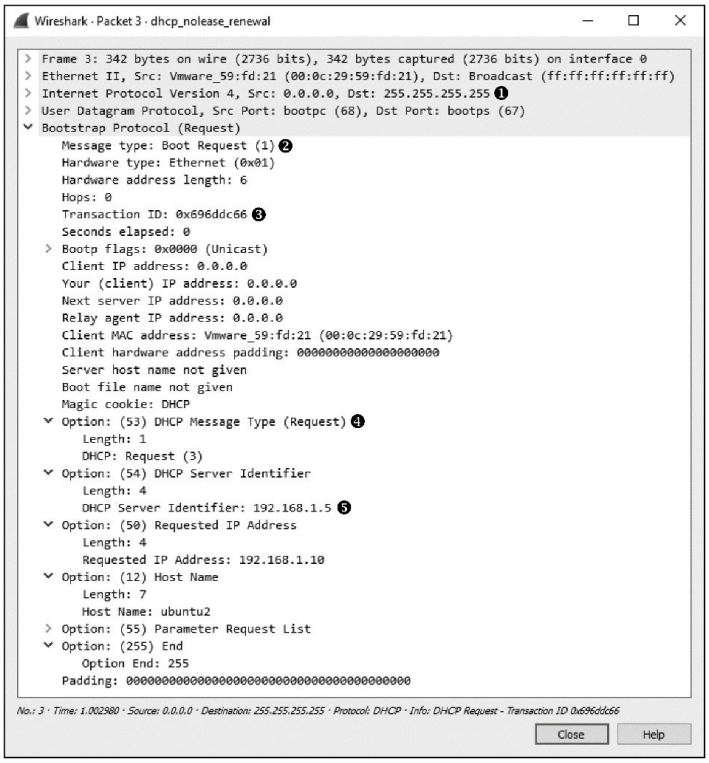

图 9-5　DHCP 请求数据包

这个捕获文件中的第三个数据包仍然从 IP 地址 0.0.0.0 处发出，因为我们还没有完成获取 IP 地址的过程。但数据包现在知道了它所要通信的 DHCP 服务器。

消息类型字段显示这是一个请求数据包。虽然这个捕获文件上的每个数据包都属于同一个续租过程，但因为这是一个新的请求/响应过程，所以它有了一个新的事务 ID。这个数据包与发现数据包相似，其所有的 IP 地址信息都是空的。

在最后的选项域，我们看到这是一个 DHCP 请求。值得注意的是，这个所要请求的 IP 地址不再是空，并且 DHCP 服务器标识符域也填有 IP 地址。

4．确认数据包

这个过程的最后一步就是 DHCP 在确认数据包中给客户端发送其所请求的 IP 地址，并在其数据库中记录相关信息，如图 9-6 所示。

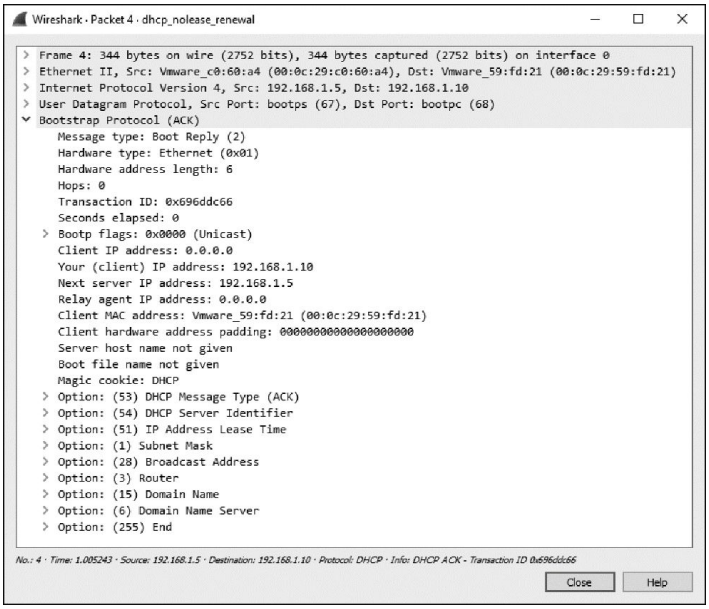

图 9-6　DHCP 确认数据包

这时客户端就有了一个 IP 地址，并且可以用它在网络上通信。