10.3.1 网关配置问题

第一个问题的场景相当简单：用户不能访问 Internet。我们已经确认该用户可以访问所有内网资源，包括其他工作站的共享内容以及运行在本地服务器上的应用程序。

这个网络架构非常简单，因为所有客户机和服务器都连接到一系列的简单交换机上。Internet 连接由一个路由器（作为默认网关）处理，IP 地址信息由 DHCP 服务提供。这种情景在小型办公室中非常常见。

1．侦听线路

为了找出问题的原因，我们可以一边用嗅探器监听线路，一边让用户尝试浏览 Internet。我们使用 2.5 节中的信息（见图 2-15），来决定放置嗅探器的方法。

网络上的交换机不支持端口镜像。为了完成测试，我们已经不可避免地妨碍了用户，所以我们假设可以使他再次下线（这是说，使用网络分流器是监听线路的推荐办法）。最后得到捕获记录文件 nowebaccess1.pcap。

2．分析

如图 10-13 所示，流量捕获记录文件以一个 ARP 请求和响应开始。用户计算机的 MAC 地址是 00:05:b3:bf:91:ee，IP 地址是 172.16.0.8。在数据包 1 中，用户的计算机发送一个 ARP 广播数据包给网络上的所有计算机，试图得到默认网关 172.16.0.10 的 MAC 地址。

No.	Time	Source	Destination	Protocol	Length	Info
1	04:32:21.445645	00:25:b3:bf:91:ee	ff:ff:ff:ff:ff:ff	ARP	42	Who has 172.16.0.10? Tell 172.16.0.8
2	04:32:21.445735	00:24:81:a1:f6:79	00:25:b3:bf:91:ee	ARP	60	172.16.0.10 is at 00:24:81:a1:f6:79

图 10-13　针对计算机默认网关的 ARP 请求和响应

根据数据包 2 中收到的响应，用户的计算机了解到 172.16.0.10 的 MAC 地址是 00:24:81:a1:f6:79。收到这个响应后，计算机就有了到达网关的路由，而网关应该可以带它接入 Internet。

ARP 响应之后，计算机会在数据包 3 中请求将网站的域名解析成 IP 地址。如图 10-14 所示，计算机发送一个 DNS 查询数据包到它的首选 DNS 服务器 4.2.2.2❶。

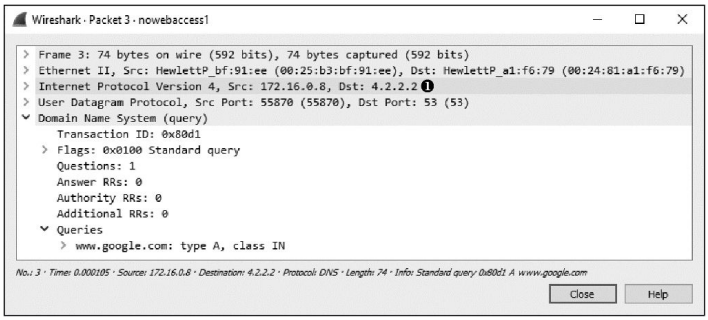

图 10-14　发送到 4.2.2.2 的 DNS 查询

正常情况下，DNS 服务器会迅速响应 DNS 查询，但在这个例子中并非如此。我们没有看到任何响应，却发现同样的 DNS 查询再次发送到不同的目的地址。如图 10-15 所示，在数据包 4 中，第二个 DNS 查询被发送到预先配置好的备用 DNS 服务器 4.2.2.1❶。

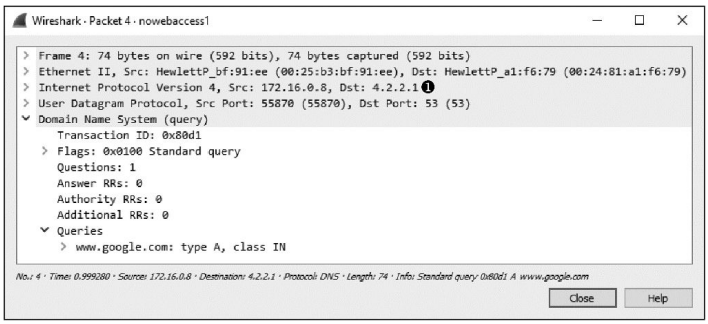

图 10-15　发送到 4.2.2.1 的第二个 DNS 查询

由于计算机仍然没有从 DNS 服务器收到响应，因此 1s 后，查询被再次发送到 4.2.2.2。如图 10-16 所示，这个过程不断重复，在接下来的几秒钟，计算机交替向配置好的首选 DNS 服务器 ❶ 和备用 DNS 服务器 ❷ 发送请求。整个过程大概花了 8s ❸，这正是用户的 Internet 浏览器报告该页无法访问之前所花的时间。

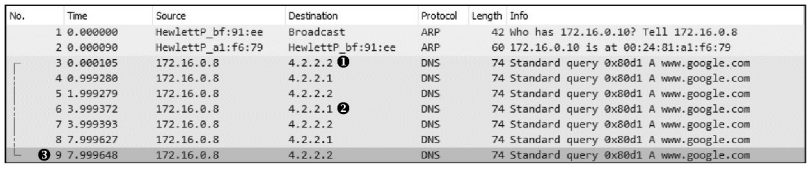

图 10-16　直到通信结束，重复的 DNS 查询才停止

基于前面看到的数据包，我们可以开始查明问题的根源了。首先，我们看见一个 ARP 请求成功地抵达网络上我们认为的默认网关，由此我们知道网关设备在线并且能连接。我们也知道用户的计算机确实在网络上传输数据包，所以我们可以假设本机的协议栈没有问题。显然当进行 DNS 请求时，问题就发生了。

就这个网络来说，DNS 请求是由 Internet 上的外部服务器（4.2.2.2 或 4.2.2.1）解析的。这意味着，要使解析顺利进行的话，负责将数据包路由到 Internet 的路由器必须成功将 DNS 查询转发到服务器，而且服务器必须响应。否则，就无法用 HTTP 请求 Web 页面。

我们知道其他用户上网都没有问题，这说明网络路由器和远程 DNS 服务器也许不是问题的原因所在。剩下唯一可能的问题来源是用户自己的计算机。

进一步检查这台故障计算机后，我们发现它不接受 DHCP 分配的地址，而是手动配置了地址信息，并且默认网关地址设置错了。被设置为默认网关的地址并不是一台路由器，它不能将 DNS 查询数据包转发到网络之外。

3．学到的知识

在这个情景中，问题出自一台配置错误的客户端。虽然这个问题相当简单，但它却严重影响了用户。对于缺少网络知识或者不能像我们这样可以快速分析数据包的人而言，排除这么简单的配置错误将花费相当多的时间。你可以看到，数据包分析并不局限于大型和复杂的问题。

注意，由于我们不知道网络上默认网关的 IP 地址，因此 Wireshark 不能准确地识别问题，但它可以告诉我们去哪里找，从而节省了宝贵时间。如果我们先与 ISP 联系或者尝试用其他手段排除远程 DNS 服务器的因素，而不是检查网关路由器，那么我们就能将注意力集中到计算机本身、实际也就是问题的原因上。

> 注意
>
> 如果我们能更熟悉这个特定网络的 IP 地址分配方案，就可以更快地分析出结果。如果我们注意到 ARP 请求被发送到与网关路由器不同的 IP 地址上，就能立刻知道问题所在。网络出现问题经常是由这些简单的配置错误造成的，通过分析少量的数据包，通常都能快速解决。