10.3.3 上游问题

与前两个场景一样，在这个场景中，有一位用户抱怨它的工作站无法上网。后来，他发现只是无法访问 Google 这个网站。进一步调查之后，我们发现这个问题影响到了机构的每一个人——谁也无法访问 Google。

这个网络的配置和前两个场景一样，仍然是用一些简单交换机和一个路由器将网络连接到 Internet。

1．侦听线路

为了解决这个问题，我们首先访问 Google 以生成流量。这是一个全网问题——意味着它也影响你的计算机，而且可能是感染恶意软件导致的——所以你不应该直接在你的设备上嗅探。当你在现实中遇到类似这样的问题时，网络分流器就是较好的解决方案，因为它允许你在短暂中断服务后完全被动地获取流量。通过网络分流器获得的流量被保存在 nowebaccess3.pcap 文件中。

2．分析

这个数据包的捕获以 DNS 流量开始，而不是我们之前看到的 ARP 流量。因为捕获的第一个数据包发往一个外部地址，并且数据包 2 包含来自那个地址的响应，所以我们可以假设 ARP 过程已经完成了，并且网关路由器的 MAC-IP 地址映射已经存在于主机的 ARP 缓存中。

如图 10-21 所示，捕获中的第一个数据包从主机 172.16.0.8 发往地址 4.2.2.1❶，并且它是一个 DNS 数据包 ❷。查看该数据包的内容，我们发现这是一个查询 Google 的 A 记录请求 ❸。

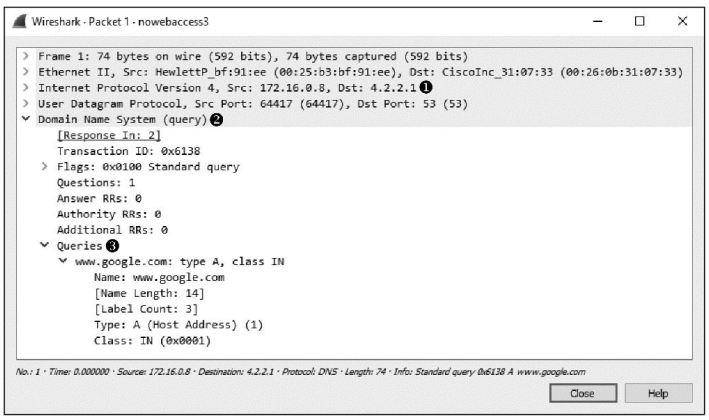

图 10-21　查询 Google 的 A 记录

如图 10-22 所示，来自 4.2.2.1 的响应是捕获文件的第 2 个数据包。查看 Packet Details 面板，我们发现响应这个请求的域名服务器提供了多个回答 ❶。此时看起来通信一切正常。

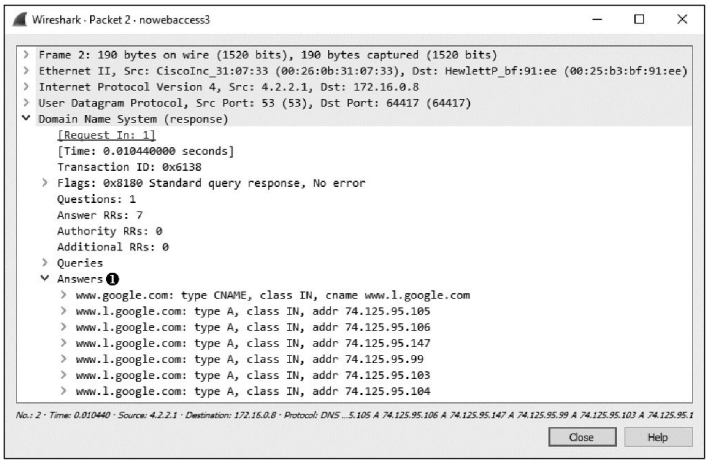

图 10-22　包含多个 A 记录的 DNS 响应

现在用户的计算机已经得到 Web 服务器的 IP 地址，它可以尝试与服务器通信了。如图 10-23 所示，通信过程从数据包 3 开始，这是一个从 172.16.0.8 发往 74.125.95.105 的 TCP 数据包 ❶。这个目标地址来自数据包 2 中 DNS 查询响应提供的第 1 个 A 记录。TCP 数据包设置了 SYN 标志 ❷，并尝试连接远程服务器的 80 端口 ❸。

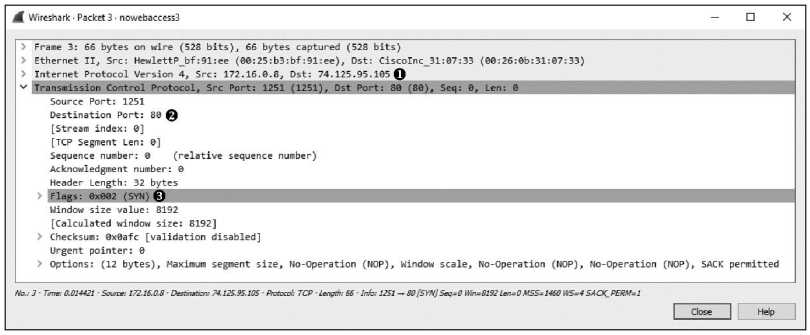

图 10-23　尝试连接 80 端口的 SYN 数据包

因为这是一个 TCP 握手过程，所以我们知道应该在响应中看到 TCP SYN/ACK 数据包，但是主机过一会儿又发送了另一个 SYN 数据包到目标。这个过程大概在 1s 后再次发生，如图 10-24 所示，到这里通信停止了，浏览器报告找不到网站。

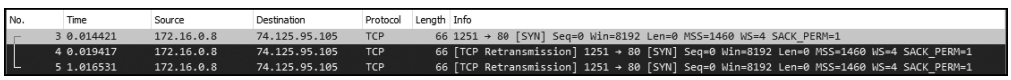

图 10-24　TCP SYN 数据包尝试了 3 次都没有收到响应

这时，我们想到由于能成功向外部 DNS 服务器提交查询请求，因此网络内的工作站可以连接到外网。DNS 服务器响应了一些看起来有效的地址，

然后我们的主机就尝试向其中一个地址建立连接。而且，我们尝试连接的本地工作站看起来功能正常。

问题是远程服务器没有响应我们的连接请求，连 TCP RST 数据包都没发过来。可能的原因有几种：Web 服务器配置错误、Web 服务器的协议栈崩溃、远程网络部署了数据包过滤设备[1]。假设本地网络没有数据包过滤设备，那么所有可能的解决方法都在远程网络上，这超出了我们的控制范围。在这个案例中，Web 服务器不能正常工作，我们的所有尝试都失败了。一旦 Google 修复故障[2]，通信就可以继续了。

3．学到的知识

这个场景中的问题不是我们能修复的。我们的分析表明，问题不在于我们网络上的主机、路由器，也不在于提供域名解析服务的外部 DNS 服务器。问题在我们的网络设施之外。

有时候发现这不是我们的问题不仅能缓解压力，也能在管理层来敲门时挽回颜面。我与很多运营商、设备厂商和软件公司打过交道，他们都说不是自己那边的问题，但你已经看到，数据包是不会说谎的。