## 10.5.2 分析

如图 10-30 所示，当工作站 172.16.16.101 尝试访问托管在总部应用服务器 172.16.16.200 的应用程序时，产生了捕获文件的第 1 个数据包。这个捕获只有两个数据包。第 1 个数据包是发送到 172.16.16.251❶ 的 DNS 请求，查询应用服务器 ❸ 的 A 记录 ❷。这是总部 172.16.16.200 服务器的 DNS 域名。

如图 10-31 所示，这个数据包的响应是服务器故障 ❶，表明 DNS 查询被阻止了。注意到这个数据包只是一个错误（服务器故障），并没有响应查询结果 ❷。

现在我们知道该通信故障与 DNS 有关。因为分公司的 DNS 查询由 DNS 服务器 172.16.16.251 解析，我们前往下一站。

为了从分公司的 DNS 服务器捕获合适的流量，我们将嗅探器留在原地，只改变端口镜像设置。现在服务器的流量就被镜像到我们的嗅探器了。捕获结果在 stranded_branchdns.pcap 文件中。

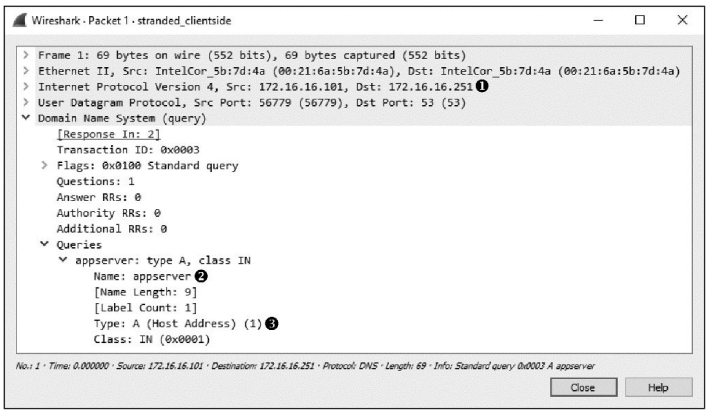


图 10-30　通信从查询应用服务器 A 记录的 DNS 请求开始

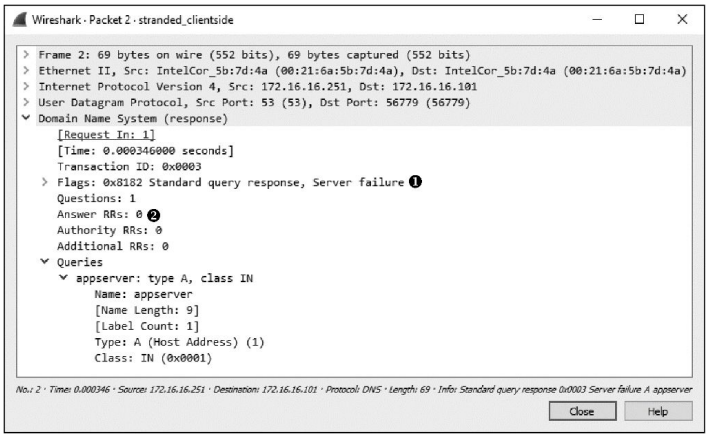

图 10-31　查询响应表明这是上游的问题

如图 10-32 所示，这个捕获的开头是我们之前看到的查询和响应，但还有一个额外的数据包。额外的数据包看起来很奇怪，因为它尝试与中心办公室的首选 DNS 服务器（172.16.16.250）❶ 的标准 DNS 服务端口 53❷ 进行通信，但它却不是我们过去看见的 UDP 类型 ❸。

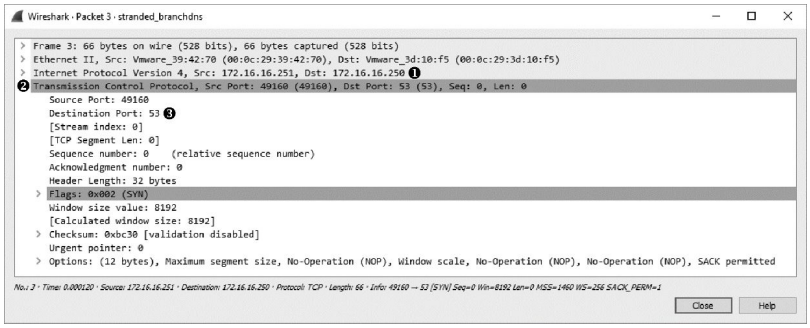


图 10-32　这个 SYN 数据包使用了 53 端口，但不是 UDP

为了找出这个数据包的用途，回顾我们在第 7 章对 DNS 的讨论。DNS 通常使用 UDP，但当响应超过一定大小时要使用 TCP。在那种情况下，我们会看见一些触发 TCP 流量的 UDP 流量。另外，TCP 也用于 DNS 的区域传送过程，它使资源记录在 DNS 服务器之间传输，这里就是该种情况。

分公司的 DNS 服务器是总部 DNS 服务器的从属服务器，意味着分公司的 DNS 服务器依赖于从总部服务器获得资源记录。分公司用户试图访问的应用服务器放置在总部，意味着总部 DNS 服务器是它的权威 DNS 服务器。要使分公司服务器能解析用户对应用服务器的 DNS 请求，总部 DNS 服务器必须把 DNS 资源记录传输给分公司 DNS 服务器，这可能是捕获文件中 SYN 数据包的来源。

SYN 数据包没有得到响应，这告诉我们总部和分公司 DNS 服务器之间失败的区域传送导致了 DNS 故障。现在我们可以进一步找出区域传送失败的原因。办公室之间的路由器或中心办公室的 DNS 服务器可能是罪魁祸首。为了找出问题，我们可以嗅探中心办公室 DNS 服务器的流量，查看 SYN 数据包是不是到达了服务器。

我没有给出中心办公室 DNS 服务器的流量捕获文件，因为根本就没有。SYN 数据包从来没有到达服务器。派遣技术人员查看连接两个办公室的路由器配置后，我们发现中心办公室的路由器被配置成只允许 53 端口的 UDP 流量进入，而 53 端口的 TCP 流量则被阻止了。这个简单的配置错误阻止了服务器间的区域传送，从而导致分支办公室的客户端无法解析对中心办公室设备的查询。