7.3.3 Echo 请求与响应

ICMP 因为 ping 工具而广为人知。ping 用来检测一个设备的可连接性。大多数信息技术专家都对 ping 很熟悉。

在命令行中输入 ping <ip 地址 >，其中将 <ip 地址 > 替换为网络上的一个实际 IP 地址，就可以使用 ping 了。如果目标设备在线，你的计算机有到达目标的通路，并且没有防火墙隔离通信的话，你将能够看到你的 ping 命令的响应。

在图 7-28 中的例子中，给出了 4 个成功显示了大小、RTT 和 TTL 的响应。Windows 还会提供一个总结信息，告诉你有多少数据包被发送、接收或者丢失。如果通信失败，会有一条信息告诉你原因。

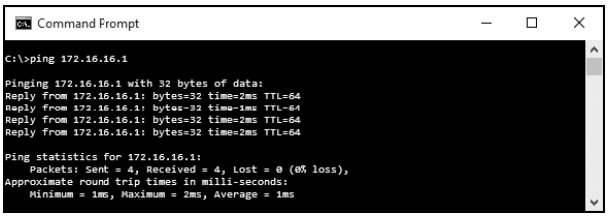

图 7-28　使用 ping 命令测试可连接性

基本上来说，ping 命令每次向一个设备发送一个数据包，并等待回复，以确定是否存在连接，如图 7-29 所示。

图 7-29　ping 命令只包含两步

> 注意
>
> 虽然 ping 对于 IT 业必不可少，但当部署了基于主机的防火墙时，它的结果就可能具有欺骗性了。现在的很多防火墙都限制了设备去响应 ICMP 数据包。这样对于安全性是有帮助的，因为潜在的攻击者可能会在使用 ping 来判断主机是否可达时，放弃进一步的行动。但这样故障排除也变得困难了起来——当知道你可以和一台设备通信时，使用 ping 检测连接却收不到任何响应会让你很抓狂。

ping 功能在实际中是简单 ICMP 通信的一个很好的例子。文件 icmp_echo.pcap 中的数据包会告诉你在运行 ping 时都发生了什么。

第一个数据包（见图 7-30）显示主机 192.168.100.138 在给 192.168.100.1 发送数据包。当你展开这个数据包的 ICMP 区段时，可通过查看类型和代码域，判断 ICMP 数据包的类型。在这个例子中，数据包的类型是 8，代码是 0，意味着这是一个 echo 请求（Wireshark 会告诉你所显示的类型/代码究竟是什么意思）。这个 echo（ping）请求是整个过程的前一半。这是一个简单的 ICMP 数据包，它使用 IP 发送，包含了很少的数据。除了指定类型、代码以及校验和，我们还会有一个序列号用来匹配请求和响应，另外，在 ICMP 数据包可变域还有一串随机文本字符。

> 注意
>
> echo 和 ping 经常会被混用，但记住，ping 实际上是一个工具的名字。ping 工具用来发送 ICMP 的 echo 请求数据包。

这个序列的第二个数据包是对我们请求的响应（见图 7-31）。这个数据包的 ICMP 区段类型是 0，代码是 0，表示这是一个 echo 响应。由于第二个数据包的序列号与第一个相匹配，因此我们可以知道这个 echo 响应包对应着之前的那个 echo 请求数据包。这个响应数据包中有着和初始请求中传输的 32 位字符串一样的内容。在第二个数据包被 192.168.100.138 成功接收到之后，ping 就会报告成功。

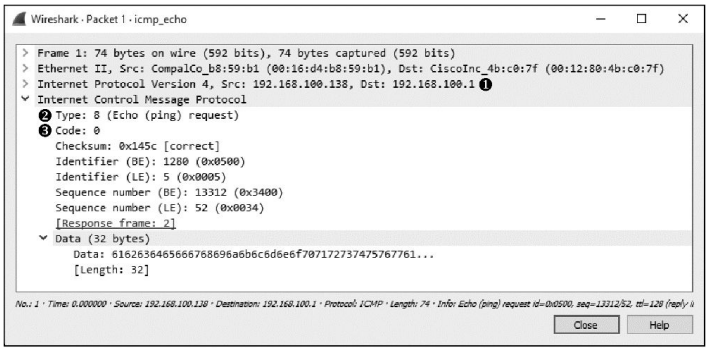

图 7-30　ICMP echo 请求数据包

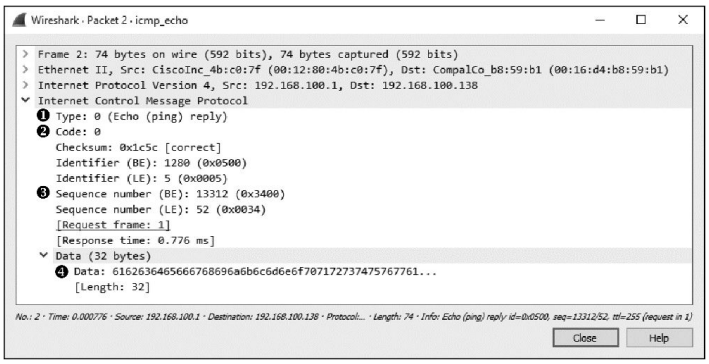

图 7-31　ICMP echo 回复数据包

你还可以使用 ping 的选项来增加它的数据填充，这样在检测不同类型的网络时，就可以强制将数据包分片。这在检测具有较小分片大小的网络时

会用到。

> 注意
>
> ICMP 的 echo 请求使用的随机文本可能会引起潜在攻击者的兴趣。攻击者可能会用这段填充的内容，来推测设备所使用的操作系统。并且攻击者可能会在这个域中放置一些数据位，作为反向连接的手段。