8.1.5 TCP 重置

在理想情况下，每一个连接都会以 TCP 终止来正常结束。但在现实中，连接经常会突然断掉。举例来说，这可能是由于一个潜在的攻击者正在进行端口扫描，或者仅仅是主机配置错误所导致。在这些情况下，就需要使用设置了 RST 标志的 TCP 数据包。RST 标志用来指出连接被异常中止，或拒绝连接请求。

文件 tcp_refuseconnection.pcapng 给出了一个包含有 RST 数据包网络流量的例子。这个文件中的第一个数据包来自 192.168.100.138，其尝试与 192.168.100.1 的 80 端口进行通信。这个主机不知道 192.168.100.1 并没有在监听 80 端口，因为那是一个思科路由器，并且并没有配置 Web 接口，也就是说并没有服务监听 80 端口的连接。为了响应这个连接请求，192.168.100.1 向 192.168.100.138 发送了一个数据包，告诉它其对于 80 端口的通信无效。图 8-11 中展示了在第二个数据包的 TCP 头中这个连接尝试突然终止的情况。RST 数据包除了包含 RST 和 ACK 标志外，没有任何其他的东西，之后也并没有额外的通信。

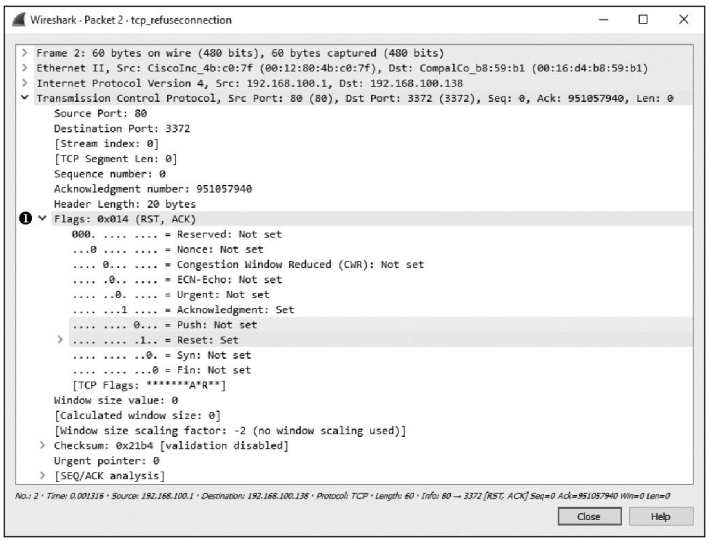

图 8-11　RST 和 ACK 标志代表着通信的结束

RST 数据包会在尝试通信序列的开始（就像这个例子一样）或者在主机通信的中途，来终止通信。