11.1.2 TCP 重复确认和快速重传

当接收方收到乱序数据包时，就发送重复的 TCP ACK 数据包。TCP 在其头部使用序号和确认号域，以确保数据被可靠接收并以发送顺序重组。

> 注意
>
> 「TCP 数据包」的准确术语其实应该是「TCP 区段」，但大多数人倾向于把它们称为「数据包」。

建立一个新的 TCP 连接时，初始序号（Initial sequence number，ISN）是握手过程中交换的最重要信息之一。一旦设置好连接两端的 ISN，接下来传输的每一个数据包都将按照数据载荷的大小增长序号。

举个例子，一台主机的 ISN 是 5000，它发送一个 500 字节的数据包给接收方。一旦接收到此数据包，接收方就会根据以下规则响应一个包含确认号 5500 的 TCP ACK 数据包：

接收数据的序号 + 接收数据的字节数 = 发出的确认号

在这个运算中，返回到发送方的确认号实际上就是接收方期待下次接收的数据包序号。图 11-6 中可以看到一个这样的例子。

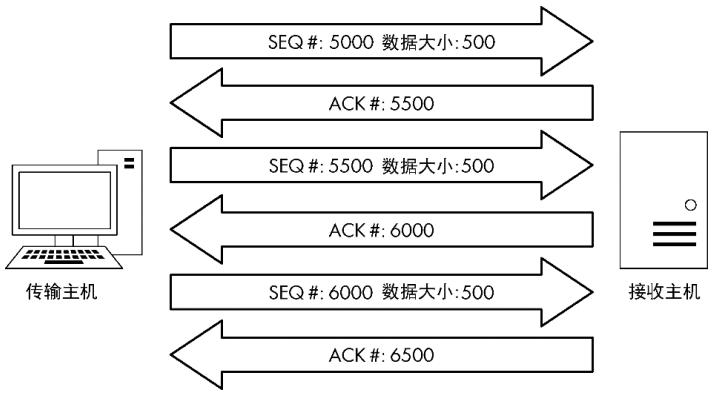

图 11-6　TCP 序号和确认号

序列号使数据接收方检测数据包丢失成为可能。当接收方追踪正在接收的序号时，如遇到不合顺序的序号，它就知道数据包丢失了。

当接收方收到一个预料之外的序号时，它会假设有一个数据包在传输中丢失了。为了正确重组数据，接收方必须要得到丢失的数据包，因此它重新发送一个包含丢失数据包的序号的 ACK 数据包，以通知发送方重传该数据包。

当传输主机收到 3 个来自接收方的重复 ACK 时，它就假设这个数据包确实在传输中丢失了，并立刻发送一个快速重传。一旦触发快速重传，其他所有正在传输的数据包都要靠边，直到把快速重传数据包发送出去为止。图 11-7 描述了这个过程。

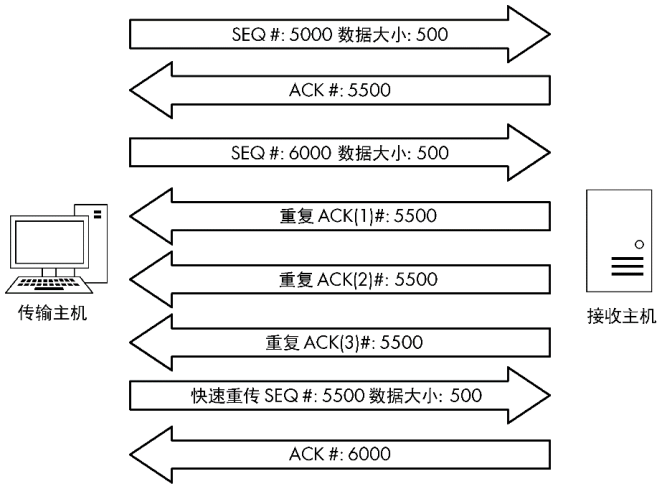

图 11-7　来自接收方的重复 ACK 导致快速重传

你将在 tcp_dupack.pcap 文件中发现重复 ACK 和快速重传的例子。捕获记录中的第一个数据包，如图 11-8 所示。

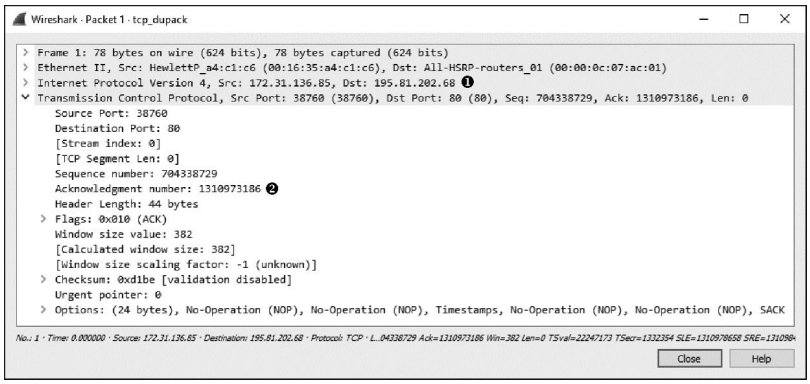

图 11-8　ACK 显示了下一个期待的序号

在网络中这个 TCP ACK 数据包从数据接收方（172.31.136.85）去往发送方（195.81.202.68）❶，包含了一个对捕获文件之前的数据包的确认。

> 注意
>
> 默认情况下，Wireshark 使用相对序号来简化对这些数字的分析，但在接下来的几节中，并未在例子和截图中使用这个特性。使用如下方法可关闭此项功能，选择 Edit->Preferences，在 Preferences 窗口中选择 Protocols，然后选择 TCP 区段，最后取消 Relative sequence numbers 和 window scaling 旁边的复选框。

如图 11-9 所示，此数据包中的确认号是 1310973186❷，这应该是接收的下一个数据包的序号。

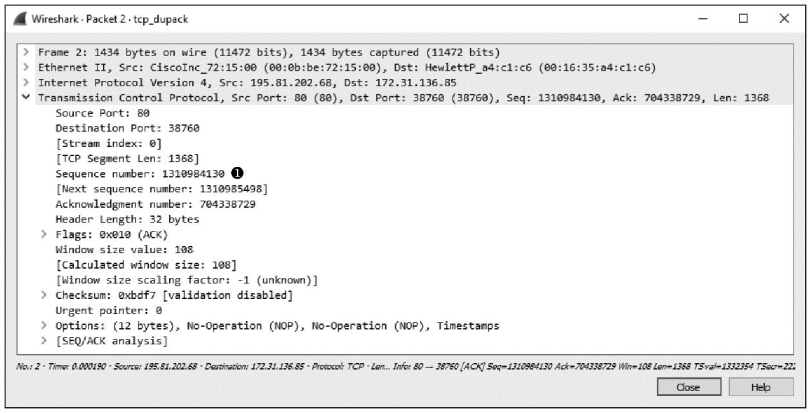

图 11-9　此数据包的序号与预料的不同

很遗憾，下一个数据包的序号是 1310984130 ❶，并非是我们所期待的。这表明期待的数据包在传输中莫名其妙地丢失了。如图 11-10 所示，接收主机注意到这个数据包的序号不符，就在捕获记录的第三个数据包中发送一个重复的 ACK。

通过查看以下信息的其中一个，你就可以确定这是一个重复的 ACK 数据包。

- Packet Details 面板中的 Info 列。这个数据包以黑底红字呈现。
- SEQ/ACK Analysis heading 下的 Packet Details 面板。若展开此标题，你会发现这个数据包被列为数据包 1 的重复 ACK。

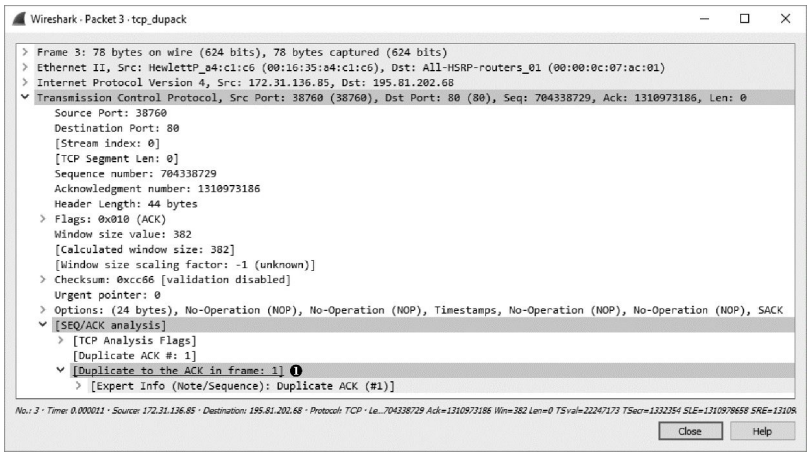

图 11-10　第一个重复 ACK 数据包

如图 11-11 所示，接下来的几个数据包继续这个过程。

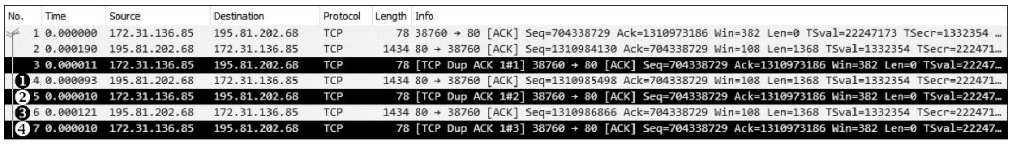

图 11-11　由于乱序数据包的影响，生成了额外的重复 ACK

捕获文件的第 4 个数据包是发送主机以错误序号发送的另一个数据区块❶。因此，接收主机发送第二个重复 ACK❷。接收方又收到一个包含错误序号的数据包 ❸。这导致它传输第三个、也是最后一个重复 ACK❹。

发送方收到来自接收方的第三个重复 ACK 之后，就强制停止所有的数据包传输，并重新发送丢失的数据包。图 11-12 显示了丢失数据包的快速重传。

在 Packet List 面板的 Info 列中再次出现了重传数据包。正如前面的例子，数据包被清楚地标记为黑底红字。这个数据包的 SEQ/ACK 分析部分告诉我们这有可能是一次快速重传 ❶（再次注意，数据包的快速重传标记信息并非数据包本身的值，而是 Wireshark 的功能）。捕获记录的最后一个数据包是确认收到快速重传的 ACK 数据包。

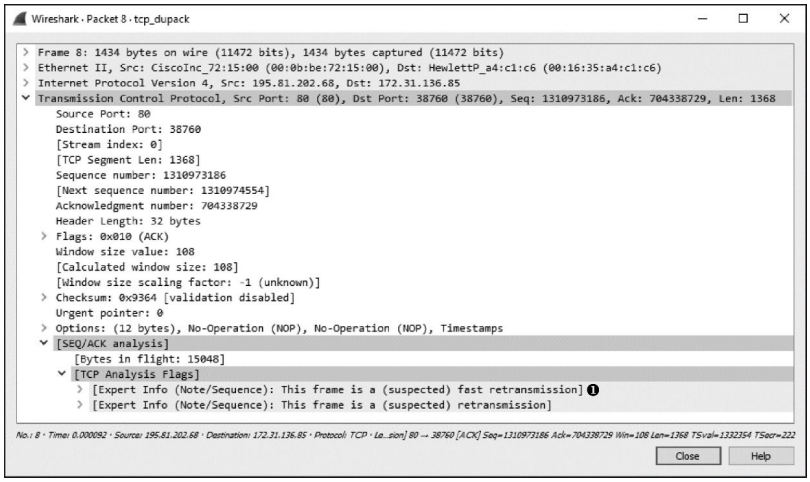

图 11-12　重复 ACK 引发了丢失数据包的快速重传

注意

当发生数据包丢失时，可能影响 TCP 通信数据流的功能是选择性确认（Selective Acknowledgement）。在上面的捕获记录里，通信双方已经在三次握手过程中协商开启了选择性 ACK。因此，一旦数据包丢失并收到重复 ACK，即使在丢失数据包之后还是成功接收了其他数据包，也只需要重传丢失的数据包。如果不启用选择性 ACK，那就必须重新传输丢失数据包之后的每一个数据包。选择性 ACK 使得数据丢失的恢复更加高效。由于大部分现代 TCP/IP 协议栈的实现都支持选择性 ACK，因此你会发现这个功能通常都会被启用。