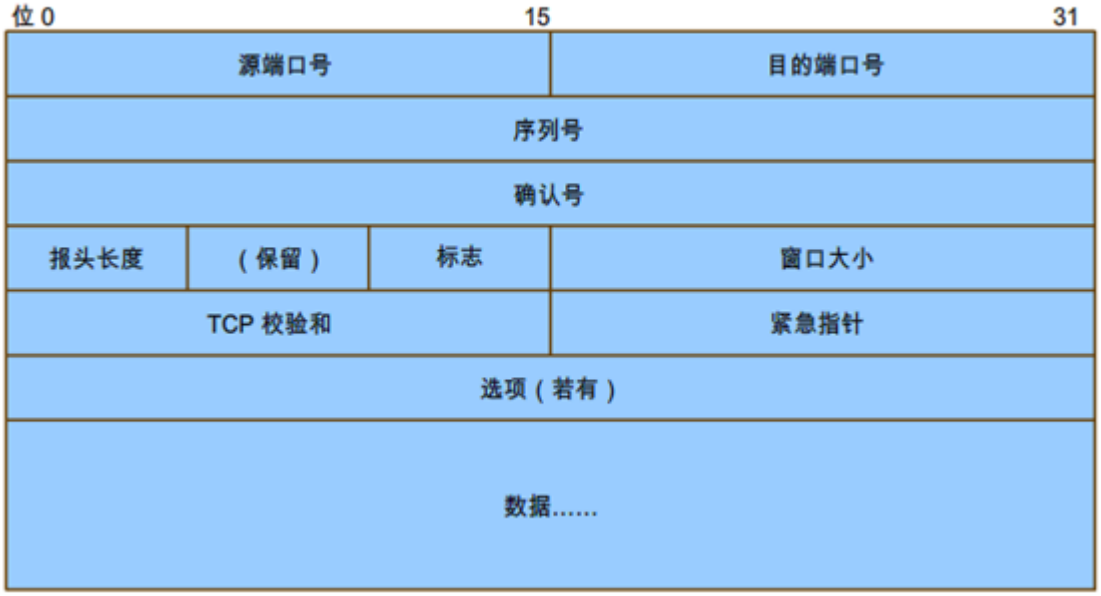
TCP 数据段报头字段

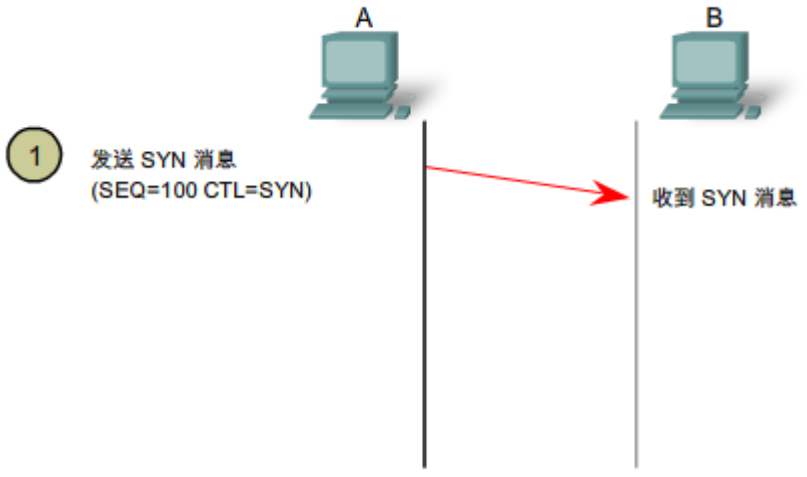


TCP 报头字段使 TCP 能够提供面向连接的可靠数据通信。

当两台主机采用 TCP 协议进行通信时，在交换数据前将建立连接。通信完成后，将关闭会话并终止连接。连接和会话机制保障了 TCP 的可靠性功能。

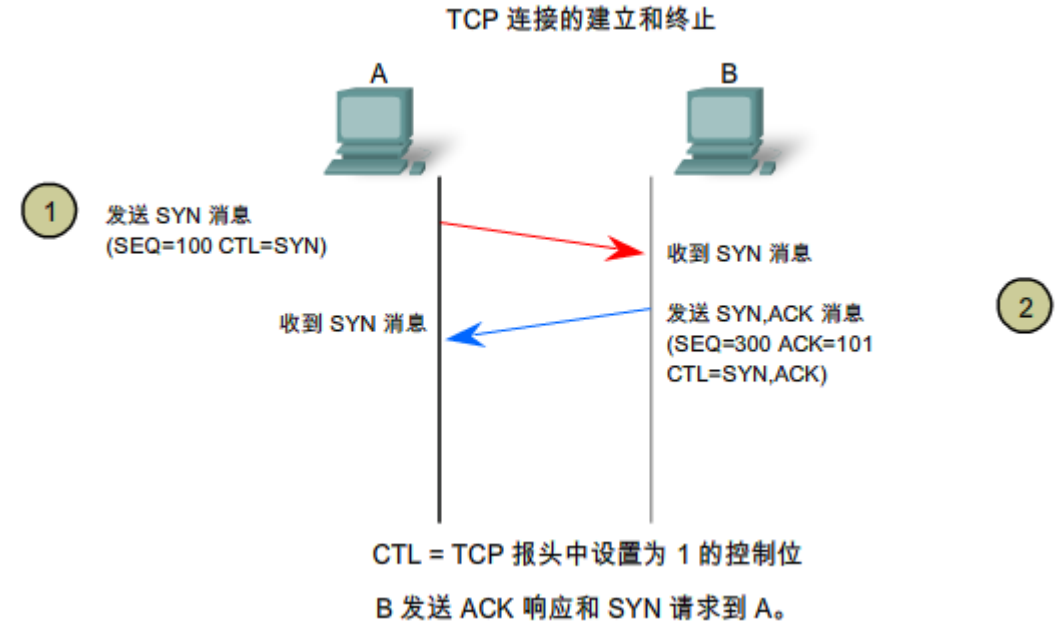
请参见图中建立并终止 TCP 连接的步骤。

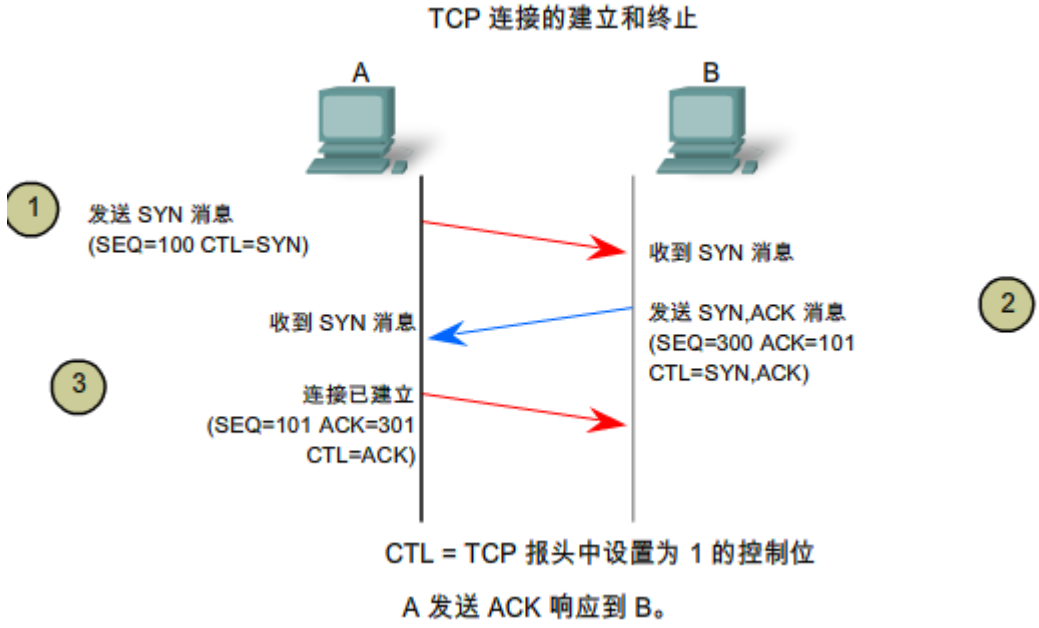
TCP 连接的建立和终止



CTL = TCP 报头中设置为 1 的控制位

A 发送 SYN 请求到 B。





主机将跟踪会话过程中的每个数据段，并使用 TCP 报头中的信息了解每台主机所接收到的数据。

每个连接都代表两股单向通信数据流或者会话。若要建立连接，主机应执行三次握手。TCP 报头中的控制位指出了连接的进度和状态。

三次握手：

1．确认目的设备存在于网络上；

2．确认目的设备有活动的服务，并且正在源客户端要使用的目的端口号上接受请求；

3．通知目的设备源客户端想要在该端口号上建立通信会话。

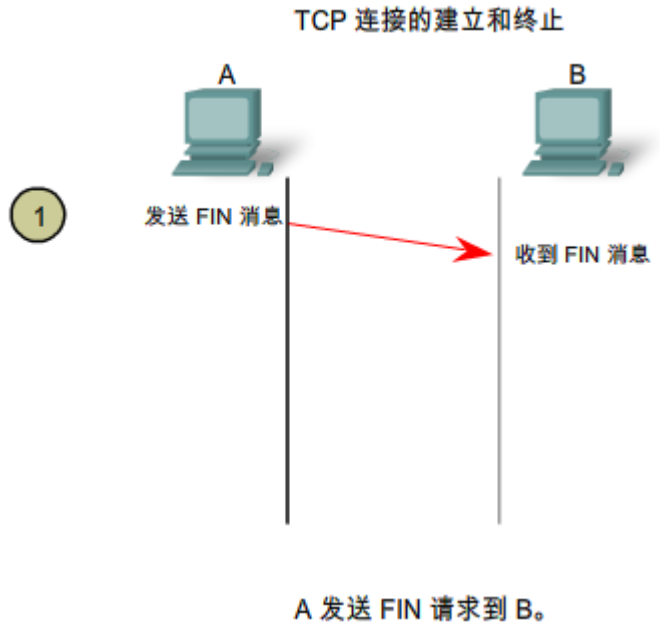
在 TCP 连接中，充当客户端的主机将向服务器发起该会话。

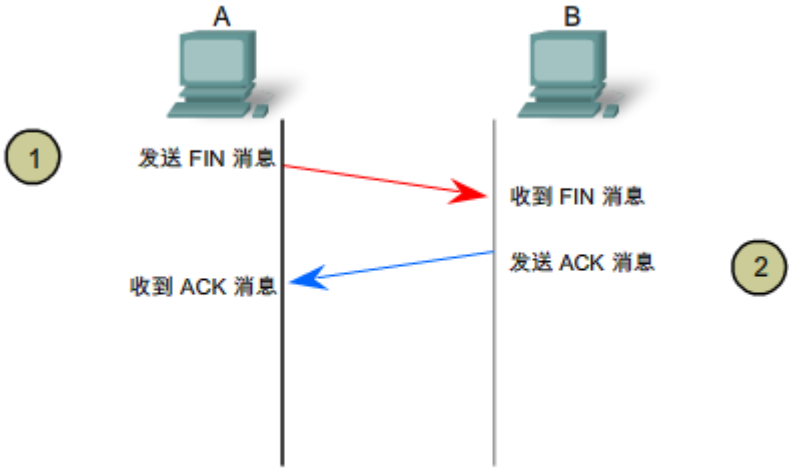
TCP 连接创建的过程分为三个步骤：

1. 客户端向服务器发送包含初始序列值的数据段，开启通信会话；
2. 服务器发送包含确认值的数据段，其值等于收到的序列值加 1，并加上其自身的同步序列值。该值比序列号大 1，因为 ACK 总是下一个预期字节或二进制八位数。通过此确认值，客户端可以将响应和上一次发送到服务器的数据段联接起来；
3. 发送带确认值的客户端响应，其值等于接受的序列值加 1。这便完成了整个建立连接的过程。

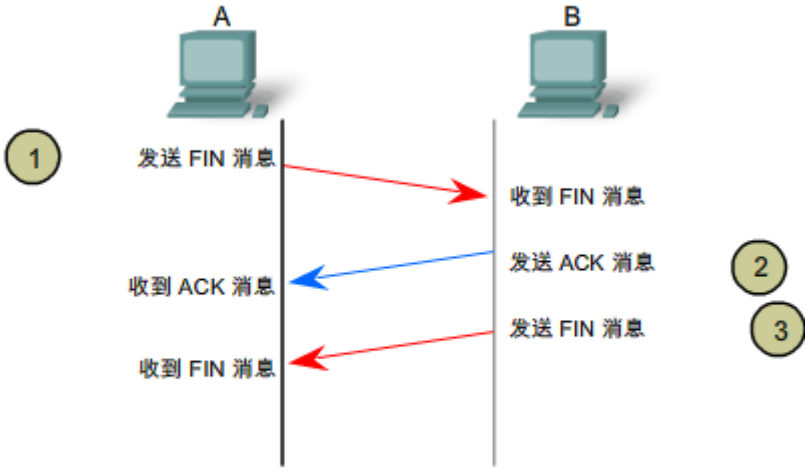
为了理解三次握手的过程，必须考察两台主机间交换的不同值。在 TCP 数据段报头中，有六个包含控制信息的 1 比特字段，用于管理 TCP 进程。这些字段分别是：
URG — 紧急指针
ACK — 确认字段
PSH — 推送功能
RST — 重置连接
SYN — 同步序列号
FIN — 发送方已传输完所有数据

这些字段用作标志，由于它们都只有 1 比特大小，所以它们都只有两个值：1 或者 0。当值设为 1 时，表示数据段中包含控制信息。
通过 4 步流程法，可以交换标志，以终止 TCP 连接。

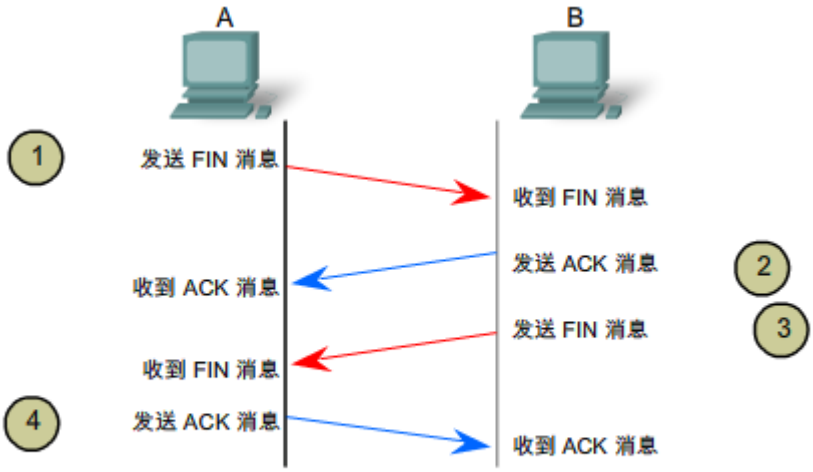




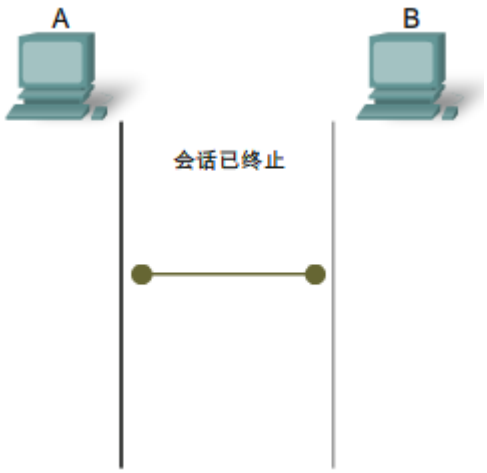
B 发送 ACK 响应到 A。



B 发送 FIN 消息到 A。



A 发送 ACK 响应到 B。



ＴＣＰ三次握手

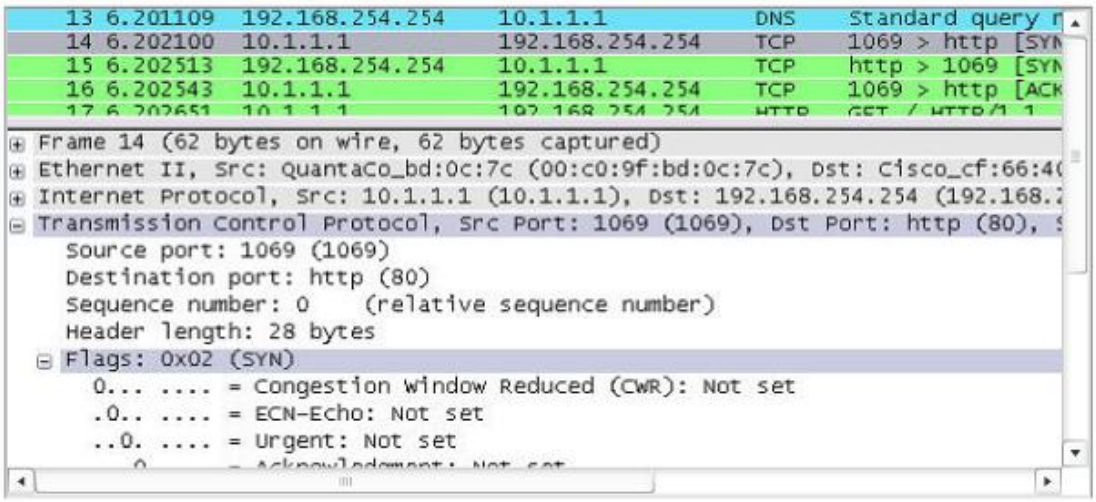
步骤 1：

TCP 客户端发送带同步序列号 (SYN) 控制标志设置的数据段，指示包含在报头中的序列号字段的初始值，用以开启三次握手。序列号的初始值称为初始序列号 (ISN)，由系统随机选取，并用于跟踪会话过程中从客户端到服务器的数据流。在会话过程中，每从客户端向服务器发送一个字节的数据，数据段报头中包含的 ISN 值就要加 1。

如图所示，协议分析器的输出结果中显示了 SYN 控制标志和相应的序列号。

SYN 控制标志被置位并且相应的序列号设定为 0。尽管图中的协议分析器已显示了序列号和确认号的相应值，但其真实值应该为 32 位二进位数字。我们可以通过研究 Packet Bytes 窗格确定数据段报头中发送的实际数值。此处您可以看到以十六进制显示的四个字节。

TCP 三次握手 (SYN)



协议分析器显示了帧 14 中的客户端初始会话请求。

此帧中的 TCP 数据段显示：

- SYN 标志设置为验证初始序列号
- 采用随机序列号有效（相关值为 0）
- 随机源端口 1069
- 公认目的端口 80（HTTP 端口）表示 Web 服务器 (http)

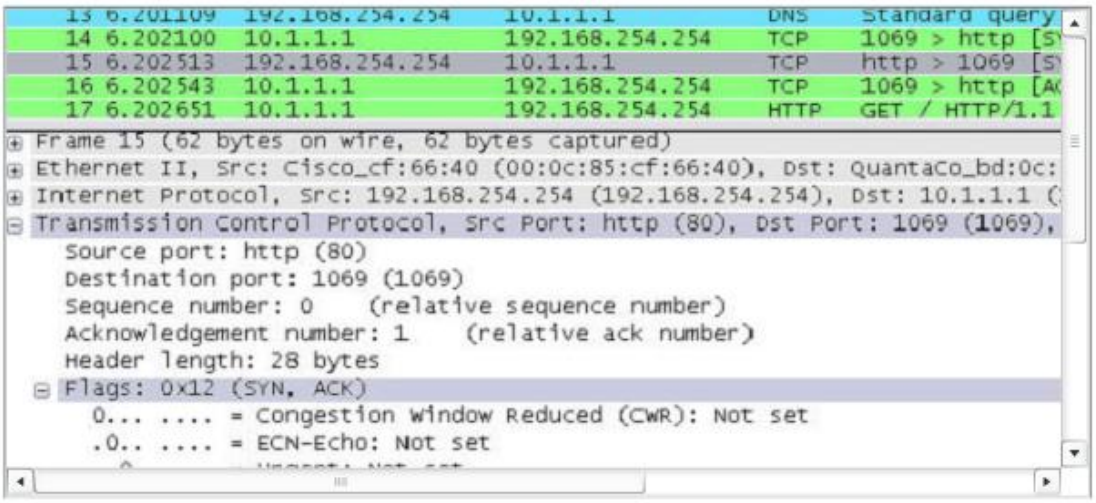
步骤 2：

TCP 服务器需要确认从客户端处收到 SYN 数据段，从而建立从客户端到服务器的会话。为了达到此目的，服务器应向客户端发送带 ACK 标志设置的数据段，表明确认编号有效。客户端将这种带确认标志设置的数据段理解为确认信息，即服务器已收到从 TCP 客户端发出的 SYN 信息。

确认编号字段的值等于客户端初始序列号加 1。此时创建从客户端到服务器的会话。ACK 标志将在会话其间保持设置。我们在前面已经学过，客户端和服务器之间的会话实际上是由两个单向的会话组成的：一个是从客户端到服务器的会话，另一个则正好相反。在三次握手过程的第二步中，服务器必须发起从服务器到客户端的响应。为开启会话，服务器应采用与客户端同样的方法使用 SYN 标志。该操作设置报头中的 SYN 控制标志，从而建立从服务器到客户端的会话。SYN 标志表明序列号字段的初始值已包含在报头中，且该值将用于跟踪会话过程中从服务器返回客户端的数据流。

如右图所示，协议分析器的输出结果中显示了 ACK 和 SYN 控制标志的设置，以及相应的序列号和确认号。

TCP 三次握手 (SYN, ACK)



协议分析器显示了帧 15 中的服务器响应

- ACK 标记设置为表示有效确认号
- 确认号与序列号相对应，两者间相差 1
- SYN 标志设置为表示从服务器到客户端会话的初始序列号
- 目的端口号 1069 与客户端源端口对应
- 源端口号 80 (HTTP) 表示 Web 服务器服务 (http)

步骤 3：

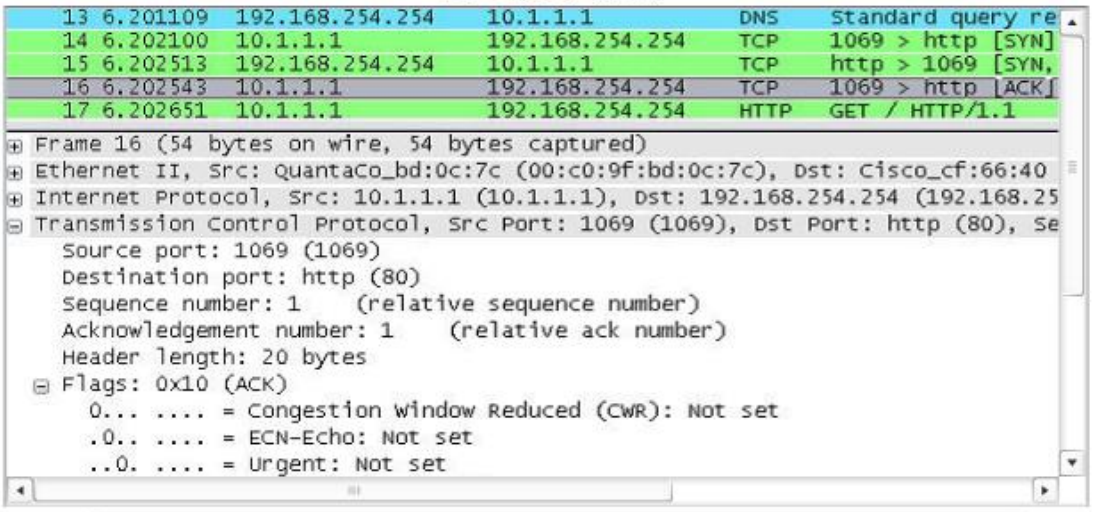
最后，TCP 客户端发送包含 ACK 信息的数据段，以示对服务器发送的 TCP SYN 信息的响应。在该数据段中，不包括用户数据。确认号字段的值比从服务器接收的初始序列号值大 1。一旦在客户端和服务器之间建立了双向会话，该通信过程中交换的所有数据段都将包含 ACK 标志设置。

如图所示，协议分析器的输出结果中显示了 ACK 控制标志，以及相应的序列号和确认号。

通过以下方式，可以加强数据网络的安全性：
拒绝建立 TCP 会话；
只允许建立特定服务的会话；
只允许已建立会话之间的通信。

以上安全策略可以应用于所有 TCP 会话，也可以仅应用于某些选定会话。

TCP 三次握手 (ACK)



协议分析器显示了帧 16 中客户端对会话的响应

此帧中的 TCP 数据段显示：

- ACK 标志设置为表示有效确认号
- 确认号与响应初始序列号相对应，两者间相差 1
- 源端口号为对应的 1069
- 目的端口号 80 (HTTP) 表示 Web 服务器服务 (http)

若要关闭连接，应设置数据段报头中的 FIN（结束） 控制标志。为终止每个单向 TCP 会话，需采用包含 FIN 数据段和 ACK 数据段的二次握手。因此，若要终止 TCP 支持的整个会话过程，需要实施四次交换，以终止两个双向会话。注意：在本部分中，为了更容易理解，采用了客户端和服务器端进行说明。实际上，终止的过程可以在任意两台完成会话的主机之间展开。

1. 当客户端的数据流中没有其它要发送的数据时，它将发送带 FIN 标志设置的数据段；

2. 服务器发送 ACK 信息，确认收到从客户端发出的请求终止会话的 FIN 信息；

3. 服务器向客户端发送 FIN 信息，终止从服务器到客户端的会话；

4. 客户端发送 ACK 响应信息，确认收到从服务器发出的 FIN 信息。

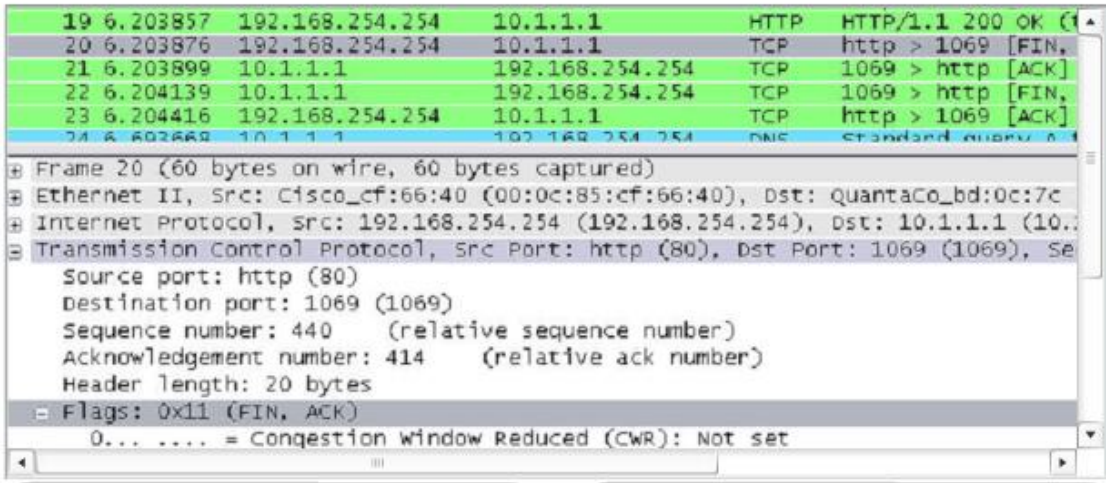
当会话中的客户端没有其它要传输的数据时，它将在数据段报头中设置 FIN 标志。然后，会话中的服务器端将发送包含 ACK 标志设置的一般数据段信息，通过确认号确认已经收到所有数据。当所有数据段得到确认后，会话关闭。

另一方向的会话采用相同的方式关闭。接收方在数据段的报头中设置 FIN 标志，然后发送到发送方，表明没有其它需要发送的数据。返回的确认信息确定已接收所有数据，随即该方向的会话关闭。

如右图所示，在数据段报头中设置了 FIN 和 ACK 控制标志，并从而关闭了 HTTP 会话。

也可以通过三次握手方式关闭连接。当客户端没有其它要传输的数据时，它将向服务器发送 FIN 信息。如果服务器也没有其它要传输的数据，它将发送同时包含 FIN 和 ACK 标志设置的响应信息，将两步并作一步。最后，客户端返回 ACK 信息。

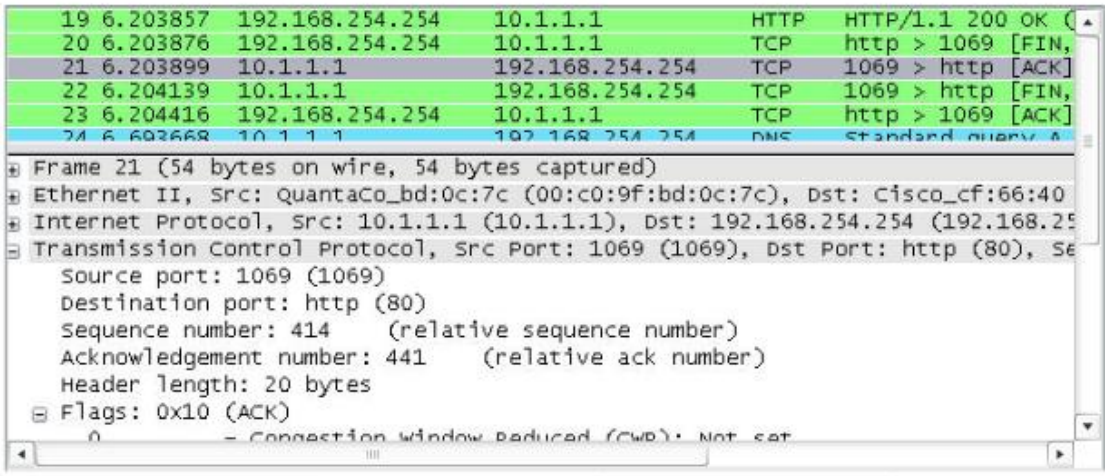
TCP 会话终止 (FIN)



协议分析器显示了帧 20（TCP FIN 请求）的详细信息。

目的端口和源端口
报头字段的内容和值

TCP 会话终止 (ACK)



协议分析器显示了帧 21（TCP ACK 响应）的详细信息。

目的端口和源端口
报头字段的内容和值