实验九 TCP 传输控制协议分析

【实验目的】

1、掌握 TCP 协议的报文形式。
2、掌握 TCP 连接的建立和释放过程。
3、掌握 TCP 数据传输中编号与确认的过程。
4、理解 TCP 重传机制。

【实验学时】

2 学时

【实验环境】

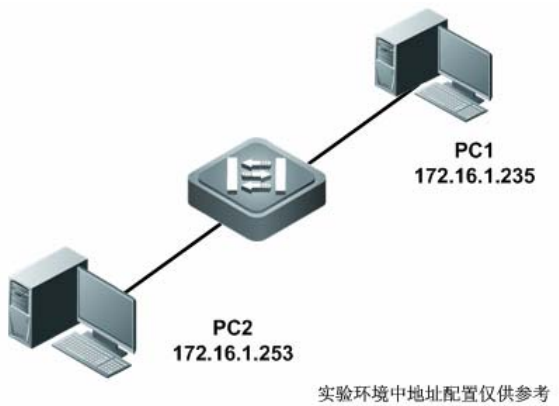

图 4-9 实验拓扑图

【实验内容】

1、学习 UDP 协议的通信过程。
2、学习分析 UDP 协议报头字段含义。

【实验流程】

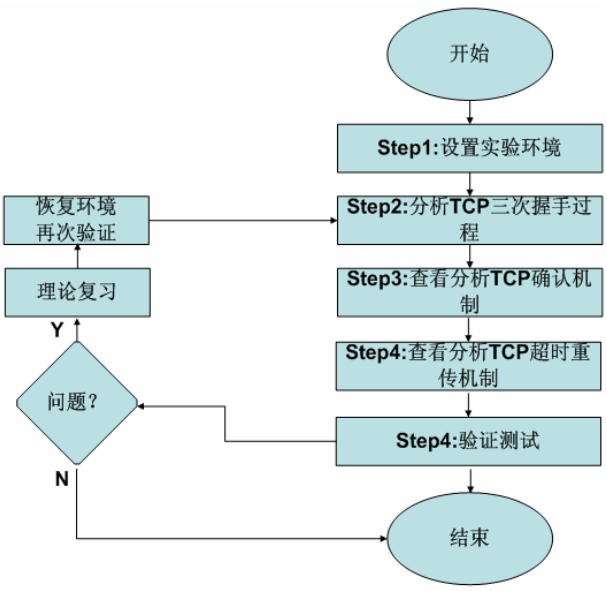

图 4-10 实验流程图

【实验原理】

TCP 报文段首部长度为 20-60 字节，报文段首部格式如下图所示。

图 4-11 TCP 报文格式

当没有选项和填充字段时，首部长度是 20 字节。其中个字段含义如下：

- 源端口地址：长度为 16 比特，定义了在主机中发送这个报文段的应用程序的端口号，如应用程序为客户端，端口号通常为随机端口，如果应用程序为服务端，端口号通常为熟知端口。
- 目的端口地址：长度为 16 比特，定义了在主机中接收报文段的应用程序的端口号。

- 序号：长度为 32 比特，定义了本数据段中封装数据的的第一个字节的序号。在 TCP 的数据传输中，传输数据前随机产生一个数字，叫初始序号，初始序号分配给需要传输的第一个字节，此后需要传输的数据在此基础上依次递增，因此需要传输的每个字节都有一个字节序号，TCP 报头中序号字段放置的是本数据段中数据部分的第一个字节的序号。
- 确认号：长度为 32 比特，定义了接收端希望从源端接收的报文段的序号，通常，接收端收到源端发送的数据后，将最后一个字节序号加 1，定义为发送数据确认号发送给源端，表示此序号之前的数据均已收到。
- 首部长度：长度为 4 比特，定义了 TCP 首部共有多少个 4 字节，首部长度可以在 20-60 字节之间，因此在当前版本中，首部长度的值可以在 5-15 之间。
- 保留：长度为 6 比特，保留为今后使用。
- 控制字段：长度为 6 比特，定义了 6 种不同的控制位或标识，其中
- URG：紧急指针有效；
- ACK：表示确认字段值有效；
- PSH：推送数据；
- RST：连接必须复位；
- SYN：在连接建立是对序号进行同步；
- FIN：终止连接。
- 窗口值：长度为 16 比特，定义了对方必须维持的窗口值，可定义的最大窗口值为 65535。
- 校验和：长度为 16 比特，定义了 TCP 首部、TCP 伪首部、数据进行的校验和。
- 紧急指针：当紧急标志位置 1 时，标识此数据包含紧急数据，紧急指针用于标识此数据段中的数据部分那些是紧急数据，紧急数据在接收端可以不按照顺序而被优先处理。
- 选项：TCP 选项字段用于把附加信息传递给目的端。

【实验步骤】

步骤一：设定实验环境

1、配置主机 IP 和路由器 IP 地址。

2、按照实验拓扑连接网络拓扑。

步骤二：查看分析 TCP 三次握手

1、在 PC2 中安装 FTP 服务端程序。

2、在 PC1 中开启协议分析软件，进行数据包抓包。

3、在 PC1 中的协议分析软件中利用工具栏中的 TCP 连接工具对 PC2 发起连接，如下图所示。

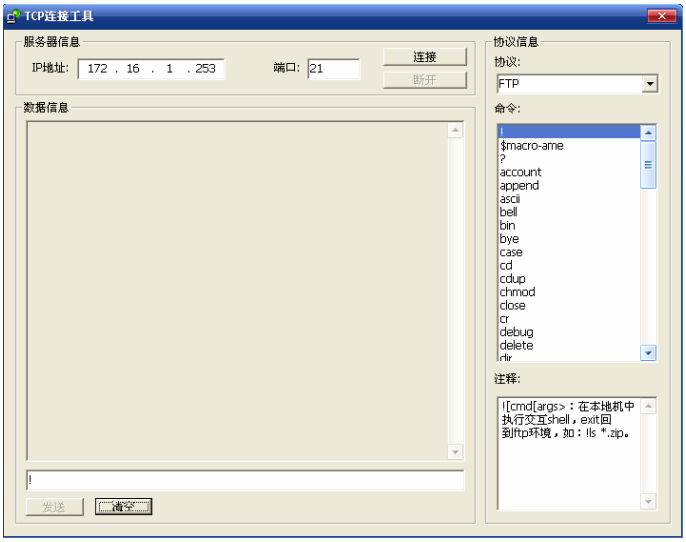

图 4-12 TCP 连接工具

在 IP 地址中填入 PC2 地址 172.16.1.253，端口填入 FTP 服务端口 21，然后点击连接。分析 PC2 中捕获到的三次握手报文。

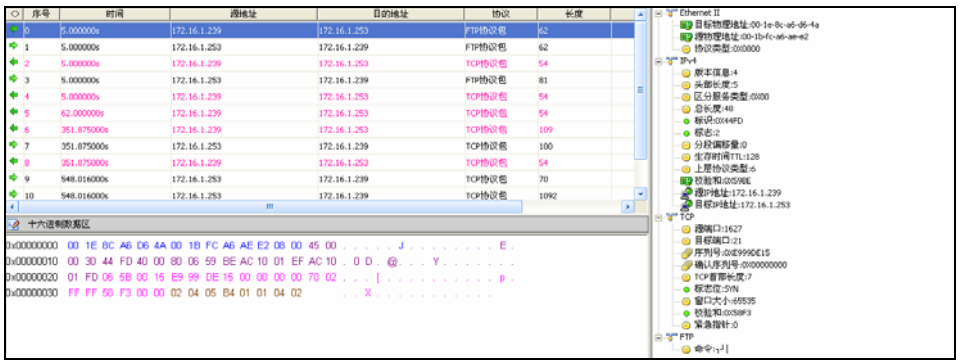

图 4-13 三次握手第一次连接

查看上图 TCP 报文中的报头部分：

- 源端口：1627，由于发起连接的是客户端，因此源端口为 TCP 程序随机出的短暂端口，在此连接中是 1627。
- 目的端口：21，由于是向 FTP 服务发起连接，因此目的端口为 FTP 服务的熟知端口，为 21。
- 序列号：0XE9999DE15，此序列号为 TCP 程序随机出的字节编号。
- 确认序号：0X00000000，第一个发出的连接请求中，确认号为 0。
- TCP 首部长度：7，TCP 首部长度包括 TCP 报头长度和数据长度，这个字段表示 TCP 报头长度，其中 20 字节为标准 TCP 报头长度，另有 8 字节选项字段长度，选项字段中和服务器端协商了最大报文段长度。
- 标识位：SYN 位置 1，只有 TCP 连接中三次握手第一次连接的报文段中 SYN 位

置 1。

- 窗口大小：65535，默认大小。
- 校验和：0X58F3，校验和是对 TCP 报头、数据和伪首部进行计算得出的校验和。
- 紧急指针：0，当紧急标识位置 1 时，此 16 位字段才有效，说明此时报文段中包含紧急数据，紧急数据到达接受端后可以不按次序优先被接受程序处理。

TCP 三次握手过程中第二个报文如下图所示。

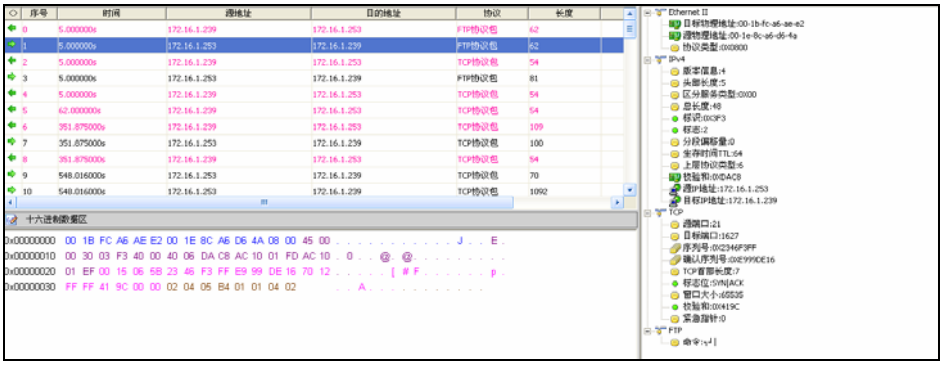

图 4-14 TCP 三次握手第二个报文

查看上图中的 TCP 报头：

- 源端口：21，服务端的源端口为相关服务的熟知端口，FTP 服务端口为 TCP21。
- 目的端口：1627，为客户端源端口复制过来得到。
- 序列号：0X2346F3FF，为服务端随机计算出的字节序号。
- 确认序列号：0XE9999DE16，确认序列号的功能是对发送端数据进行确认，为发送端序号 0XE9999DE15+1 得到。
- TCP 首部长度：7，包含 20 字节标准 TCP 首部长度和 8 字节选项长度。
- 标志位：SYN 位和 ACK 位置 1，表示此报文为 TCP 三次握手的第二个报文。
- 窗口大小：65535，为默认大小。
- 校验和：0X419C，TCP 校验和为 TCP 首部、数据和伪首部三部分计算得出校验和。
- 紧急指针：0。

TCP 三次握手第三个报文如下图所示。

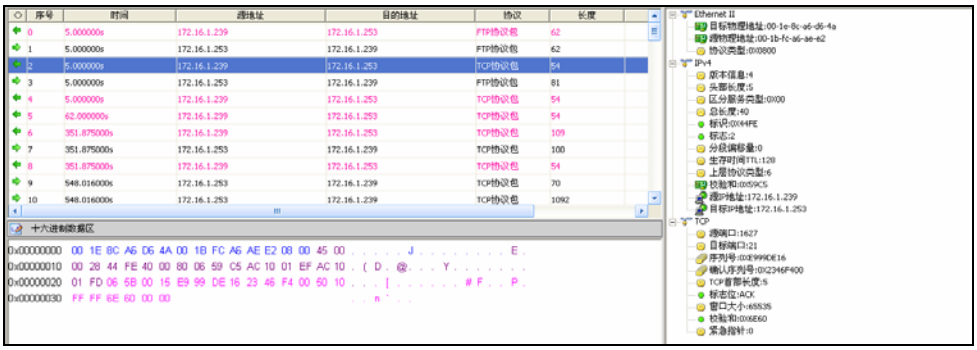

图 4-15 TCP 三次握手第三个报文

查看 TCP 三次握手第三个报文首部

- 源端口：1627，同一个连接发送的数据，源端口保持不变。
- 目的端口：21，对同一个服务发送的数据段中的目的端口保持不变。
- 序列号：0XE9999DE，为前一个数据段序列号加 1。
- 确认序号：0X2346F3FF，由于此报文是对服务端发回的连接应答消息的确认，因此是上一个报文序号 0X2346F3FF 加 1。
- TCP 首部长度：5，标准 TCP 首部长度为 5*4 字节=20 字节。
- 标识位：TCP 三次握手第三个报文段 ACK 位置 1。
- 窗口大小：65535，默认窗口大小。
- 校验和：0X6E60，为 TCP 首部、数据、伪首部计算得出的校验和。
- 紧急指针：0，未使用紧急指针。

通过上面的 TCP 三次握手的报文，可以很清楚的分析出在 TCP 连接建立时，客户端和服务端所进行的工作。三次报文的重要区别在于标识位的不同，第一个报文，SYN 位置 1，第二个报文是对第一个报文的确认，SYN 位置 1，ACK 位置 1，第三个报文是确认报文，ACK 位置 1。

步骤三：查看分析 TCP 确认机制

1、在 PC1 中开启协议分析软件进行数据包捕获。

2、在 PC1 协议分析软件工具栏中的 TCP 连接工具中连接到 PC2 的 FTP 服务器并发送 dir 命令，如下图所示。

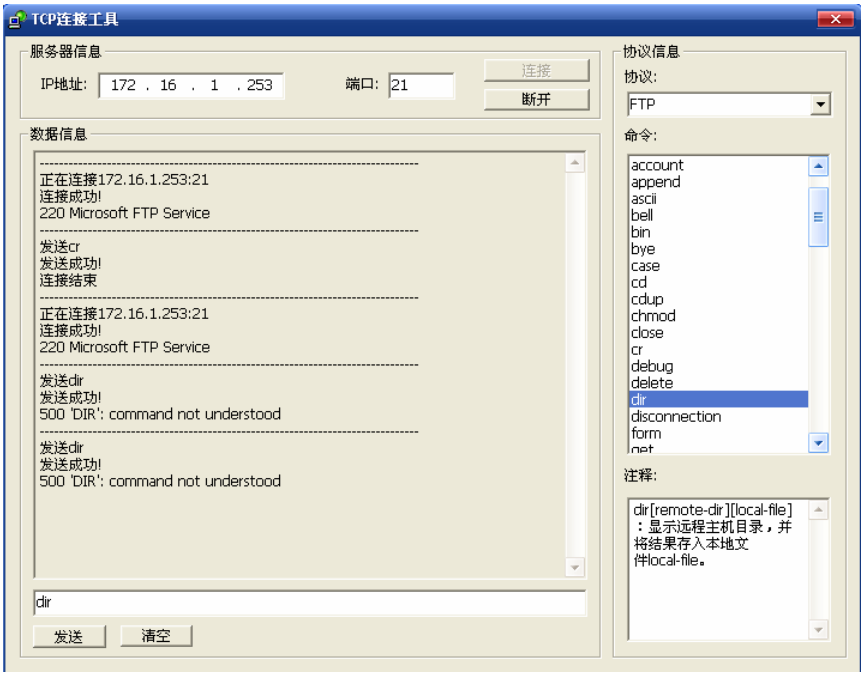

图 4-16 发送 FTP 命令

3、分析捕获到的 FTP 数据包，如下图所示。

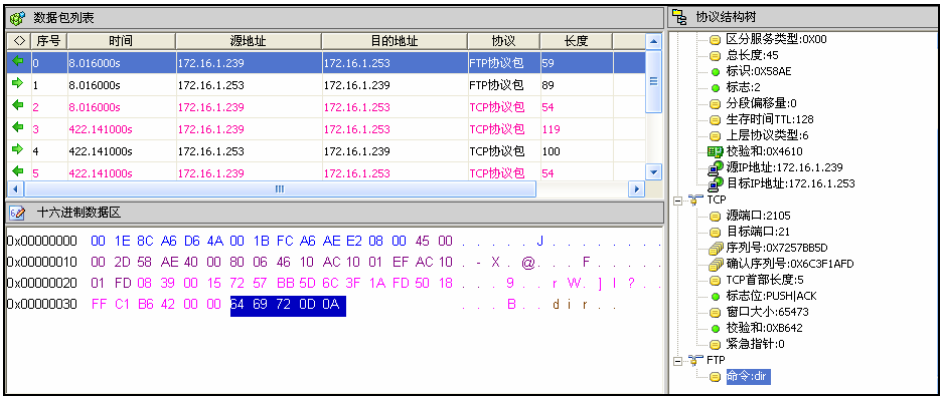

图 4-17 发送 FTP 命令

分析上图中 TCP 数据段首部，可以看到序列号为 0X7257BB5D，数据部分长度为 5 字节。再查看从 PC2 会返回的确认数据段，如下图所示。

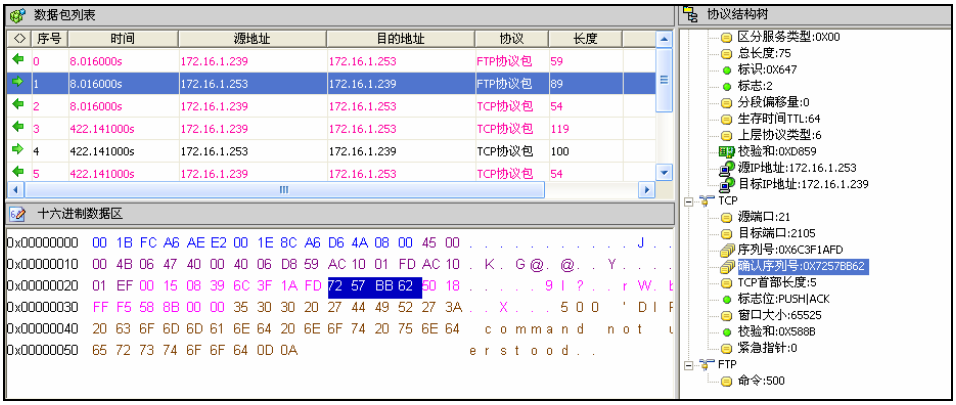

图 4-18 TCP 确认报文

查看上图中 TCP 数据段的报头部分，确认序号为 0X7257BB62，因为 0X7257BB5D+5=0X7257BB62，因此，此确认序号的含义为上一个发送的 TCP 数据段信息全部处理，发送端可以发送 0X7257BB62 以后的数据，此即是 TCP 确认机制的过程。

步骤四：查看 TCP 连接超时重传过程

1、查看 PC1 中 ARP 缓存记录，确保有 PC2 中 ARP 记录，如下图所示。

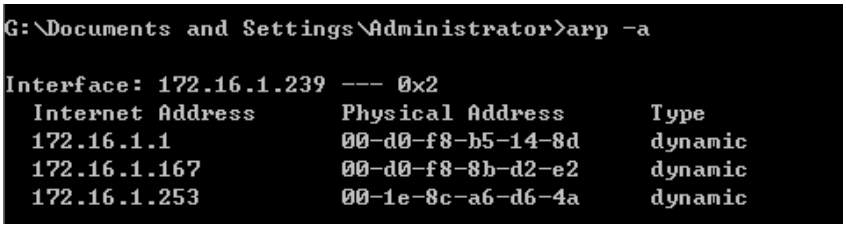

图 4-19 查看 PC1 中 ARP 缓存记录

2、将 PC2 从网络中断开，确保 PC2 不会对 PC1 发送的 TCP 连接请求进行回应。

3、在 PC1 中开启协议分析软件，进行数据包捕获。

4、在 PC1 中用工具栏中的 TCP 连接工具对 PC2 的 FTP 服务发起连接，如下图所示。

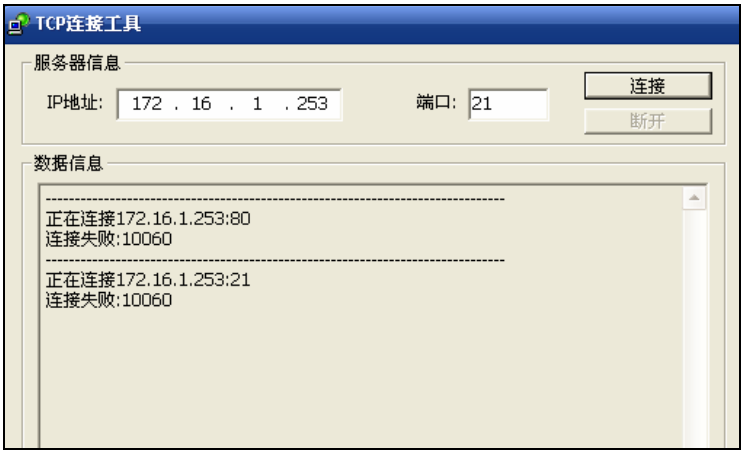

图 4-20 TCP 连接工具发起连接

5、在 PC1 中分析捕获的 TCP 数据段，如下图所示。

图 4-21 TCP 超时重传数据段

从上图中可以看到，在发出 SYN 位置 1 的 TCP 连接请求没有得到相应后，连接工具又发送了第二个相同的 SYN 位置 1 的 TCP 连接请求，进行重传，确定数据段为重传数据段可以通过 TCP 首部中的序列号确认，例如本例中，重传数据段中的序列号均为 0XA82D33B5。

【思考问题】

1、TCP 在建立连接时为什么需要 3 次握手，而断开连接是需要 4 次握手？

2、请举例说明日常应用中，哪些应用在传输层采用 TCP，哪些应用在传输层采用 UDP？

3、当出现超时没有收到确认报文时，TCP 连接默认会进行几次重传？