第五部分.3
TCP建立与终止

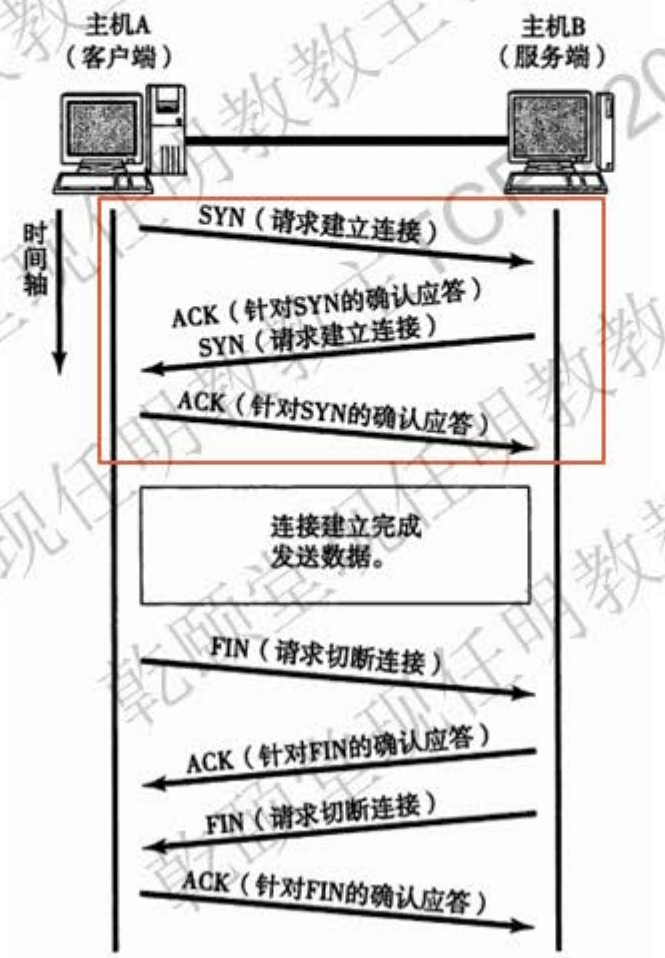
乾颐堂现任明教教主TCPIP2017

TCP连接的建立与终止

- TCP是一个面向连接的协议。无论哪一方向另一方发送数据之前，都必须先在双方之间建立一条连接。
- 这种两端间连接的建立与无连接协议如UDP不同。UDP向另一端发送数据报时，无需任何预先的握手。

乾颐堂现任明教教主TCPIP2017

三次握手建立连接



乾颐堂现任明教教主TCPIP2017

三次握手详细介绍

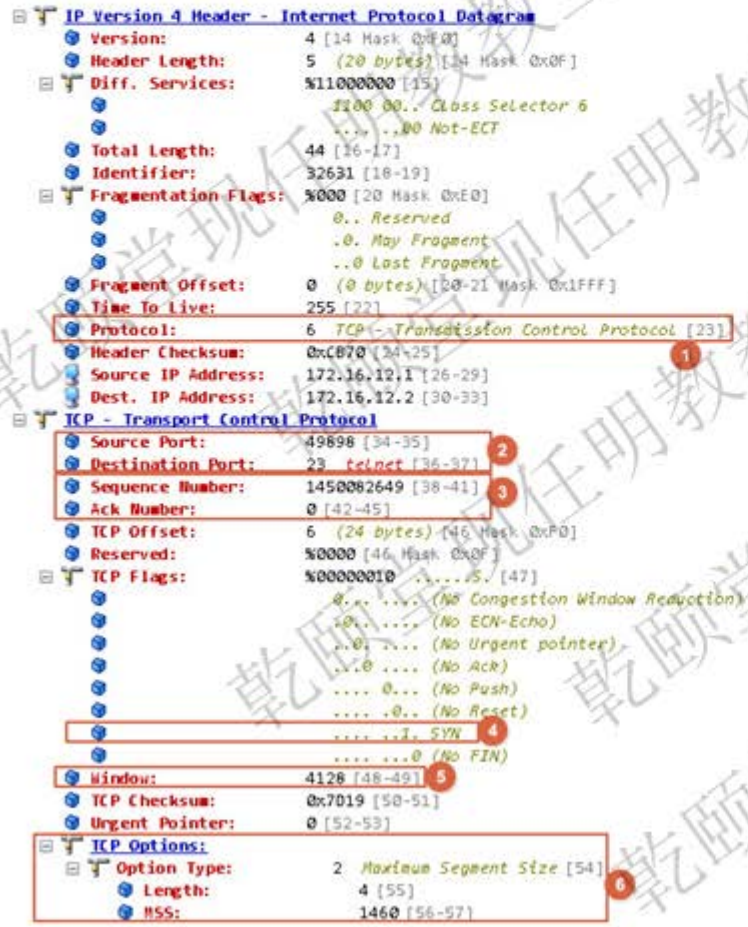
TCP用三路握手（three-way handshake）过程创建一个连接。在连接创建过程中，很多参数要被初始化，例如序号被初始化以保证按序传输和连接的强壮性。

一对终端同时初始化一个它们之间的连接是可能的。但通常是由一端打开一个套接字（socket）然后监听来自另一方的连接，这就是通常所指的被动打开（passive open）。服务器端被被动打开以后，用户端就能开始创建主动打开（active open）。

- 客户端通过向服务器端发送一个SYN来创建一个主动打开，作为三次握手的一部分。客户端把这段连接的序号设定为随机数A。
- 服务器端应当为一个合法的SYN回送一个SYN/ACK。ACK的确认码应为A+1，SYN/ACK包本身又有一个随机序号B。
- 最后，客户端再发送一个ACK。当服务端受到这个ACK的时候，就完成了三次握手，并进入了连接创建状态。此时包序号被设定为收到的确认号A+1，而响应则为B+1。

现任明教教主
乾颐堂TCP/IP 2017

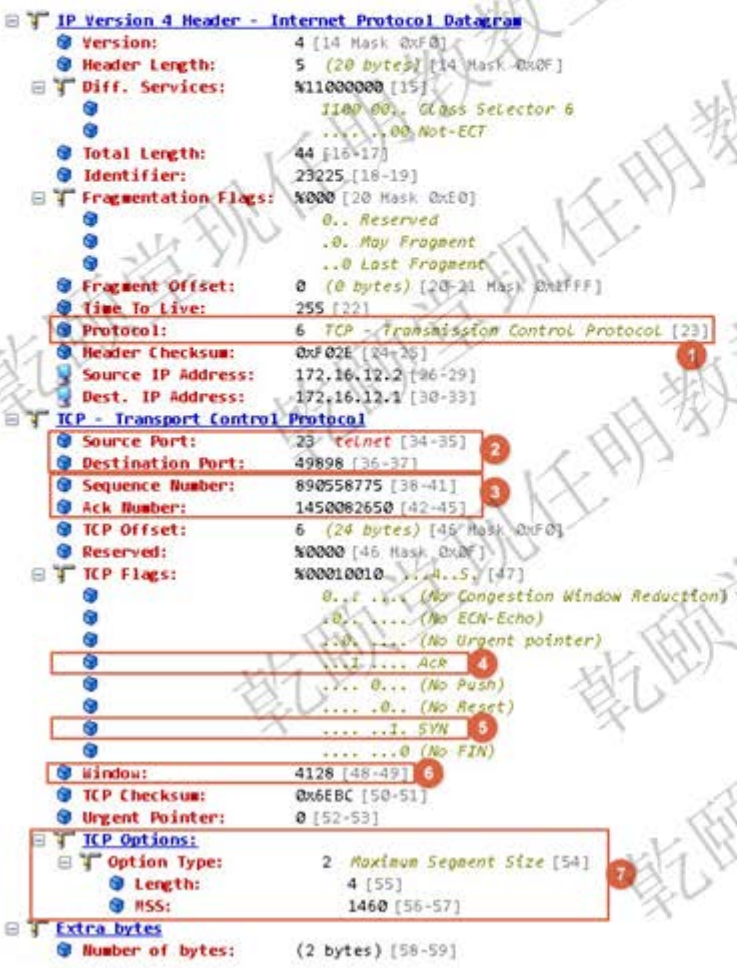
SYN



1.IP协议号为6
2.源端口为大于1023的随机端口
目的端口为知名端口（TCP/23）
3.序列号为，初始化序列号A=1450082649
确认序列号为0
4.SYN Flag被置位
5.窗口大小为4128
6.TCP Option MSS 1460

乾颐堂现任明教教主TCPIP2017

SYN+ACK



1.IP协议号为6
2.源端口为知名端口（TCP/23）
目的端口为大于1023的随机端口
3.序列号为，初始化序列号B=890558775
确认序列号为A+1=1450082649+1
4.ACK Flag被置位
5.SYN Flag被置位
6.窗口大小为4128
7.TCP Option MSS 1460

乾颐堂现任明教教主 TCPIP2017

现任明教教主
乾颐堂TCP/IP 2017

第五部分.3:TCP建立与终止

ACK

```
IP Version 4 Header - Internet Protocol Datagram
  Version:              4 [14 Mask 0xF0]
  Header Length:        5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:       %11000000 [15]
                          1100 00.. Class Selector 6
                          .... ..00 Not-ECT
  Total Length:         40 [16-17]
  Identifier:           32632 [18-19]
  Fragmentation Flags:  %000 [20 Mask 0xE0]
                          0.. Reserved
                          .0. May Fragment
                          ..0 Last Fragment
  Fragment Offset:      0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:         255 [22]
  Protocol:             6  TCP - Transmission Control Protocol [23]
  Header Checksum:      0xCB73 [24-25]
  Source IP Address:    172.16.12.1 [26-29]
  Dest. IP Address:     172.16.12.2 [30-33]
TCP - Transport Control Protocol
  Source Port:          49898 [34-35]
  Destination Port:     23  telnet [36-37]
  Sequence Number:      1450082650 [38-41]
  Ack Number:           890558776 [42-45]
  TCP Offset:           5  (20 bytes) [46 Mask 0xF0]
  Reserved:             %0000 [46 Mask 0x0F]
  TCP Flags:            %00010000 ...A.... [47]
                          0... .... (No Congestion Window Reduction)
                          .0.. .... (No ECN-Echo)
                          ..0. .... (No Urgent pointer)
                          ...1 .... ACK
                          .... 0... (No Push)
                          .... .0.. (No Reset)
                          .... ..0. (No SYN)
                          .... ...0 (No FIN)
  Window:               4128 [48-49]
  TCP Checksum:         0x8679 [50-51]
  Urgent Pointer:       0 [52-53]
  No TCP Options
Extra bytes
  Number of bytes:      (6 bytes) [54-59]
```

1.IP协议号为6
2.源端口为大于1023的随机端口
目的端口为知名端口（TCP/23）
3.序列号为A+1=1450082649+1
确认序列号为B+1=890558775+1
4.ACK Flag被置位
5.窗口大小为4128

乾颐堂现任明教教主TCPIP2017

数据传输

在TCP的数据传送状态，很多重要的机制保证了TCP的可靠性和强壮性。它们包括：使用序号，对收到的TCP报文段进行排序以及检测重复的数据；使用校验和来检测报文段的错误；使用确认和计时器来检测和纠正丢包或延时。

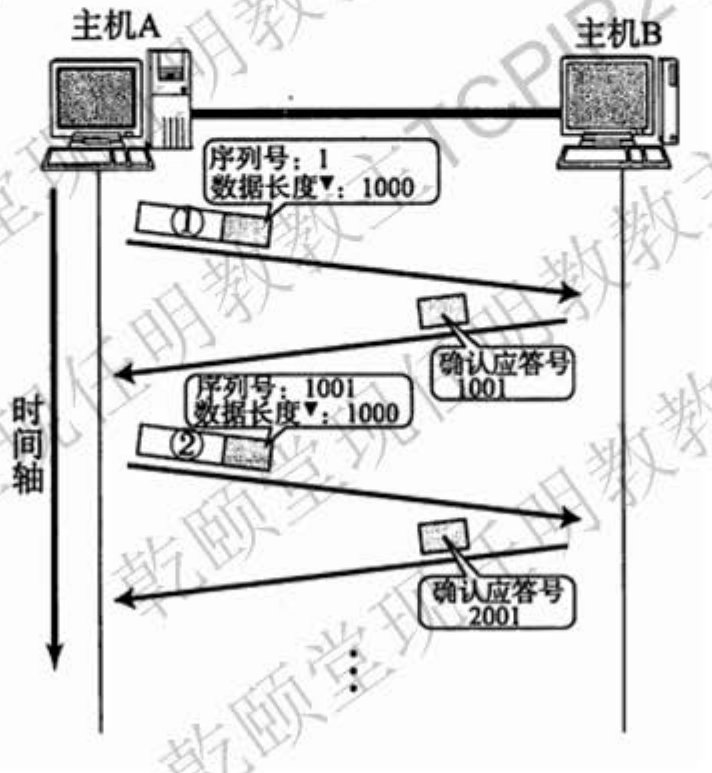
序列号和确认

在TCP的连接创建状态，两个主机的TCP层间要交换初始序号（ISN：initial sequence number）。这些序号用于标识字节流中的数据，并且还是对应用层的数据字节进行记数的整数。通常在每个TCP报文段中都有一对序号和确认号。TCP报文发送者认为自己的字节编号为序号，而认为接收者的字节编号为确认号。TCP报文的接收者为了确保可靠性，在接收到一定数量的连续字节流后才发送确认。这是对TCP的一种扩展，通常称为选择确认（Selective Acknowledgement）。选择确认使得TCP接收者可以对乱序到达的数据块进行确认。每一个字节传输过后，ISN号都会递增1。

通过使用序号和确认号，TCP层可以把收到的报文段中的字节按正确的顺序交付给应用层。序号是32位的无符号数，在它增大到232-1时，便会回绕到0。对于ISN的选择是TCP中关键的一个操作，它可以确保强壮性和安全性。

数据传输示意图

· 序列号与确认应答号



乾颐堂现任明教教主TCPIP2017

数据传输抓包分析

```
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [14 Mask 0xF0]
  Header Length:          5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:         %11000000 [15]
                            1100 00.. Class Selector 6
                            .... ..00 Not-ECT
  Total Length:           41 [16-17]
  Identifier:             32648 [18-19]
  Fragmentation Flags:    %000 [20 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:           255 [22]
  Protocol:               6  TCP - Transmission Control Protocol [23]
  Header Checksum:        0xCB62 [24-25]
  Source IP Address:      172.16.12.1 [26-29]
  Dest. IP Address:       172.16.12.2 [30-33]
TCP - Transport Control Protocol
  Source Port:            49898 [34-35]                          (1)
  Destination Port:       23  telnet [36-37]                    (1)
  Sequence Number:        1450082687 [38-41]                     (2)
  Ack Number:             890558848 [42-45]
  TCP Offset:             5  (20 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00011000  ...AP... [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...1 .... Ack                        (3)
                            .... 1... Push
                            .... .0.. (No Reset)
                            .... ..0. (No SYN)
                            .... ...0 (No FIN)
  Window:                 4056 [48-49]
  TCP Checksum:           0x134B [50-51]
  Urgent Pointer:         0 [52-53]
  No TCP Options
TELNET - Network Virtual Terminal                                (4)
  Line  1:                s [54 Mask 0xFFFFFFFF]
```

2.序列号A=1450082687

3.每一个包都有ACK

4.一个字节数据“s”

```
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [14 Mask 0xF0]
  Header Length:          5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:         %11000000 [15]
                            1100 00.. Class Selector 6
                            .... ..00 Not-ECT
  Total Length:           41 [16-17]
  Identifier:             23238 [18-19]
  Fragmentation Flags:    %000 [20 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:           255 [22]
  Protocol:               6  TCP - Transmission Control Protocol [23]
  Header Checksum:        0xF024 [24-25]
  Source IP Address:      172.16.12.2 [26-29]
  Dest. IP Address:       172.16.12.1 [30-33]
TCP - Transport Control Protocol
  Source Port:            23  telnet [34-35]                     (1)
  Destination Port:       49898 [36-37]                          (1)
  Sequence Number:        890558848 [38-41]
  Ack Number:             1450082688 [42-45]                     (2)
  TCP Offset:             5  (20 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00011000  ...AP... [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...1 .... Ack                        (3)
                            .... 1... Push
                            .... .0.. (No Reset)
                            .... ..0. (No SYN)
                            .... ...0 (No FIN)
  Window:                 4090 [48-49]
  TCP Checksum:           0x1328 [50-51]
  Urgent Pointer:         0 [52-53]
  No TCP Options
TELNET - Network Virtual Terminal                                (4)
  Line  1:                s [54 Mask 0xFFFFFFFF]
```

2.确认序列号
A+1=1450082687+1

3.每一个包都有ACK

4.回显数据“s”

乾颐堂现任明教教主 TCP/IP 2017

连接的终结

乾颐堂现任明教教主TCPIP2017

连接终结详细介绍

The connection termination phase uses **a four-way handshake（四次握手）**, **with each side of the connection terminating independently（每一端连接的终结是独立的）**. When an endpoint wishes to stop its half of the connection, it transmits a FIN packet, which the other end acknowledges with an ACK. Therefore, a typical tear-down requires a pair of FIN and ACK segments from each TCP endpoint. After the side that sent the first FIN has responded with the final ACK, it waits for a timeout before finally closing the connection, during which time the local port is unavailable for new connections; this prevents confusion due to delayed packets being delivered during subsequent connections.

A connection can be **"half open"（一般叫做半闭）** in which case one side has terminated its end, but the other has not. The side that has terminated can no longer send any data into the connection, but the other side can. The terminating side should continue reading the data until the other side terminates as well.

It is also possible to terminate the connection by a **3-way handshake（两次FIN交换更为准确）**, when host A sends a FIN and host B replies with a FIN & ACK (merely combines 2 steps into one) and host A replies with an ACK.

第一次FIN交换

接受方
B ↓ ↑ A
发起方

FIN位有一个字节的“重量”

```
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [14 Mask 0xF0]
  Header Length:          5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:         %11000000 [15]
                            1100 00.. Class Selector 6
                            .... ..00 Not-ECT
  Total Length:           40 [16-17]
  Identifier:             23263 [18-19]
  Fragmentation Flags:    %000 (20 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:           255 [22]
  Protocol:               6  TCP - Transmission Control Protocol [23]
  Header Checksum:        0xF00C [24-25]
  Source IP Address:      172.16.12.2 [26-29]
  Dest. IP Address:       172.16.12.1 [30-33]
TCP - Transport Control Protocol
  Source Port:            23  telnet [34-35]      (1)
  Destination Port:       49898 [36-37]
  Sequence Number:        890559455 [38-41]       (2)
  Ack Number:             1450082711 [42-45]
  TCP Offset:             5  (20 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00011001  ...AP..F [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...1 .... Ack           (3)
                            .... 1... Push
                            .... .0.. (No Reset)
                            .... ..0. (No SYN)
                            .... ...1 FIN           (4)
  Window:                 4067 [48-49]
  TCP Checksum:           0x83C9 [50-51]
  Urgent Pointer:         0 [52-53]
  No TCP Options
Extra bytes
  Number of bytes:        (6 bytes) [54-59]
```

1.端口号说明是接收方主动断开连接

2.序列号B=890559455
确认序列号A=1450082711

3.ACK Flag置位

4.FIN Flag置位

```
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [14 Mask 0xF0]
  Header Length:          5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:         %11000000 [15]
                            1100 00.. Class Selector 6
                            .... ..00 Not-ECT
  Total Length:           40 [16-17]
  Identifier:             32675 [18-19]
  Fragmentation Flags:    %000 [20 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:           255 [22]
  Protocol:               6  TCP - Transmission Control Protocol [23]
  Header Checksum:        0xCB48 [24-25]
  Source IP Address:      172.16.12.1 [26-29]
  Dest. IP Address:       172.16.12.2 [30-33]
TCP - Transport Control Protocol
  Source Port:            49898 [34-35]
  Destination Port:       23  telnet [36-37]     (1)
  Sequence Number:        1450082711 [38-41]      (2)
  Ack Number:             890559456 [42-45]
  TCP Offset:             5  (20 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00010000  ...A.... [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...1 .... Ack           (3)
                            .... 0... (No Push)
                            .... .0.. (No Reset)
                            .... ..0. (No SYN)
                            .... ...0 (No FIN)
  Window:                 3449 [48-49]
  TCP Checksum:           0x863B [50-51]
  Urgent Pointer:         0 [52-53]
  No TCP Options
Extra bytes
  Number of bytes:        (6 bytes) [54-59]
```

2.序列号A=1450082711
确认序列号
B+1=890559455+1

3.ACK Flag置位

乾颐堂现任明教教主TCPIP2017

现任明教教主
乾颐堂TCP/IP 2017

第二次FIN交换

接受方
B ↓ ↑ A
发起方

FIN位有一个字节的“重量”

```
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [14 Mask 0xF0]
  Header Length:          5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:         %11000000 [15]
                            1100 00.. Class Selector 6
                            .... ..00 Not-ECT
  Total Length:           40 [16-17]
  Identifier:             32676 [18-19]
  Fragmentation Flags:    %000 [20 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:           255 [22]
  Protocol:               6  TCP - Transmission Control Protocol [23]
  Header Checksum:        0xCB47 [24-25]
  Source IP Address:      172.16.12.1 [26-29]
  Dest. IP Address:       172.16.12.2 [30-33]
TCP - Transport Control Protocol
  Source Port:            49898 [34-35]                    (1)
  Destination Port:       23  telnet [36-37]
  Sequence Number:        1450082711 [38-41]               (2)
  Ack Number:             890559456 [42-45]
  TCP Offset:             5  (20 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00011001  ...AP..F [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...1 .... Ack                (3)
                            .... 1... Push
                            .... .0.. (No Reset)
                            .... ..0. (No SYN)
                            .... ...1 FIN                (4)
  Window:                 3449 [48-49]
  TCP Checksum:           0x8632 [50-51]
  Urgent Pointer:         0 [52-53]
  No TCP Options
Extra bytes
  Number of bytes:        (6 bytes) [54-59]
```

1.端口号说明是发起方主动断开连接

2.序列号A=1450082711
确认序列号B+1=890559456

3.ACK Flag置位

4.FIN Flag置位

```
IP Version 4 Header - Internet Protocol Datagram
  Version:                4 [14 Mask 0xF0]
  Header Length:          5  (20 bytes) [14 Mask 0x0F]
  Diff. Services:         %11000000 [15]
                            1100 00.. Class Selector 6
                            .... ..00 Not-ECT
  Total Length:           40 [16-17]
  Identifier:             23264 [18-19]
  Fragmentation Flags:    %000 [20 Mask 0xE0]
                            0.. Reserved
                            .0. May Fragment
                            ..0 Last Fragment
  Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
  Time To Live:           255 [22]
  Protocol:               6  TCP - Transmission Control Protocol [23]
  Header Checksum:        0xF008 [24-25]
  Source IP Address:      172.16.12.2 [26-29]
  Dest. IP Address:       172.16.12.1 [30-33]
TCP - Transport Control Protocol
  Source Port:            23  telnet [34-35]               (1)
  Destination Port:       49898 [36-37]
  Sequence Number:        890559456 [38-41]                (2)
  Ack Number:             1450082712 [42-45]
  TCP Offset:             5  (20 bytes) [46 Mask 0xF0]
  Reserved:               %0000 [46 Mask 0x0F]
  TCP Flags:              %00010000  ...A.... [47]
                            0... .... (No Congestion Window Reduction)
                            .0.. .... (No ECN-Echo)
                            ..0. .... (No Urgent pointer)
                            ...1 .... Ack                (3)
                            .... 0... (No Push)
                            .... .0.. (No Reset)
                            .... ..0. (No SYN)
                            .... ...0 (No FIN)
  Window:                 4067 [48-49]
  TCP Checksum:           0x83D0 [50-51]
  Urgent Pointer:         0 [52-53]
  No TCP Options
Extra bytes
  Number of bytes:        (6 bytes) [54-59]
```

2.序列号B+1=890559456
确认序列号
A+1=1450082711+1

3.ACK Flag置位

乾颐堂现任明教教主 TCP/IP 2017

现任明教教主
乾颐堂TCP/IP 2017

异常终止（Reset）

1.建立连接
2.VM断开接口
3.清除TCP会话
4.发起流量
5.会话被Rest

2.序列号A=1260944976
确认序列号B=612296016

3.ACK Flag置位

4.发送数据“回车”

2.序列号B=612296016
确认序列号A=0

3.Reset Flag置位

乾颐堂现任明教教主 TCP/IP 2017