

1

TCP数据分析实验

冯巾松

fengjinsong@tongji.edu.cn

TCP概述

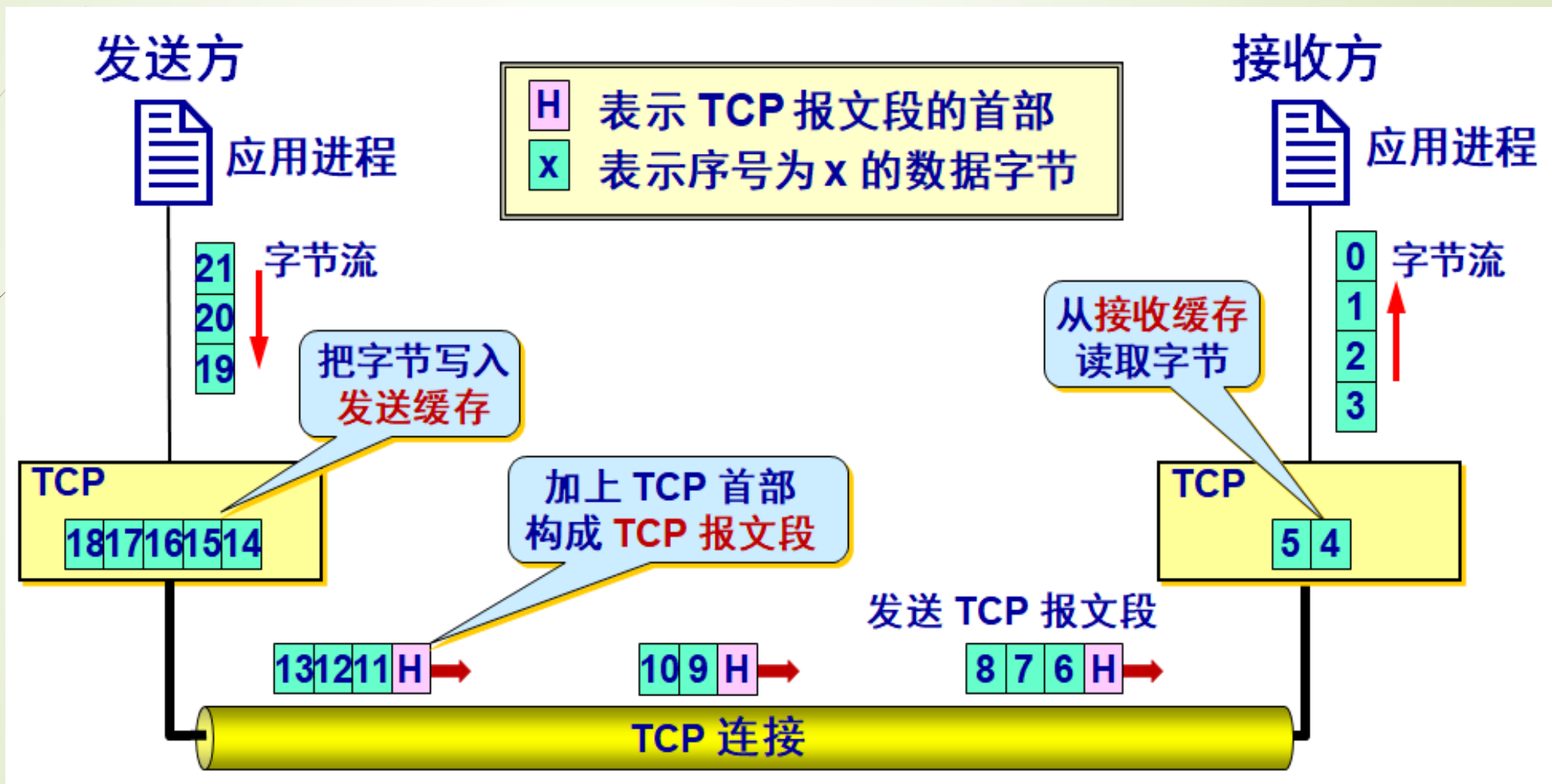
2

➡ TCP是传输层的协议，功能是为在IP的数据报服务之上增加了最基本的服务：复用和分用以及差错检测。

➡ TCP是一个基于连接的四层协议，提供全双工、可靠地传输系统。它能够保证数据被远程主机接收。并且能够为高层协议提供flow-controlled 服务。空间上，TCP 需要在端系统中维护连接状态，需要一定的开销。此连接装入包括接收和发送缓存，拥塞控制参数和序号与确认号的参数。

TCP 面向字节流示意

3



TCP的报文格式

➡ TCP报文是TCP层传输的数据单元，也叫报文段



TCP报文字段

- 源端口：源端口和IP地址的作用是标识报文的返回地址。
- 目的端口：端口指明接收方计算机上的应用程序接口。

TCP报头中的源端口号和目的端口号同IP数据报中的源IP与目的IP唯一确定一条TCP连接

TCP报文字段

- **序号和确认序号**：是TCP可靠传输的关键部分。
- **序号**是本报文段发送的数据组的第一个字节的序号。在TCP传送的流中，每一个字节一个序号。例如：一个报文段的序号为300，此报文段数据部分共有100字节，则下一个报文段的序号为400。所以序号确保了TCP传输的有序性。
- **确认序号**，即ACK，指明下一个期待收到的字节序号，表明该序号之前的所有数据已经正确无误的收到。确认号只有当ACK标志为1时才有效。比如建立连接时，SYN报文的ACK标志位为0。

TCP报文字段

7

- ➡ **数据偏移 / 首部长度**：4bits。由于首部可能含有可选项内容，因此TCP报头的长度是不确定的，报头不包含任何任选字段则长度为20字节，4位首部长度字段所能表示的最大值为1111，转化为10进制为15， $15 * 32 / 8 = 60$ ，故报头最大长度为60字节。
- ➡ **首部长度也叫数据偏移**，是因为首部长度实际上指示了数据区在报文段中的起始偏移值。
- ➡ **保留**：为将来定义新的用途保留，现在一般置0。

TCP报文字段

8

➡ **控制位：**URG ACK PSH RST SYN FIN，共 6 个，每个标志位表示一个控制功能。

1) URG：紧急指针标志，为1时表示紧急指针有效，为0则忽略紧急指针。

2) ACK：确认序号标志，为1时表示确认号有效，为0表示报文中不含确认信息，忽略确认号字段。

3) PSH：push标志，为1表示是带有push标志的数据，指示接收方在接收到该报文段以后，应尽快将这个报文段交给应用程序，而不是在缓冲区排队。

TCP报文字段

9

4) RST: 重置连接标志, 用于重置由于主机崩溃或其他原因而出现错误的连接。或者用于拒绝非法的报文段和拒绝连接请求。

5) SYN: 同步序号, 用于建立连接过程, 在连接请求中, $SYN=1$ 和 $ACK=0$ 表示该数据段没有使用捎带的确认域, 而连接应答捎带一个确认, 即 $SYN=1$ 和 $ACK=1$ 。

6) FIN: finish标志, 用于释放连接, 为1时表示发送方已经没有数据发送了, 即关闭本方数据流

TCP报文字段

10

- ➡ **窗口**：滑动窗口大小，用来告知发送端接受端的缓存大小，以此控制发送端发送数据的速率，从而达到流量控制。窗口大小是一个16bit 字段，因而窗口大小最大为65535。
- ➡ **校验和**：奇偶校验，此校验和是对整个的TCP报文段，包括TCP头部和TCP数据，以16位字进行计算所得。由发送端计算和存储，并由接收端进行验证。

TCP报文字段

11

- **紧急指针**：只有当URG 标志置 1 时紧急指针才有效。紧急指针是一个正的偏移量，和顺序号字段中的值相加表示紧急数据最后一个字节的序号。TCP的紧急方式是发送端向另一端发送紧急数据的一种方式。
- **选项和填充**：最常见的可选字段是最长报文大小，又称为MSS（Maximum Segment Size），每个连接方通常都在通信的第一个报文段（为建立连接而设置SYN标志为1的那个段）中指明这个选项，它表示本端所能接受的最大报文段的长度。选项长度不一定是32位的整数倍，所以要加填充位，即在这个字段中加入额外的零，以保证TCP头是32的整数倍。

TCP报文字段

12

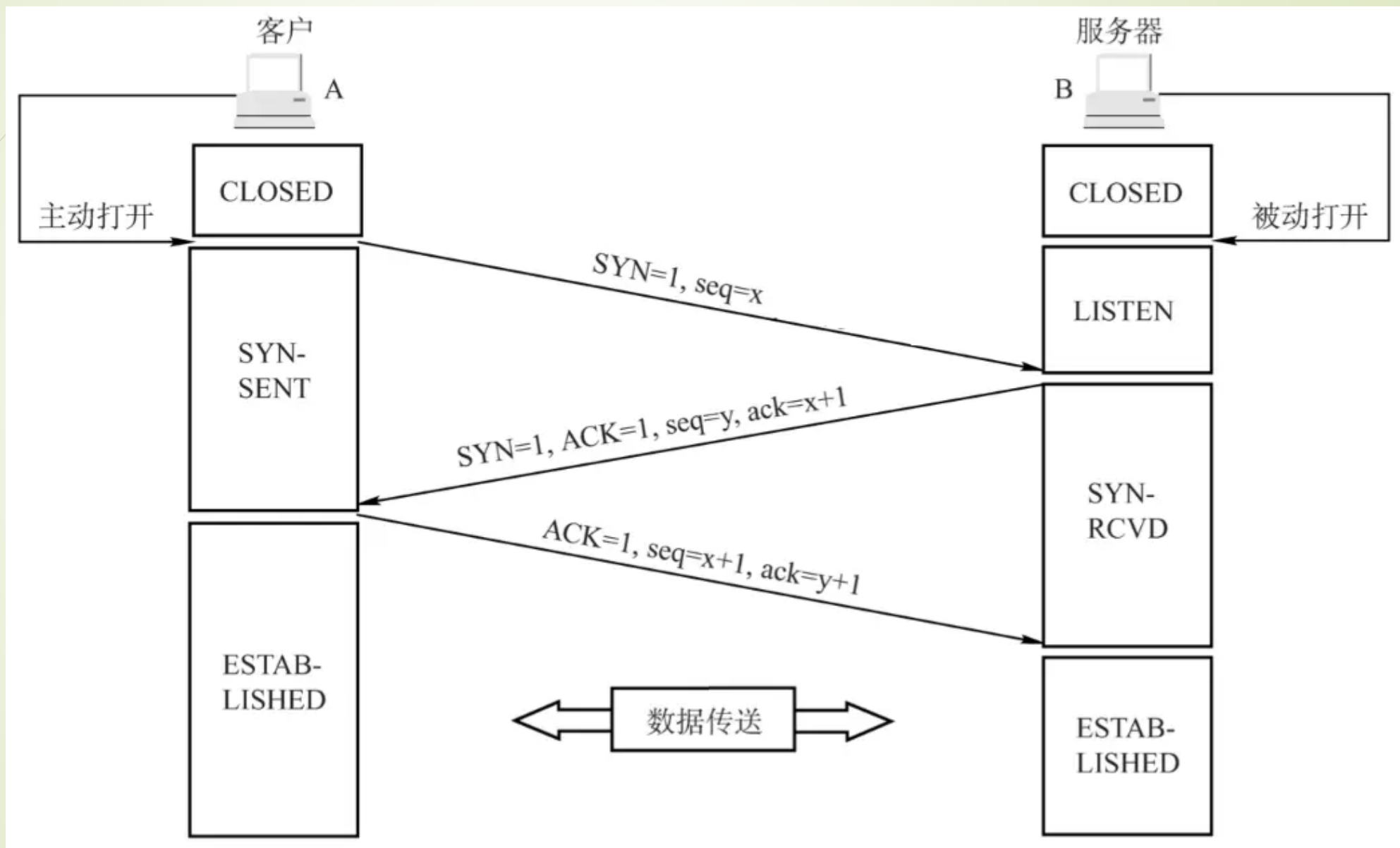
➡ **数据部分：** TCP 报文段中的数据部分是可选的。在一个连接建立和一个连接终止时，双方交换的报文段仅有 TCP 首部。如果一方没有数据要发送，也使用没有任何数据的首部来确认收到的数据。在处理超时的许多情况中，也会发送不带任何数据的报文段。

TCP连接过程

- ➡ TCP连接过程简单一句话概括：“三次握手四次挥手”，实质就是TCP通信的连接和断开。
- ➡ 所谓三次握手(Three-way Handshake)，是指建立一个TCP连接时，需要客户端和服务端总共发送3个包。三次握手的目的是连接服务器指定端口，建立TCP连接，并同步连接双方的序列号和确认号并交换 TCP 窗口大小信息。

TCP 三次握手示意

14



TCP连接过程 - 第一次握手

- ➡ 客户端发送一个TCP的SYN标志位置1的包指明客户打算连接的服务器的端口，以及初始序号X,保存在包头的序列号(Sequence Number)字段里

源端口				目标端口			
X							
接收序号							
偏置值	保留	URG	ACK	PUSH	RESERVED	FIN	窗口
检查和				紧急指针			
任选项+补丁							
用户数据							

TCP连接过程 - 第二次握手

- ➡ 服务器发回确认包(ACK)应答。即SYN标志位和ACK标志位均为1同时，将确认序号(Acknowledgement Number)设置为客户的ISN加以1，即 $X+1$ 。

源端口					目标端口				
Y									
X+1									
偏置值	保留	U R G	1	P S H	R S T	1	F I N	窗口	
检查和					紧急指针				
任选项+补丁									
用户数据									

TCP连接过程 - 第三次握手

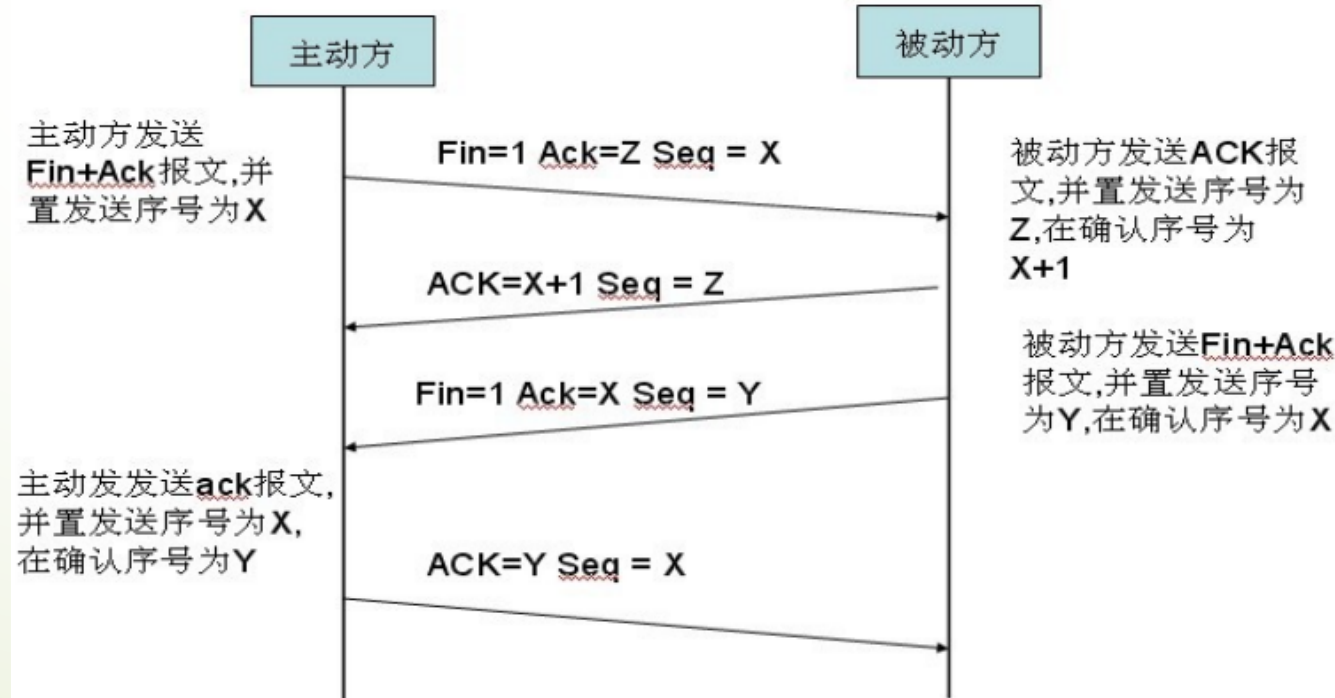
- ➡ 客户端再次发送确认包(ACK) SYN标志位为0, ACK 标志位为1.并且把服务器发来ACK的序号字段+1, 放在确定字段中发送给对方。并且在数据段放写 ISN的+1。

源端口				目标端口			
发送顺序号							
Y+1							
偏置值	保留	URG	1	PSH	SYN	FIN	窗口
检查和				紧急指针			
任选项+补丁							
DATA (X+1)							

TCP连接过程 - 四次挥手

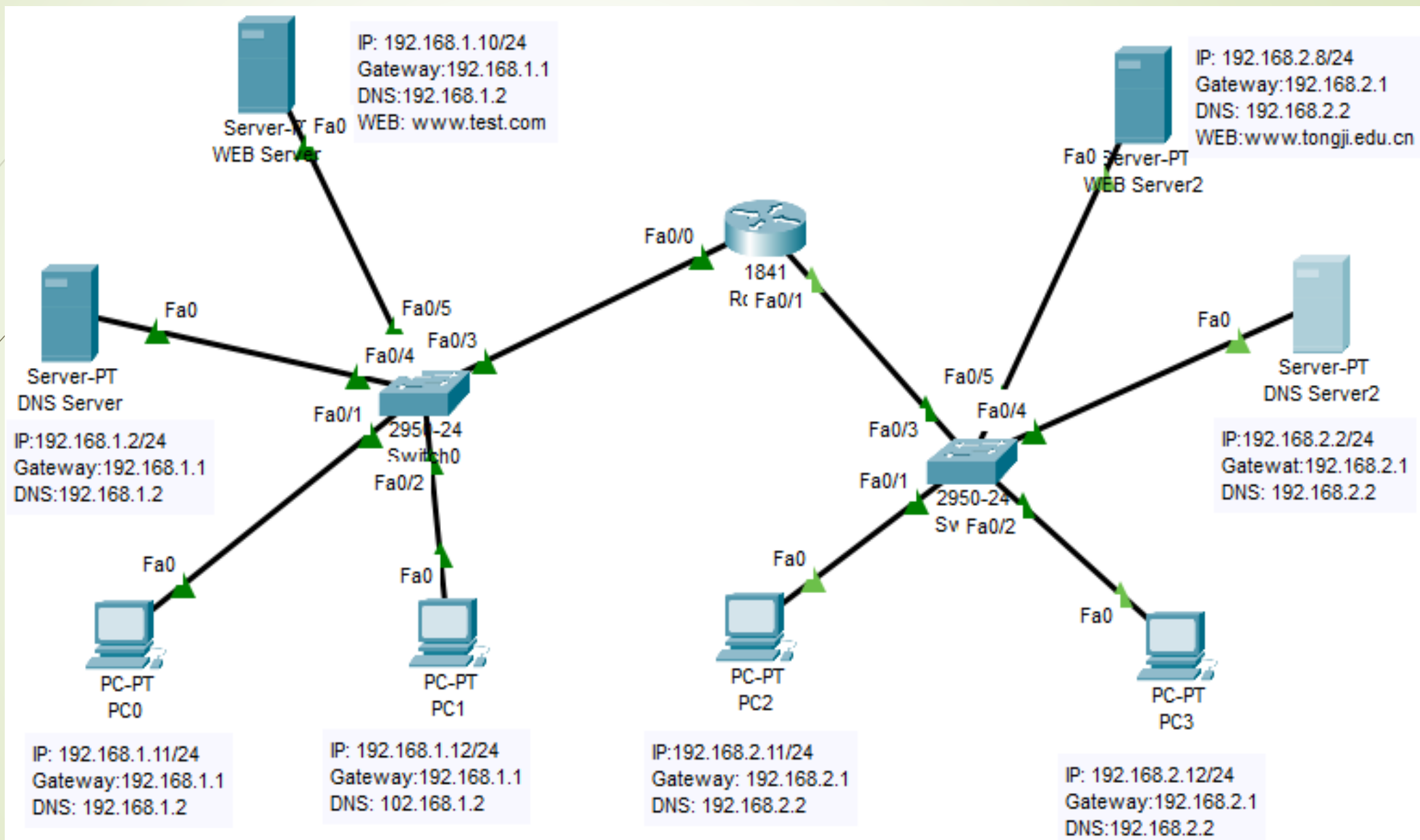
- TCP连接的拆除需要发送四个包，因此称为四次挥手(four-way handshake)。
- 客户端或服务器均可主动发起挥手动作，在socket编程中，任何一方执行close()操作即可产生挥手操作。

TCP 四次挥手



实验网络拓扑图

22




PT软件分析TCP报文

■ 搭建网络结构图

- 1) 设置WEB服务器和简单的DNS服务器；
- 2) 打开PC0浏览器，输入配置Web服务器的Web 地址，如www.tongji.edu.cn或www.test.com，产生TCP数据报文

PT软件分析TCP报文

24



PDU Information at Device: PC0

At Device: PC0
Source: PC0
Destination: 192.168.2.8

OSI Model **Outbound PDU Details**

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1026, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.8
Layer2	Layer 2: Ethernet II Header 0050.0FAB.0418 >> 0005.5E96.9C01
Layer1	Layer 1: Port(s):

1. TCP accepts a window size up to 65535 bytes.
2. TCP adds Maximum Segment Size Option to the TCP SYN header with Maximum Segment Size equal to 1460 bytes.
3. The device sends a TCP SYN segment.
4. Sent segment information: the sequence number 0, the ACK number 0, and the data length 24.

Challenge Me << Previous Layer Next Layer >>

PT软件分析TCP报文

25

PDU Information at Device: PC0

OSI Model Outbound PDU Details

PDU Formats

SRC IP: 192.168.1.11	
DST IP: 192.168.2.8	
OPT: 0x0	0x0
DATA (VARIABLE LENGTH)	

TCP

0	16	31	Bits
SRC PORT: 1026		DEST PORT: 80	
SEQUENCE NUM: 0			
ACK NUM: 0			
OFF.	RES.	SYN	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

PT软件分析TCP报文

26

PDU Information at Device: Switch0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

SRC IP: 192.168.1.11	
DST IP: 192.168.2.8	
OPT: 0x0	0x0
DATA (VARIABLE LENGTH)	

TCP

0 16 31 Bits			
SRC PORT: 1029 DEST PORT: 80			
SEQUENCE NUM: 0			
ACK NUM: 0			
OFF.	RES.	SYN	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION		PADDING	
DATA (VARIABLE)			

PDU Information at Device: Router0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

4	IHL	DSCP: 0x0	TL: 44
ID: 0x2		0x2	0x0
TTL: 127	PRO: 0x6		CHKSUM
SRC IP: 192.168.2.8			
DST IP: 192.168.1.11			
OPT: 0x0		0x0	
DATA (VARIABLE LENGTH)			

TCP

0 16 31 Bits			
SRC PORT: 80 DEST PORT: 1031			
SEQUENCE NUM: 0			
ACK NUM: 1			
OFF.	RES.	SYN + ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION		PADDING	
DATA (VARIABLE)			

PT软件分析TCP报文

27

PDU Information at Device: Switch0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

4	4	IHL	DSCP: 0x0	TL: 40
ID: 0x19		0x2	0x0	
TTL: 128	PRO: 0x6	CHKSUM		
SRC IP: 192.168.1.11				
DST IP: 192.168.2.8				
OPT: 0x0		0x0		
DATA (VARIABLE LENGTH)				

TCP

0		16		31		Bits
SRC PORT: 1030		DEST PORT: 80				
SEQUENCE NUM: 1						
ACK NUM: 1						
OFF.	RES.	ACK	WINDOW			
CHECKSUM: 0x0			URGENT POINTER			
OPTION				PADDING		
DATA (VARIABLE)						

PDU Information at Device: PC0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

4	4	IHL	DSCP: 0x0	TL: 40
ID: 0x25		0x2	0x0	
TTL: 128	PRO: 0x6	CHKSUM		
SRC IP: 192.168.1.11				
DST IP: 192.168.2.8				
OPT: 0x0		0x0		
DATA (VARIABLE LENGTH)				

TCP

0		16		31		Bits
SRC PORT: 1028		DEST PORT: 80				
SEQUENCE NUM: 1						
ACK NUM: 1						
OFF.	RES.	ACK	WINDOW			
CHECKSUM: 0x0			URGENT POINTER			
OPTION				PADDING		
DATA (VARIABLE)						

PT软件分析TCP报文

28

PDU Information at Device: Server0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0		16		31		Bits	
SRC PORT: 80				DEST PORT: 1035			
SEQUENCE NUM: 1							
ACK NUM: 103							
OFF.	RES.	PSH + ACK		WINDOW			
CHECKSUM: 0x0				URGENT POINTER			
OPTION				PADDING			
DATA (VARIABLE)							

HTTP

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 369
Content-Type: text/html
Server: PT-Server/5.2
HTTP DATA..
```

PDU Information at Device: Router0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0		16		31		Bits	
SRC PORT: 80				DEST PORT: 1035			
SEQUENCE NUM: 1							
ACK NUM: 103							
OFF.	RES.	PSH + ACK		WINDOW			
CHECKSUM: 0x0				URGENT POINTER			
OPTION				PADDING			
DATA (VARIABLE)							

HTTP

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 369
Content-Type: text/html
Server: PT-Server/5.2
HTTP DATA..
```

PT软件分析TCP报文

29

PDU Information at Device: Switch0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

TTL: 128		PRO: 0x6		CHKSUM	
SRC IP: 192.168.1.11					
DST IP: 192.168.2.8					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

TCP

0		16		31		Bits	
SRC PORT: 1035		DEST PORT: 80					
SEQUENCE NUM: 103							
ACK NUM: 472							
OFF.	RES.	FIN + ACK	WINDOW				
CHECKSUM: 0x0			URGENT POINTER				
OPTION				PADDING			
DATA (VARIABLE)							

PDU Information at Device: Switch1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0		4		8		16		19		31		Bits	
4		IHL		DSCP: 0x0		TL: 40							
ID: 0xf				0x2		0x0							
TTL: 128		PRO: 0x6		CHKSUM									
SRC IP: 192.168.2.8													
DST IP: 192.168.1.11													
OPT: 0x0										0x0			
DATA (VARIABLE LENGTH)													

TCP

0		16		31		Bits	
SRC PORT: 80		DEST PORT: 1035					
SEQUENCE NUM: 472							
ACK NUM: 104							
OFF.	RES.	FIN + ACK	WINDOW				
CHECKSUM: 0x0			URGENT POINTER				
OPTION				PADDING			
DATA (VARIABLE)							

PT软件分析TCP报文

30

PDU Information at Device: PC0

OSI Model Inbound PDU Details Outbound PDU Details

At Device: PC0
Source: PC0
Destination: 192.168.2.8

In Layers

Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 80, Dst Port: 1035
Layer 3: IP Header Src. IP: 192.168.2.8, Dest. IP: 192.168.1.11
Layer 2: Ethernet II Header 0005.5E96.9C01 >> 0005.0FAB.0418
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 1035, Dst Port: 80
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.8
Layer 2: Ethernet II Header 0005.0FAB.0418 >> 0005.5E96.9C01
Layer 1: Port(s): FastEthernet0

1. The device sends a TCP ACK segment.
2. Sent segment information: the sequence number 104, the ACK number 472, and the data length 20.

Challenge Me << Previous Layer Next Layer >>

PDU Information at Device: PC0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0	4	8	16	19	31	Bits
4	4	8	DSCP: 0x0			TL: 40
ID: 0xf			0x2	0x0		
TTL: 127		PRO: 0x6		CHKSUM		
SRC IP: 192.168.2.8						
DST IP: 192.168.1.11						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

TCP

0	16	31	Bits
SRC PORT: 80		DEST PORT: 1035	
SEQUENCE NUM: 472			
ACK NUM: 104			
OFF.	RES.	FIN + ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

PT软件分析TCP报文

31

PDU Information at Device: PC0

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 40			
ID: 0xf			0x2	0x0		
TTL: 127		PRO: 0x6		CHKSUM		
SRC IP: 192.168.2.8						
DST IP: 192.168.1.11						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

TCP

0	16	31	Bits
SRC PORT: 80		DEST PORT: 1035	
SEQUENCE NUM: 472			
ACK NUM: 104			
OFF.	RES.	FIN + ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

PDU Information at Device: PC0

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 40			
ID: 0x34			0x2	0x0		
TTL: 128	PRO: 0x6		CHKSUM			
SRC IP: 192.168.1.11						
DST IP: 192.168.2.8						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

TCP

0	16	31	Bits
SRC PORT: 1035		DEST PORT: 80	
SEQUENCE NUM: 104			
ACK NUM: 472			
OFF.	RES.	ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

PT软件分析TCP报文

32

PDU Information at Device: PC0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 40			
ID: 0xf			0x2	0x0		
TTL: 127		PRO: 0x6	CHKSUM			
SRC IP: 192.168.2.8						
DST IP: 192.168.1.11						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

TCP

0	16	31	Bits
SRC PORT: 80		DEST PORT: 1035	
SEQUENCE NUM: 472			
ACK NUM: 104			
OFF.	RES.	FIN + ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

PDU Information at Device: Server0

OSI Model Inbound PDU Details

PDU Formats

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 40			
ID: 0x34			0x2	0x0		
TTL: 127		PRO: 0x6	CHKSUM			
SRC IP: 192.168.1.11						
DST IP: 192.168.2.8						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

TCP

0	16	31	Bits
SRC PORT: 1035		DEST PORT: 80	
SEQUENCE NUM: 104			
ACK NUM: 472			
OFF.	RES.	ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

PT软件分析TCP报文

33

PDU Information at Device: Server0

OSI Model Inbound PDU Details

At Device: Server0
Source: PC0
Destination: 192.168.2.8

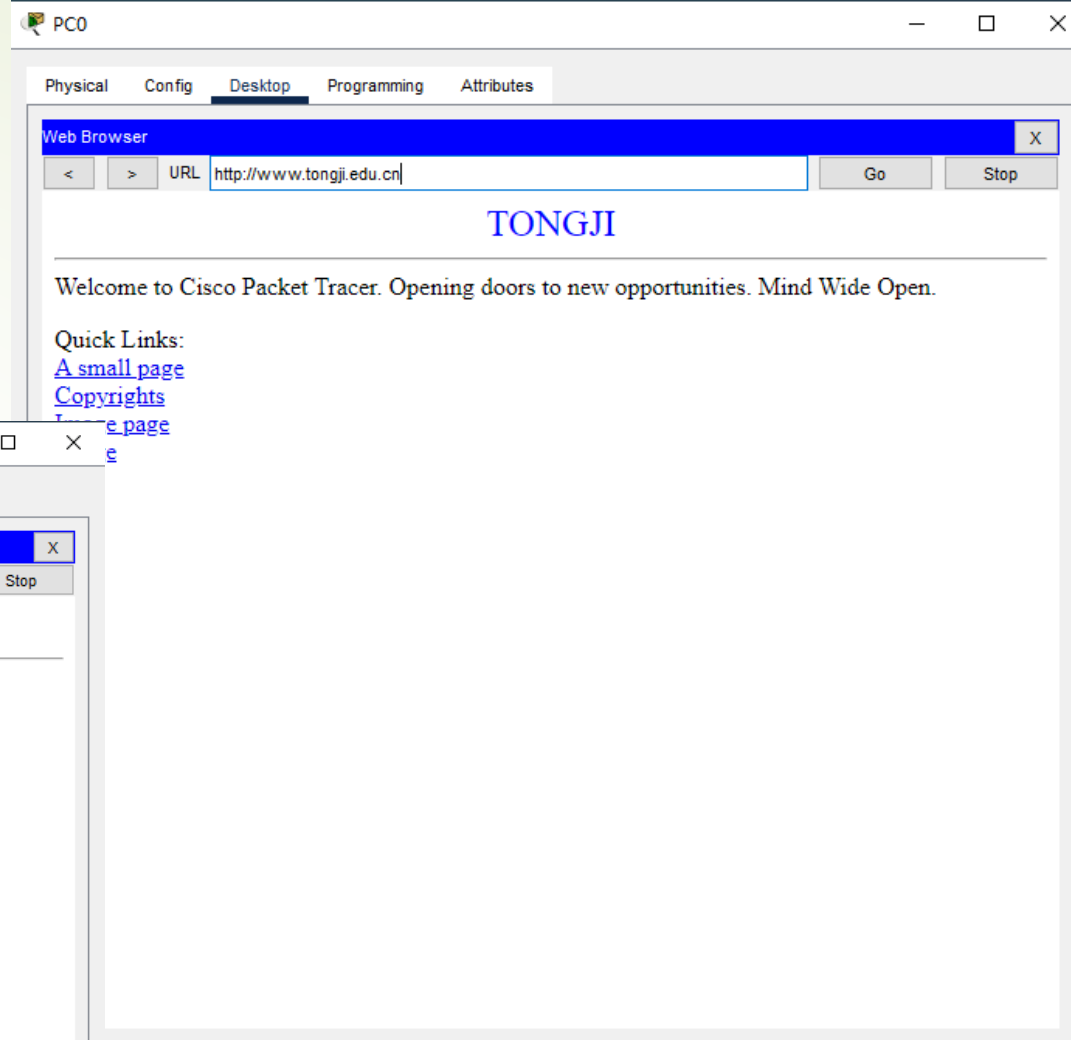
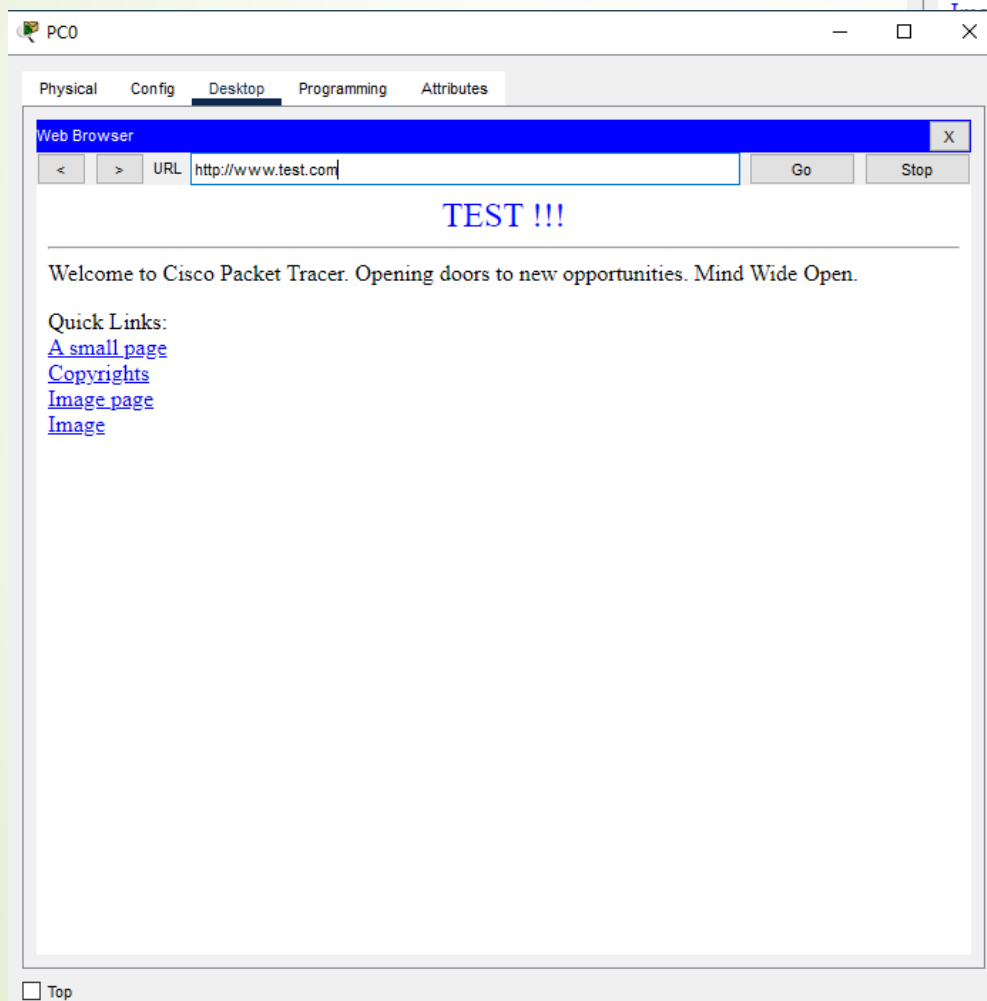
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1035, Dst Port: 80	Layer4
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.8	Layer3
Layer 2: Ethernet II Header 0005.5E96.9C02 >> 00E0.A39A.8929	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The device receives a TCP ACK segment on the connection to 192.168.1.11 on port 1035.
2. Received segment information: the sequence number 104, the ACK number 472, and the data length 20.
3. The TCP segment has the expected peer sequence number.
4. The device sets the connection state to CLOSED.

Challenge Me << Previous Layer Next Layer >>

PT软件分析TCP报文

PC0 WEB Browser



Wireshark TCP报文抓取分析

35

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15872	3485.47789	192.168.1.5	120.241.16.104	TCP	57742 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15875	3485.81728	192.168.1.5	64.233.189.188	TCP	[TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 win=65048 Len=1
15876	3485.99918	64.233.189.188	192.168.1.5	TCP	[TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 win=67840 Len=0 SLE=1012 SRE=1013
15881	3486.93942	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15882	3486.97651	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [SYN, ACK] Seq=0 Ack=1 win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
15883	3486.97659	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=1 Ack=1 win=65536 Len=0
15884	3486.97671	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=274
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25067	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRE=21
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic

Frame 15881: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Destination: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Source: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)

Type: IP (0x0800)

Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 120.241.16.104 (120.241.16.104)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 52

Identification: 0x2316 (8982)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x8ca7 [correct]

Source: 192.168.1.5 (192.168.1.5)

Destination: 120.241.16.104 (120.241.16.104)

Transmission Control Protocol, Src Port: 57743 (57743), Dst Port: 36688 (36688), Seq: 0, Len: 0

Source port: 57743 (57743)

Destination port: 36688 (36688)

[Stream index: 1147]

Sequence number: 0 (relative sequence number)

Header length: 32 bytes

Flags: 0x02 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion window Reduced (CWR): Not set

.... 0... = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...0 = Acknowledgement: Not set

.... ...0 = Push: Not set

.... ...0 = Reset: Not set

.... ...1 = Syn: Set

.... ...0 = Fin: Not set

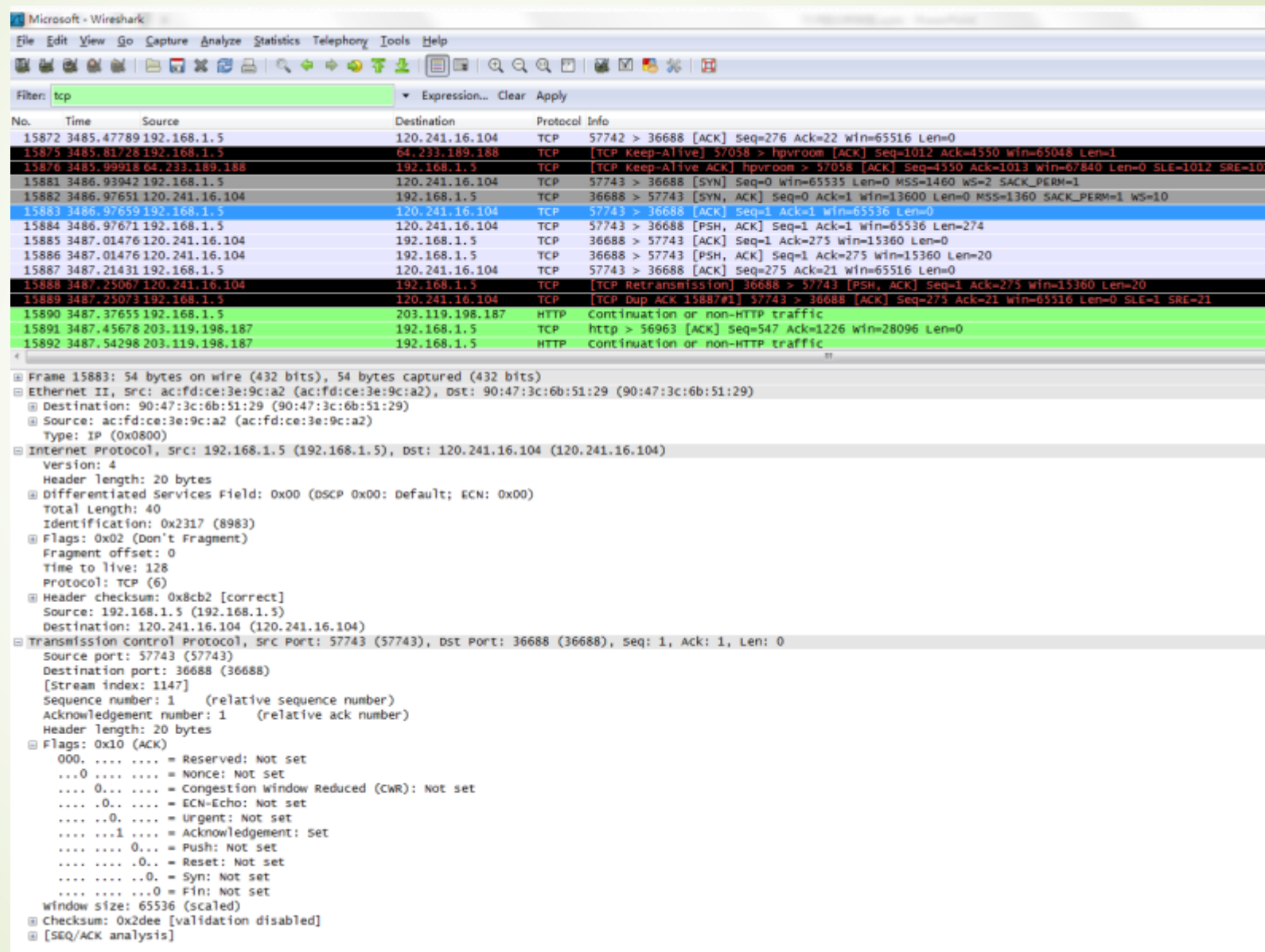
Window size: 65535

Checksum: 0x90b9 [validation disabled]

Options: (12 bytes)

Wireshark TCP报文抓取分析

36



The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, filtered by 'tcp'. The middle pane shows the details of the selected packet (Frame 15883), including Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP) fields. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Info
15872	3485.47789	192.168.1.5	120.241.16.104	TCP	57742 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15875	3485.81728	192.168.1.5	64.233.189.188	TCP	[TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 win=65048 Len=1
15876	3485.99918	64.233.189.188	192.168.1.5	TCP	[TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 win=67840 Len=0 SLE=1012 SRE=1013
15881	3486.93942	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15882	3486.97651	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [SYN, ACK] Seq=0 Ack=1 win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
15883	3486.97659	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=1 Ack=1 win=65536 Len=0
15884	3486.97671	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=274
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25067	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRE=21
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic

Frame 15883 Details:

- Frame 15883: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
- Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
 - Destination: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
 - Source: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
 - Type: IP (0x0800)
- Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 120.241.16.104 (120.241.16.104)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 40
 - Identification: 0x2317 (8983)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0x8cb2 [correct]
 - Source: 192.168.1.5 (192.168.1.5)
 - Destination: 120.241.16.104 (120.241.16.104)
- Transmission Control Protocol, Src Port: 57743 (57743), Dst Port: 36688 (36688), Seq: 1, Ack: 1, Len: 0
 - Source port: 57743 (57743)
 - Destination port: 36688 (36688)
 - [Stream index: 1147]
 - Sequence number: 1 (relative sequence number)
 - Acknowledgement number: 1 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x10 (ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - 0... = Congestion window Reduced (cwr): Not set
 -0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -1 = Acknowledgement: Set
 - 0... = Push: Not set
 - 0.. = Reset: Not set
 -0. = Syn: Not set
 - 0 = Fin: Not set
 - Window size: 65536 (scaled)
 - Checksum: 0x2dee [validation disabled]
 - [SEQ/ACK analysis]

Wireshark TCP报文抓取分析

37

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The bottom pane shows the detailed view of a selected packet (No. 15884).

Packet List:

No.	Time	Source	Destination	Protocol	Info
15872	3485.47789	192.168.1.5	120.241.16.104	TCP	57742 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15875	3485.81728	192.168.1.5	64.233.189.188	TCP	[TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 win=65048 Len=1
15876	3485.99918	64.233.189.188	192.168.1.5	TCP	[TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 win=67840 Len=0 SLE=1012 SRC=1013
15881	3486.93942	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15882	3486.97651	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [SYN, ACK] Seq=0 Ack=1 win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
15883	3486.97659	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=1 Ack=1 win=65536 Len=0
15884	3486.97671	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=274
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25007	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRC=21
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic

Packet Details (No. 15884):

- Destination: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
- Source: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
- Type: IP (0x0800)
- Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 120.241.16.104 (120.241.16.104)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 314
 - Identification: 0x2318 (8984)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0x8b9f [correct]
 - Source: 192.168.1.5 (192.168.1.5)
 - Destination: 120.241.16.104 (120.241.16.104)
- Transmission Control Protocol, Src Port: 57743 (57743), Dst Port: 36688 (36688), Seq: 1, Ack: 1, Len: 274
 - Source port: 57743 (57743)
 - Destination port: 36688 (36688)
 - [Stream index: 1147]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 275 (relative sequence number)]
 - Acknowledgement number: 1 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x18 (PSH, ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - ...0 = Congestion Window Reduced (CWR): Not set
 -0. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -1. = Acknowledgement: Set
 -1. = Push: Set
 -0. = Reset: Not set
 -0. = Syn: Not set
 -0. = Fin: Not set
 - Window size: 65536 (scaled)
 - Checksum: 0x7050 [validation disabled]
 - [SEQ/ACK analysis]
- Data (274 bytes)
 - Data: 000a1b10003852000000011200001fbd81a8150000000070...
 - Length: 274

Wireshark TCP报文抓取分析

38

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15872	3485.47789	192.168.1.5	120.241.16.104	TCP	57742 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15875	3485.81728	192.168.1.5	64.233.189.188	TCP	[TCP keep-alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 win=65048 Len=1
15876	3485.99918	64.233.189.188	192.168.1.5	TCP	[TCP keep-alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 win=67840 Len=0 SLE=1012 SRE=10
15881	3486.93942	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15882	3486.97651	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [SYN, ACK] Seq=0 Ack=1 win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
15883	3486.97659	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=1 Ack=1 win=65536 Len=0
15884	3486.97671	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=274
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25067	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRE=21
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=347 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	continuation or non-HTTP traffic

Frame 15885: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

- Ethernet II, Src: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29), Dst: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
 - Destination: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
 - Source: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
 - Type: IP (0x0800)
- Internet Protocol, Src: 120.241.16.104 (120.241.16.104), Dst: 192.168.1.5 (192.168.1.5)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x04 (DSCP 0x01: Unknown DSCP; ECN: 0x00)
 - Total Length: 40
 - Identification: 0x0eac (3756)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 54
 - Protocol: TCP (6)
 - Header checksum: 0xeb19 [correct]
 - Source: 120.241.16.104 (120.241.16.104)
 - Destination: 192.168.1.5 (192.168.1.5)
- Transmission Control Protocol, Src Port: 36688 (36688), Dst Port: 57743 (57743), Seq: 1, Ack: 275, Len: 0
 - Source port: 36688 (36688)
 - Destination port: 57743 (57743)
 - [Stream index: 1147]
 - Sequence number: 1 (relative sequence number)
 - Acknowledgement number: 275 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x10 (ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - 0... = Congestion Window Reduced (CWR): Not set
 - 0... = ECN-Echo: Not set
 - 0... = Urgent: Not set
 - 0... = Acknowledgement: set
 - 0... = Push: Not set
 - 0... = Reset: Not set
 - 0... = Syn: Not set
 - 0... = Fin: Not set
 - Window size: 15360 (scaled)
 - Checksum: 0x6ccd [validation disabled]
 - [SEQ/ACK analysis]

Wireshark TCP报文抓取分析

39

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15872	3485.47789	192.168.1.5	120.241.16.104	TCP	57742 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15875	3485.81728	192.168.1.5	64.233.189.188	TCP	[TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 win=65048 Len=1
15876	3485.99218	64.233.189.188	192.168.1.5	TCP	[TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1012 win=67840 Len=0 SLE=1012
15881	3486.93942	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15882	3486.97651	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [SYN, ACK] Seq=0 Ack=1 win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
15883	3486.97659	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=1 Ack=1 win=65536 Len=0
15884	3486.97671	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=274
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25067	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRE=21
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic

4

Frame 15886: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29), Dst: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)

Destination: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)

Source: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Type: IP (0x0800)

Internet Protocol, Src: 120.241.16.104 (120.241.16.104), Dst: 192.168.1.5 (192.168.1.5)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x04 (DSCP 0x01: Unknown DSCP; ECN: 0x00)

Total Length: 60

Identification: 0x0ead (3757)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 54

Protocol: TCP (6)

Header checksum: 0xeb04 [correct]

Source: 120.241.16.104 (120.241.16.104)

Destination: 192.168.1.5 (192.168.1.5)

Transmission Control Protocol, Src Port: 36688 (36688), Dst Port: 57743 (57743), Seq: 1, Ack: 275, Len: 20

Source port: 36688 (36688)

Destination port: 57743 (57743)

[Stream index: 1147]

Sequence number: 1 (relative sequence number)

[Next sequence number: 21 (relative sequence number)]

Acknowledgement number: 275 (relative ack number)

Header length: 20 bytes

Flags: 0x18 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgement: Set

....1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

Window size: 15360 (scaled)

checksum: 0x198b [validation disabled]

[SEQ/ACK analysis]

Data (20 bytes)

Wireshark TCP报文抓取分析

40

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15872	3485.47789	192.168.1.5	120.241.16.104	TCP	57742 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15873	3485.81728	192.168.1.5	64.233.189.188	TCP	[TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 win=65048 Len=1
15876	3485.99918	64.233.189.188	192.168.1.5	TCP	[TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 win=67840 Len=0 SLE=1012 SRE=1013
15881	3486.93942	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15882	3486.97651	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [SYN, ACK] Seq=0 Ack=1 win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
15883	3486.97659	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=1 Ack=1 win=65536 Len=0
15884	3486.97671	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=274
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25007	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRE=21
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic

Frame 15887: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Destination: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Source: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)

Type: IP (0x0800)

Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 120.241.16.104 (120.241.16.104)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 40

Identification: 0x2319 (8985)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x8cb0 [correct]

Source: 192.168.1.5 (192.168.1.5)

Destination: 120.241.16.104 (120.241.16.104)

Transmission Control Protocol, Src Port: 57743 (57743), Dst Port: 36688 (36688), Seq: 275, Ack: 21, Len: 0

Source port: 57743 (57743)

Destination port: 36688 (36688)

[Stream index: 1147]

Sequence number: 275 (relative sequence number)

Acknowledgement number: 21 (relative ack number)

Header Length: 20 bytes

Flags: 0x10 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion window Reduced (CWR): Not set

.... 0... = ECN-Echo: Not set

.... 0... = Urgent: Not set

.... 1... = Acknowledgement: Set

.... 0... = Push: Not set

.... 0... = Reset: Not set

.... 0... = Syn: Not set

.... 0... = Fin: Not set

Window size: 65516 (scaled)

Checksum: 0x2ccd (validation disabled)

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 15886]

[The RTT to ACK the segment was: 0.199555000 seconds]

Wireshark TCP报文抓取分析

41

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25067	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLE=1 SRE=
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic
15893	3487.74631	192.168.1.5	203.119.198.187	TCP	56963 > http [ACK] Seq=1226 Ack=929 win=16445 Len=0
15894	3488.21417	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [FIN, ACK] Seq=275 Ack=21 win=65516 Len=0
15895	3488.25148	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [FIN, ACK] Seq=21 Ack=276 win=15360 Len=0
15896	3488.25155	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15898	3488.86922	183.192.200.40	192.168.1.5	TCP	[TCP keep-alive] http > 57110 [ACK] Seq=9925 Ack=20921 win=43008 Len=0
15899	3488.86929	192.168.1.5	183.192.200.40	TCP	[TCP keep-alive ACK] 57110 > http [ACK] Seq=20921 Ack=9926 win=64896 Len=0
15900	3490.01454	192.168.1.5	120.241.16.104	TCP	57744 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1

Frame 15894: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Destination: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)

Source: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)

Type: IP (0x0800)

Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 120.241.16.104 (120.241.16.104)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 40

Identification: 0x231d (8989)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x8cac [correct]

Source: 192.168.1.5 (192.168.1.5)

Destination: 120.241.16.104 (120.241.16.104)

Transmission Control Protocol, Src Port: 57743 (57743), Dst Port: 36688 (36688), Seq: 275, Ack: 21, Len: 0

Source port: 57743 (57743)

Destination port: 36688 (36688)

[Stream index: 1147]

Sequence number: 275 (relative sequence number)

Acknowledgement number: 21 (relative ack number)

Header length: 20 bytes

Flags: 0x11 (FIN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion window reduced (cwr): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgement: Set

.... 0... = Push: Not set

.... 0.. = Reset: Not set

....0. = Syn: Not set

....1 = Fin: Set

Window size: 65516 (scaled)

Checksum: 0x2ccc [validation disabled]

Wireshark TCP报文抓取分析

42

The image shows a Wireshark packet capture of a TCP connection. The top pane displays a list of captured packets. Packet 15889 is selected, and the bottom pane shows its detailed structure.

Packet List:

No.	Time	Source	Destination	Protocol	Info
15885	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [ACK] Seq=1 Ack=275 win=15360 Len=0
15886	3487.01476	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15887	3487.21431	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0
15888	3487.25007	120.241.16.104	192.168.1.5	TCP	[TCP Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 win=15360 Len=20
15889	3487.25073	192.168.1.5	120.241.16.104	TCP	[TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 win=65516 Len=0 SLK=1 SRTT=0
15890	3487.37655	192.168.1.5	203.119.198.187	HTTP	Continuation or non-HTTP traffic
15891	3487.45678	203.119.198.187	192.168.1.5	TCP	http > 56963 [ACK] Seq=547 Ack=1226 win=28096 Len=0
15892	3487.54298	203.119.198.187	192.168.1.5	HTTP	Continuation or non-HTTP traffic
15893	3487.74631	192.168.1.5	203.119.198.187	TCP	56963 > http [ACK] Seq=1226 Ack=929 win=16445 Len=0
15894	3488.21437	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [FIN, ACK] Seq=275 Ack=21 win=65516 Len=0
15895	3488.25148	120.241.16.104	192.168.1.5	TCP	36688 > 57743 [FIN, ACK] Seq=21 Ack=276 win=15360 Len=0
15896	3488.25155	192.168.1.5	120.241.16.104	TCP	57743 > 36688 [ACK] Seq=276 Ack=22 win=65516 Len=0
15898	3488.86922	183.192.200.40	192.168.1.5	TCP	[TCP Keep-Alive] http > 37110 [ACK] Seq=9925 Ack=20921 win=43008 Len=0
15899	3488.86929	192.168.1.5	183.192.200.40	TCP	[TCP Keep-Alive ACK] 57110 > http [ACK] Seq=20921 Ack=9926 win=64896 Len=0
15900	3490.01454	192.168.1.5	120.241.16.104	TCP	57744 > 36688 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1

Packet 15895 Details:

- Frame 15895: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
- Ethernet II, Src: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29), Dst: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
- Destination: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2)
- Source: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
- Type: IP (0x0800)
- Internet Protocol, Src: 120.241.16.104 (120.241.16.104), Dst: 192.168.1.5 (192.168.1.5)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x04 (DSCP 0x01: Unknown DSCP; ECN: 0x00)
- Total Length: 40
- Identification: 0x0eaf (3759)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 54
- Protocol: TCP (6)
- Header checksum: 0xeb16 [correct]
- Source: 120.241.16.104 (120.241.16.104)
- Destination: 192.168.1.5 (192.168.1.5)
- Transmission Control Protocol, Src Port: 36688 (36688), Dst Port: 57743 (57743), Seq: 21, Ack: 276, Len: 0
- Source port: 36688 (36688)
- Destination port: 57743 (57743)
- [Stream index: 1147]
- Sequence number: 21 (relative sequence number)
- Acknowledgement number: 276 (relative ack number)
- Header length: 20 bytes
- Flags: 0x11 (FIN, ACK)
- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- 0... = Congestion window Reduced (CWR): Not set
-0.. = ECN-Echo: Not set
-0. = Urgent: Not set
-1 = Acknowledgement: Set
- 0... = Push: Not set
- 0.. = Reset: Not set
-0. = Syn: Not set
-1 = Fin: Set
- Window size: 15360 (scaled)
- Checksum: 0x6cb7 [validation disabled]
- [SEQ/ACK analysis]
- [This is an ACK to the segment in frame: 15894]
- [The RTT to ACK the segment was: 0.037112000 seconds]

实验主要分析内容

- 1.分析在Packet tracer中TCP报文情况；
- 2.用WireShark抓取TCP数据包；
- 3.查看TCP报文字段内容，并解读；
- 4.仔细研读TCP连接建立过程数据报文；
- 5.仔细研读TCP拆链过程数据报文