TCP数据分析实验

同济大学软件学院



一个发义。

1. TCP的概述

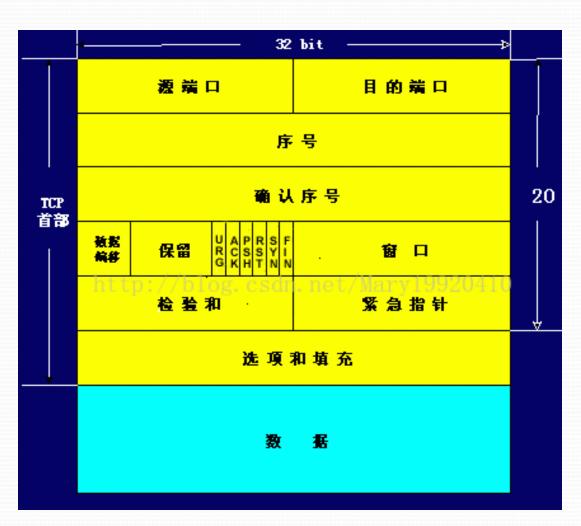
TCP是传输层的协议、功能即为在IP的 数据报服务之上增加了最基本的服务: 复用和 分用以及差错检测。TCP是一个基于连接的四 层协议,提供全双工地,可靠地传输系统。它 能够保证数据被远程主机接收。并且能够为高 层协议提供flow-controlled 服务。空间上,TCP 需要在端系统中维护连接状态,需要一定的开 销。此连接装入包括接收和发送缓存,拥塞控 制参数和序号与确认号的参数。UDP不维护连 接状态,也不跟踪这些参数,开销小。空间和 时间上都具有优势。



2. 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数话

3. TCP报文字段

A、端口号: 用来标识同一台计算机的不同的应用进程。

- 1) 源端口:源端口和IP地址的作用是标识报文的返回地址。
- 2) 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数注

- 3.TCP报文字段
- B、序号和确认号: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数注

- 3.TCP报文字段
- C、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。
- D、保留: 为将来定义新的用途保留, 现在一般置O。



(上致义)居

- 3.TCP报文字段
- E、控制位: URG ACK PSH RST SYN FIN, 共 6个,每一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。



一个数人。

- 3.TCP报文字段
- E、控制位: URG ACK PSH RST SYN FIN
- 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数法

3.TCP报文字段

F、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。窗口大小时一个16bit字段,因而窗口大小最大为65535。

G、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数式括

3.TCP报文字段

- H、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。
- I、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。



TCP数注

3.TCP报文字段

- 1、选项和填充: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。
- J、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数注据

3.TCP报文字段

- 1、选项和填充: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。
- J、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。



4. TCP连接过程

相对于SOCKET开发者,TCP创建过程和链接折除过程是由TCP/IP协议栈自动创建的。因此开发者并不需要控制这个过程。但是对于理解TCP底层运作机制,相当有帮助。TCP连接过程简单一句话概括: "三次握手四次挥手"。

MA. TCP三次握手

所谓三次握手(Three-way Handshake),是指建立一个TCP连接时,需要客户端和服务器总共发送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.在socket编程中,客户端执行connect()时。将触发三次握手。 13

TCP数法

4.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					
		(2	()					
		接收川	页序号					
偏置值	保留	UAPR F RCSS1 I GKHT N	窗口					
	检查和	印	紧急指针					
任选项+补丁								
	用户数据							



TCP数排

4.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					
		(7						
		X-	+1)					
偏置值	保留	U PR F ROSSDI G HT N	窗口					
	检查和	印	紧急指针					
	任选项+补丁							
		用户	数据					



同為大學軟件學院

TCP数对据

4.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!]	目标端口			
		发送川	页序号			
		Ý.	+1>			
偏置值	保留	U PRSF R1SSYI G HTNN	窗口			
	检查和	印	紧急指针			
任选项+补丁						
		<u> DATA</u>	(X+1)>			

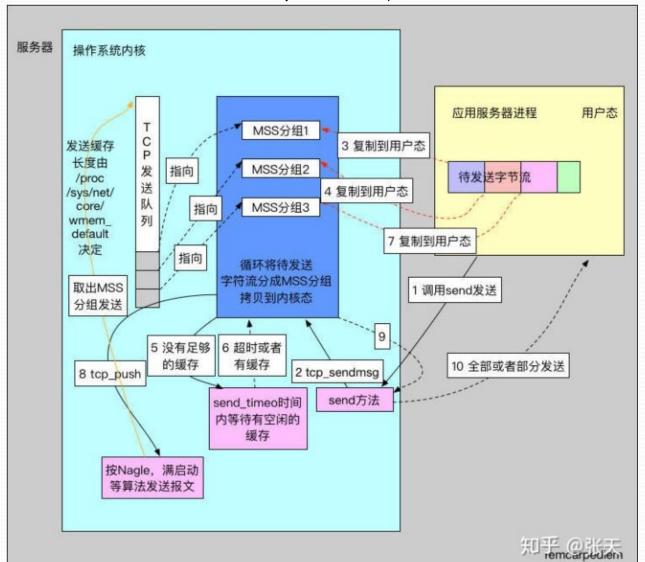


4. TCP连接过程

Tip:SYN攻击在三次握手过程中,服务器发送 SYN-ACK之后,收到客户端的ACK之前的TCP连接 称为半连接(half-open connect).此时服务器处于 Syn_RECV状态.当收到ACK后,服务器转入 ESTABLISHED状态。攻击客户端在短时间内伪造 大量不存在的IP地址,向服务器不断地发送syn包, 服务器回复确认包,并等待客户的确认,由于源 地址是不存在的,服务器需要不断的重发直至超 时,这些伪造的SYN包将长时间占用未连接队列, 正常的SYN请求被丢弃,目标系统运行缓慢,严 重者引起网络堵塞甚至系统瘫痪。

4. TCP连接过程

Tip2:TCP发送报文,操作系统内核与用户态





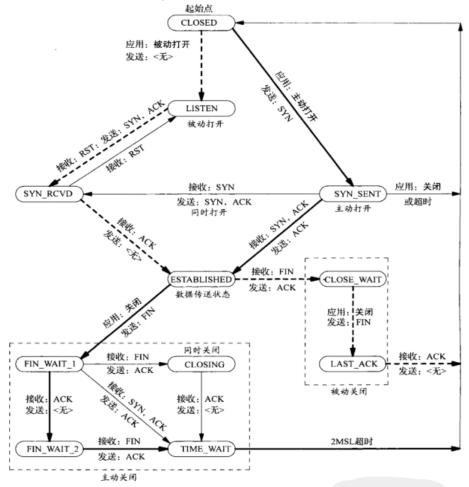
4.TCP连接过程 B.TCP四次挥手

TCP的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 主动方 主动方发送 被动方发送ACK报 Fin=1 Ack=Z Seg = X Fin+Ack报文.并 文.并置发送序号为 置发送序号为X Z.在确认序号为 ACK=X+1 Seq = Z被动方发送Fin+Ack 报文.并置发送序号 Fin=1 Ack=X Seg = Y 为Y.在确认序号为X 主动发发送ack报文. 并置发送序号为X, 在确认序号为Y ACK=Y Seg = X

4. TCP连接过程

C. TCP三次握手会涉及TCP的状态转换图如下



---表示客户的正常状态转换

□用: 表示状态转换在应用进程发起操作时发生

安收: 表示状态转换在接收到分节时发生

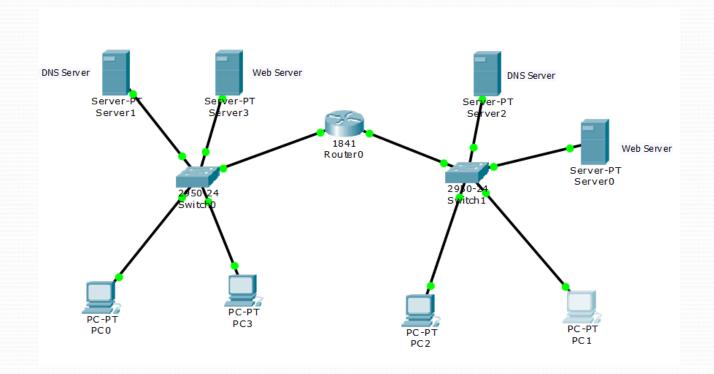
x: 表示故心特换在按收到 送: 表示这个转换发送什么



TCP数法科文文

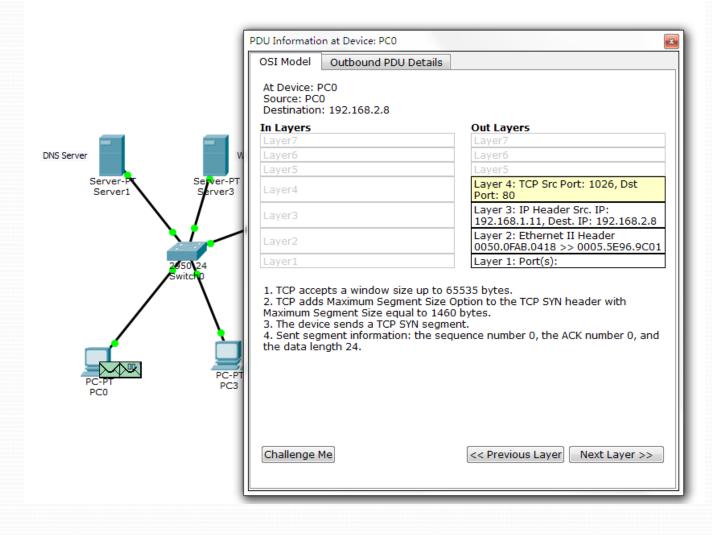
5.Packet Tracer 分析TCP报文 网络结构图

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





TCP数据报文





TCP数法据报文

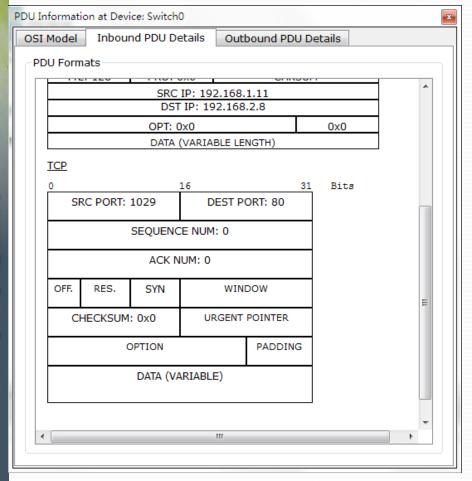
5. Packet Tracer 分析TCP报文

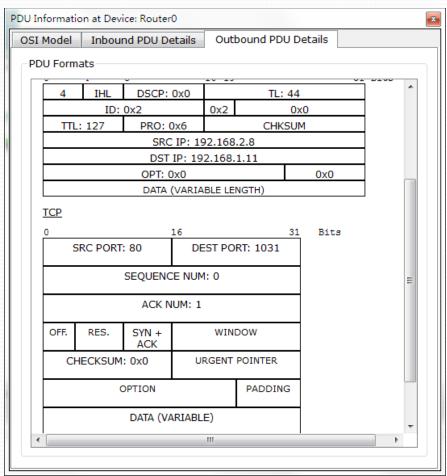
OSI Model Outbound PDU Details PDU Formats SRC IP: 192.168.1.11 DST IP: 192.168.2.8 OPT: 0x0 0x0 DATA (VARIABLE LENGTH) **TCP** Bits SRC PORT: 1026 DEST PORT: 80 SEQUENCE NUM: 0 ACK NUM: 0 OFF. RES. SYN WINDOW CHECKSUM: 0x0 URGENT POINTER PADDING OPTION DATA (VARIABLE)



]题大学政体学的ool of Software Engineering. Longi University

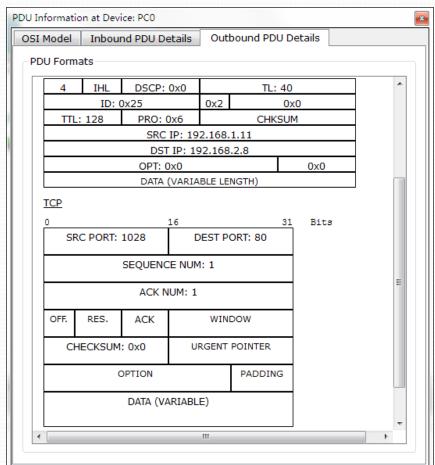
TCP数法据报文





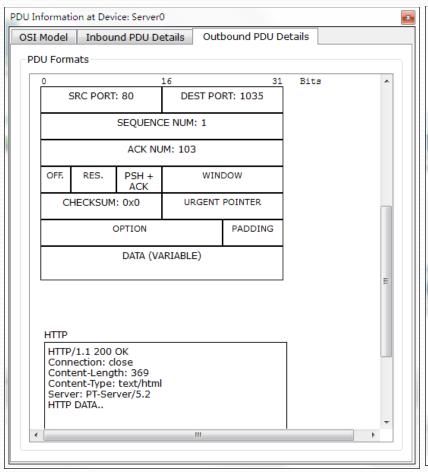
TCP数据报文

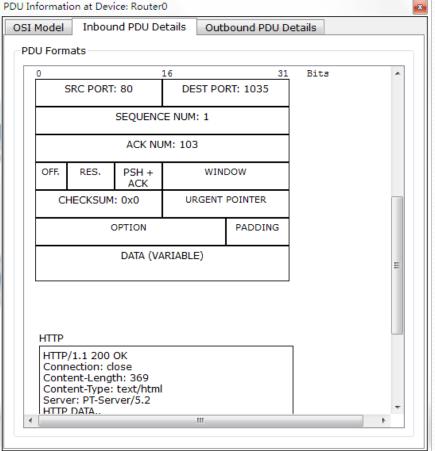
DUI	informati	on at Devi	ice: Switch()			×				
OSI	I Model	Inbou	nd PDU De	etails Ou	tbound PDL	J Details					
PI	PDU Formats										
	4	IHL	DSCP:	0x0	TL:	40					
		ID: (0x19	0x2		0x0					
	TTL	: 128	PRO: 0)x6	CHKS	SUM					
				IP: 192.168			4				
				IP: 192.16	8.2.8		-				
			OPT: 0		ENGTU)	0x0					
			DAIA (VARIABLE L	ENGTH)		_				
	<u>TCP</u>										
	0 16 31 Bits										
	SF	C PORT:	1030								
			SEQUENC	_	=						
	SEQUENCE NO.11 I										
	OFF.	RES.	ACK	WII	NDOW						
	Cl	HECKSUM	: 0x0	URGEN'	POINTER						
		(OPTION	PADDING	3						
	DATA (VARIABLE)										





TCP数法据报文

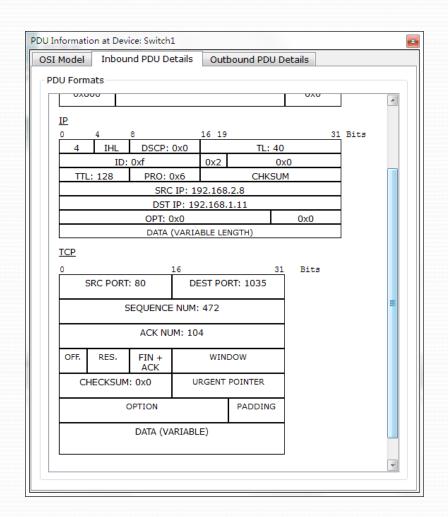






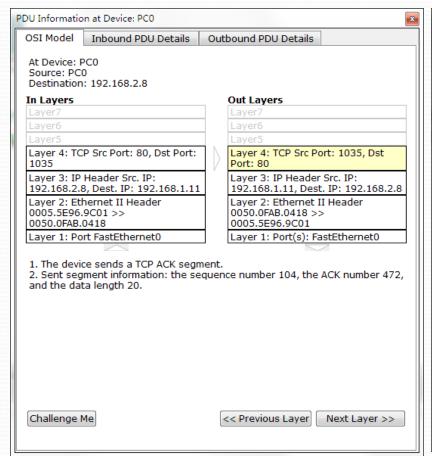
TCP数排列文

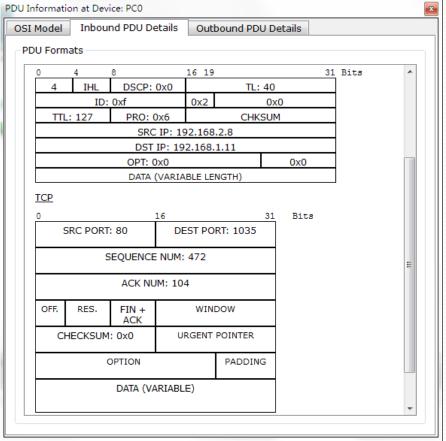
odel	Inhour						l l	
	Inboui	nd PDU De	etails	Outl	ound PDU	Details		
Format	ts							
	ъ. о	жээ	_	UNZ		UNU	H 🔊	
TTL:	128				UM	_		
							4	
				2.168	.2.8		4	
					10711	0x0	-	
		DAIA	VARIA	SLE LEI	NGTH)		_	
<u>CP</u>								
			16		:	31 Bits		
SRC	PORT:	1035	D	EST PO	ORT: 80			
SKOTOKII 1955 BESTTOKII 00								
OFF. RES. FIN + WINDOW							=	
		ACK						
CHECKSUM: 0x0 URGENT P								
					-			
	C							
DATA (VARIABLE)								
DAIA (VAIGABLE)								
							*	
				III			•	
	SRC	SRC PORT: S OFF. RES. CHECKSUM:	SRC DST OPT: 0 DATA (CP SRC PORT: 1035 SEQUENCE ACK NU OFF. RES. FIN + ACK CHECKSUM: 0x0 OPTION	SRC IP: 192 DST IP: 19 OPT: 0x0 DATA (VARIAN P SRC PORT: 1035 D SEQUENCE NUM: 472 OFF. RES. FIN + ACK CHECKSUM: 0x0 UR OPTION DATA (VARIABLE	SRC IP: 192.168. DST IP: 192.168. OPT: 0x0 DATA (VARIABLE LEI OPT: 0x0 DATA (VARIABLE LEI OPT: 0x0 DATA (VARIABLE LEI OPT: 0x0 ACK NUM: 472 OFF. RES. FIN + WING ACK CHECKSUM: 0x0 URGENT OPTION	SRC IP: 192.168.1.11 DST IP: 192.168.2.8 OPT: 0x0 DATA (VARIABLE LENGTH) SRC PORT: 1035 DEST PORT: 80 SEQUENCE NUM: 103 ACK NUM: 472 OFF. RES. FIN + WINDOW CHECKSUM: 0x0 URGENT POINTER OPTION PADDING DATA (VARIABLE)	SRC IP: 192.168.1.11 DST IP: 192.168.2.8 OPT: 0x0 DATA (VARIABLE LENGTH) OPTION SEQUENCE NUM: 103 ACK NUM: 472 OFF. RES. FIN + WINDOW CHECKSUM: 0x0 URGENT POINTER OPTION PADDING DATA (VARIABLE)	





TCP数对据技文



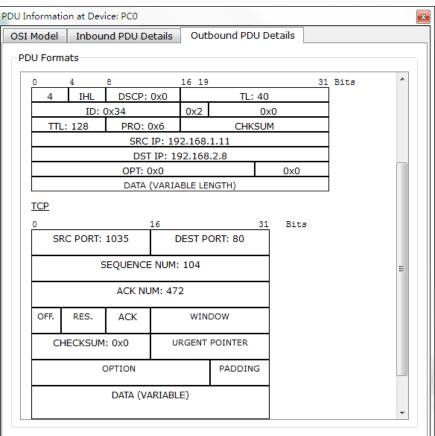




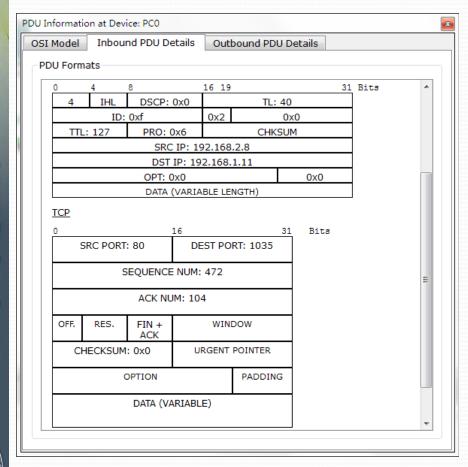
) 回過大學軟件哪門 School of Software Engineering. Tongli Universit

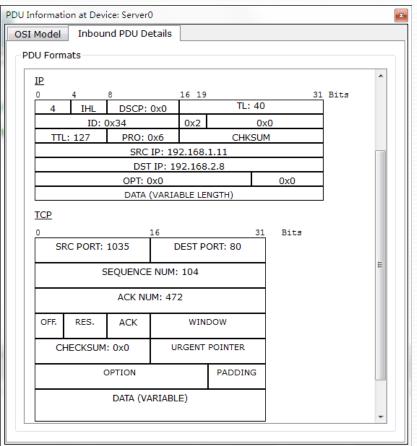
TCP数排列文

PDU In	DU Information at Device: PC0									
OSI	OSI Model Inbound PDU Details Outbound PDU Details									
_PD	OU Form	nats								
	0	4	8		31 Bits	*				
	4 IHL DSCP: 0x0					TL: 40				
			0xf		0x2		0x0	_		
	Πι	L: 127	PRO: (CHKS	JM	_		
					92.168			\dashv		
					2.168.	1.11	0.40	_		
			OPT: 0		ABLE LE	NGTH)	0x0	\dashv		
			DAIA	(VAICE	OLL LL	NOTH)				
	<u>TCP</u>									
	0			16			1 Bits			
	SRC PORT: 80 DEST PORT: 1035									
		5	EQUENCE	1						
				4						
			ACK NU							
	OFF.	RES.	FIN + ACK							
	CHECKSUM: 0x0 URGENT POINTER									
	OPTION						1			
			DATA (VA							
									•	

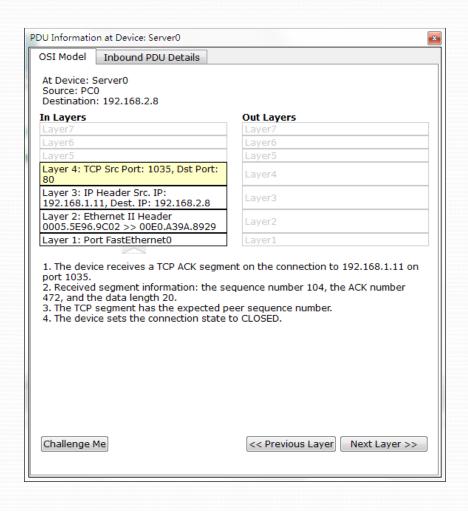


TCP数法据技文





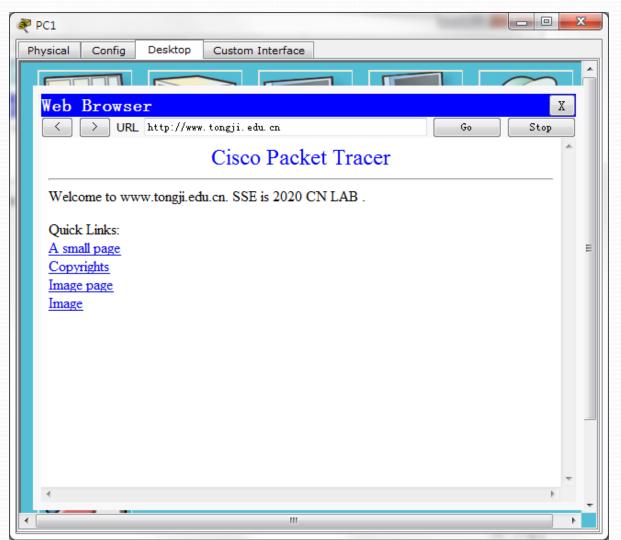
TCP数法目技文





TCP数法据技文

4. Packet Tracer 分析报文 PC1 WEB Browser

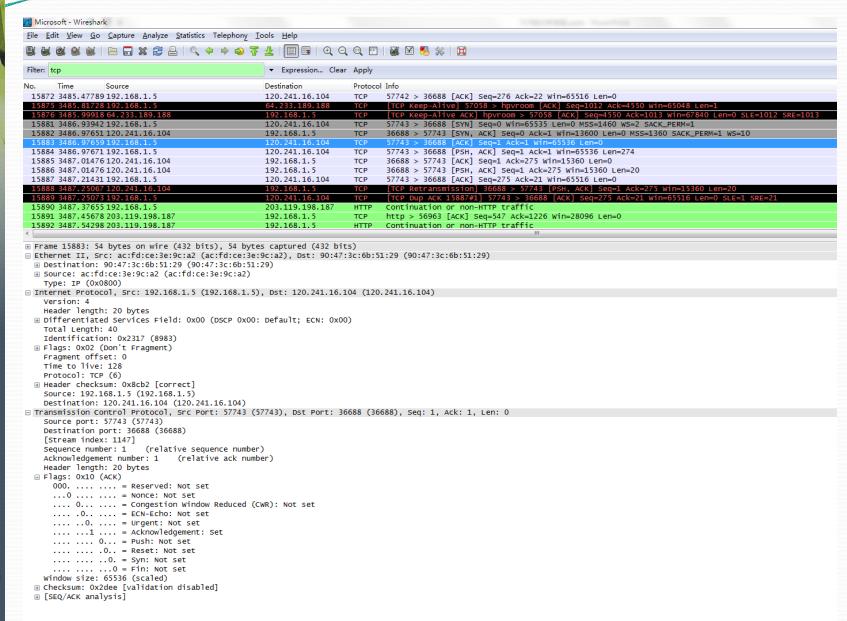


⊕ Options: (12 bytes)

5. WireShark TCP报文採取分析

File Edit View Go Capture Analyze Statistics Telephony Tools Help ▼ Expression... Clear Apply Filter: tcp Time Source Destination Protocol Info 15872 3485, 47789 192, 168, 1, 5 120, 241, 16, 104 57742 > 36688 [ACK] Seq=276 Ack=22 Win=65516 Len=0 15875 3485.81728 192.168.1.5 64.233.189.188 [TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 Win: 120.241.16.104 36688 > 57743 [SYN, ACK] Seq=0 Ack=1 Win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10 15882 3486.97651 120.241.16.104 192.168.1.5 15883 3486.97659 192.168.1.5 120.241.16.104 57743 > 36688 [ACK] Seg=1 Ack=1 Win=65536 Len=0 57743 > 36688 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=274 15884 3486.97671 192.168.1.5 120.241.16.104 15885 3487.01476 120.241.16.104 192.168.1.5 36688 > 57743 [ACK] Seq=1 Ack=275 Win=15360 Len=0 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 Win=15360 Len=20 15886 3487.01476 120.241.16.104 192.168.1.5 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 Retransmission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 Win=15360 Len [TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 Win=65516 Len=0 SLE=1 15889 3487.25073 192.168.1.5 120.241.16.104 15890 3487.37655 192.168.1.5 203.119.198.187 Continuation or non-HTTP traffic http > 56963 [ACK] Seq=547 Ack=1226 Win=28096 Len=0 15891 3487.45678 203.119.198.187 192.168.1.5 15892 3487.54298 203.119.198.187 192.168.1.5 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) Fragment offset: 0 Time to live: 128 Protocol: TCP (6) 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 set0.. = ECN-Echo: Not set0. = Urgent: Not set 0 = Acknowledgement: Not set 0... = Push: Not set0.. = Reset: Not set ±1. = Syn: Set 0 = Fin: Not set Window size: 65535 ⊕ Checksum: 0x90b9 [validation disabled]

File Edit View Go Capture Analyze Statistics Telephony Tools Help 🕎 👹 👺 🎕 🕍 | 🗀 🔚 🗶 😂 占 | º. 🌣 🌳 🐬 🛂 | | 🗐 📴 | º. Q. @, 🗹 | 🖼 🗹 🕵 ¾ | 🖼 Filter: tcp ▼ Expression... Clear Apply Destination Protocol Info Time Source 15872 3485, 47789 192, 168, 1, 5 120.241.16.104 57742 > 36688 [ACK] Seg=276 Ack=22 Win=65516 Len=0 15875 3485.81728 192.168.1.5 64.233.189.188 [TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=45 15881 3486.93942 192.168.1.5 120.241.16.104 57743 > 36688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1 15882 3486.97651 120.241.16.104 36688 > 57743 [SYN, ACK] Seq=0 Ack=1 Win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10 192.168.1.5 15883 3486.97659 192.168.1.5 120.241.16.104 57743 > 36688 [ACK] Seg=1 Ack=1 Win=65536 Len=0 15884 3486.97671 192.168.1.5 120.241.16.104 57743 > 36688 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=274 15885 3487.01476 120.241.16.104 192.168.1.5 36688 > 57743 [ACK] Seq=1 Ack=275 Win=15360 Len=0 15886 3487.01476 120.241.16.104 192.168.1.5 36688 > 57743 [PSH, ACK] Seg=1 Ack=275 Win=15360 Len=20 15887 3487.21431 192.168.1.5 120.241.16.104 57743 > 36688 [ACK] Seq=275 Ack=21 Win=65516 Len=0 5888 3487.25067 120.241.16.10 15889 3487.25073 192.168.1.5 [TCP Dup ACK 15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 Wi 15890 3487.37655 192.168.1.5 203.119.198.187 Continuation or non-HTTP traffic 15891 3487.45678 203.119.198.187 192.168.1.5 http > 56963 [ACK] Seg=547 Ack=1226 Win=28096 Len=0 15892 3487, 54298 203, 119, 198, 187 192.168.1.5 Continuation or non-HTTP traffic □ 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) Fragment offset: 0 Time to live: 128 Protocol: TCP (6) 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 set0.. = ECN-Echo: Not set0. = Urgent: Not set 0 = Acknowledgement: Not set 0... = Push: Not set0.. = Reset: Not set 0 = Fin: Not set Window size: 65535 ⊕ Checksum: 0x90b9 [validation disabled] ⊕ Options: (12 bytes)





e <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Teleph	T 1 11 1		
	-		
[[m] [6] [8] [m] [m] [m] [m] [2] [2] [2] [2] [2] [2] [2] [2] [2] [2	🧇 7 🛂 🗐 🖫 🗨 🤄	2, 🔍 🛅	
ter: tcp	▼ Expression Clea	r Apply	
•	•		d
. Time Source	Destination	Protoco	
L5872 3485.47789 192.168.1.5 L5875 3485.81728 192.168.1.5	120.241.16.104 64.233.189.188	TCP TCP	57742 > 36688 [ACK] Seq=276 Ack=22 Win=65516 Len=0 [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=1012 ACK=4330 WIII=63048 Len=1 [TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 WIII=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
L5884 3486.97671 192.168.1.5 L5885 3487.01476 120.241.16.104	120.241.16.104 192.168.1.5	TCP TCP	57743 > 36688 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=274 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
L5891 3487.45678 203.119.198.187 L5892 3487.54298 203.119.198.187	192.168.1.5 192.168.1.5	TCP HTTP	http > 56963 [ACK] Seq=547 Ack=1226 Win=28096 Len=0 Continuation or non-HTTP traffic
19092 3407. 34290 203.119.190.107	192.100.1.3	HILLE	Continuation of hon-intraction
Identification: 0x2318 (8984) Plags: 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 (120.241.16.10	14)		
Transmission Control Protocol, Src Port: 577 Source port: 57743 (57743) Destination port: 36688 (36688) [Stream index: 1147] Sequence number: 1 (relative sequence r [Next sequence number: 275 (relative seach Acknowledgement number: 1 (relative ack)	number) quence number)]	6688 (36	688), Seq: 1, ACK: 1, Len: 2/4



File Set	Microsoft - Wireshark			THE PROPERTY NAMED IN
Filter Top	<u>File Edit View Go Capture Analyze Statistics Telephony I</u>	ools <u>H</u> elp		
Time	<mark>및 현 영 영 현</mark> 는 <mark>급 X</mark> 22 음 Q 수 수 💠 📆	½ 🗐 🛢 ⊕ ⊖	0 1	
1887 2485.4789192.168.1.5	Filter: tcp	▼ Expression Clear	Apply	
1887 3485.4789192.168.1.5 10.241.16.104 TCP TCP TCP STYAL > 36688 [Acx] Seq=276 Ack-22 wine5516 Lemo 1875 4885.12819.2168.1.5 10.241.6.104 TCP TCP REPARATIVE Acts November 1975 1875 1875 1875 1875 1875 1875 1875 18	No. Time Source	Destination	Protoco	Info
1867 3485.0248192.186.13 107.108.1.3 107.4				
13881 3486.9382 1932.186.1.5 10.241.16.104 102.186.1.5 102.241.16.104 102.186.1.5 102.241.16.104 102.186.1.5 102.241.16.104 103.286.286.27632 102.241.16.104 103.286.286.27632 102.241.16.104 103.286.286.27632 102.241.16.104 103.286.286.27632 102.241.16.104 103.286.286.286.286.286.286.286.286.286.286	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
1882 346.97631 120.241.16.104	15876 3485.99918 64.233.189.188			
1883 3486.9765192.168.1.5 120.241.16.104 TCP 57743 > 36688 [Ref. seq-1 Ack-1 Winne5336 Lene-0] 1884 3486.9765192.168.1.5 120.241.16.104 TCP 57743 > 36688 [Ref. seq-1 Ack-1 Winne5336 Lene-774] 1885 3476.9767.192.168.1.5 120.241.16.104 TCP 57743 > 36688 [Ref. seq-1 Ack-1 Winne5336 Lene-774] 1886 3486.9767.192.168.1.5 120.241.16.104 TCP 57743 > 36688 [Ack, Seq-1 Ack-1 Winne5336 Lene-704] 1887 3487.2481.92.168.1.5 120.241.16.104 TCP 57743 > 36688 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1888 3487.2481.92.168.1.5 120.241.16.104 TCP 57743 > 36688 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1888 3487.25967.190.241.36.104 120.241.16.104 TCP 57743 > 36688 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 > 36688 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP TCP TCP 57743 Sep 58 [Ack, Seq-1 Ack-2 Winne5336 Lene-704] 1889 3487.25967.190.241.36.105 TCP				
1888 1486.9767.192.168.1.5 120.241.16.104 TCP 57743 36688 [PSH, ACK] Seq-14 ACCL WinneSSSS Lem274				
1585 1487-01476 120-241.16.104 192-168.1.5 107 1668.5 57743 [Key, Sequel Acter_275 winn-1580 ten=0 1586 1487-01476 120-241.16.104 192-168.1.5 120-241.16.104 170 1586 1487-01476 120-241.16.104 170 1586 1487-01476 120-241.16.104 170 1774 120-241.16.105 120-241.16.104 170 1774 120-241.16.105 120-241.16.104 170 1774 120-241.16.105 12				
1888 3487.01476120_241.16.104 192.168.1.5 10.241.16.104 17C 57743 [PSH, ACK] Sequ-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.16.104 102_141.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.16.104 102_141.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 102_141.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3487_25067_120_241.61.014 17C 57743 36888 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1888 3688 [ACK] Seq-275 Ack-27 Winn-18360 Lem-20 1				
13889 3487-25007 120-241.16.1.04				
1589 3487.2907.3192.1683.1.5 10.241.16.104 TCP TCP DUD ACT 15807.21 577.43 3688 [ACK] Seq=275 ACK=22 Win=5510 ten-0 SEK=1 SEK=21 15801 3487.45678.203.119.198.187 192.168.1.5 TCP http > 50905 [ACK] Seq=375 ACK=120 Win=28096 Len-0 15802 3487.59288.203.119.198.187 192.168.1.5 TCP http > 50905 [ACK] Seq=376.Ack=1220 win=28096 Len-0 15802 3487.59288.203.119.198.187 192.168.1.5 TCP http > 50905 [ACK] Seq=376.Ack=1220 win=28096 Len-0 15802 3487.59288.203.119.198.187 192.168.1.5 TCP http > 50905 [ACK] Seq=376.Ack=1220 win=28096 Len-0 15802 3487.59288.203.119.198.187 192.168.1.5 TCP http > 50905 [ACK] Seq=376.Ack=1220 win=28096 Len-0 15802 3487.5928.203 192.168.1.5 TCP http > 50905 [ACK] Seq=376.Ack=1220 win=28096 Len-0 15802 3487.5928 TCP	15887 3487.21431 192.168.1.5	120.241.16.104		
1889 3487,37655192.168.1.5 203.119.198.187 TIP Continuation or non-HTP traffic				
1889 1887; 2450;8203.119,198.187 192.168.1.5 TCP http > 59693 [AcK] Seq=347 Ack=1226 win=28096 Len=0 1899 2487; 2450;820.3119,198.187 192.168.1.5 HTTP Continuation on non-HTTP traffic				
SSSIZ 3487, 34298 203,119.198.187				
### Trans 15885: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) ### Trans 15885: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) ### Trans 15885: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) ### Destination: actifice:3e:90:47:3c:6b:51:29 (90:47:3c:6b:51:29) ### Dosurce: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29) ### Type: IP (0x800) ### Trans 120 bytes ### Different 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 (0scp 0x01: unknown 0scp; ECN: 0x00) ### Total Length: 40 ### Identification: 0x0eac (3756)				
□ Ethernet II, Src: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29), Dst: acifd:ce:3e:9c:a2 (acifd:ce:3e:9c:a2) □ Destination: acifd:ce:3e:9c:a2 (acifd: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 Poot: 36688 (36688), Dst Port: 57743 (57743), Seq: 1, Ack: 275, Len: 0 Source port: 36688 (36688) Destination: 192.168.1.5 (192.168.1.5) □ Sequence number: 1 (relative sequence number) Acknowledgement number: 275 (relative ack number) Header length: 20 bytes □ Flags: 0x10 (Ack) 0x00 = Reserved: Not set	←	132.100.1.3		esternation state of the control of
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. = Jurgent: Not set 0. = Push: Not set 0. = Push: Not set 0. = Reset: Not set 0. = Reset: Not set 0. = Syn: Not set	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)			
window size: 15360 (scaled)	Destination port: 57743 (57743) [Stream index: 1147] Sequence number: 1 (relative sequence number Acknowledgement number: 275 (relative ack nu Header length: 20 bytes □ Flags: 0x10 (ACK) 000 = Reserved: Not set0 = Nonce: Not set0 = Congestion window Reduced (COO)0 = ECN-Echo: Not set0 = Urgent: Not set0 - = Vurgent: Not set0 - = Push: Not set0 - = Push: Not set0 - = Push: Not set0 - = Syn: Not set0 - Syn: Not set0 - Syn: Not set0 - Fin: Not set	mber)		



Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help | | 🖹 🔚 🗶 🐉 🖺 | Q. 🗢 🖈 🦈 👍 | 📳 🖪 | Ð. Q. Q. 🖭 | 🖼 🗵 🕵 % | 🖼 Filter: tcp ▼ Expression... Clear Apply Destination Protocol Info Time Source 15872 3485.47789 192.168.1.5 120.241.16.104 57742 > 36688 [ACK] Seg=276 Ack=22 Win=65516 Len=0 15875 3485.81728 192.168.1.5 [TCP Keep-Alive] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 64.233.189.188 [TCP Keep-Alive ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 Win=67840 15876 3485.99918 64.233.189.188 192.168.1.5 TCP 15881 3486.93942 192.168.1.5 120.241.16.104 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 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 57743 > 36688 [ACK] Seq=1 Ack=1 Win=65536 Len=0 120.241.16.104 TCP 57743 > 36688 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=274 15884 3486.97671 192.168.1.5 120.241.16.104 TCP 15885 3487.01476 120.241.16.104 192.168.1.5 36688 > 57743 [ACK] Seq=1 Ack=275 Win=15360 Len=0 15886 3487.01476 120.241.16.104 192.168.1.5 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 Win=15360 Len=20 15887 3487.21431 192.168.1.5 120.241.16.104 57743 > 36688 [ACK] Seq=275 Ack=21 Win=65516 Len=0 15888 3487.25067 120.241.16.10 192.168.1.5 9 3487.25073 192.168.1.5 15890 3487.37655 192.168.1.5 203.119.198.187 HTTP Continuation or non-HTTP traffic 192.168.1.5 15891 3487.45678 203.119.198.187 TCP http > 56963 [ACK] Seq=547 Ack=1226 Win=28096 Len=0 15892 3487.54298 203.119.198.187 192.168.1.5 Continuation or non-HTTP traffic 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) 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 set0.. = ECN-Echo: Not set0. = Urgent: Not set = Acknowledgement: Set = Push: Set0.. = Reset: Not set0. = Syn: Not set 0 = Fin: Not set Window size: 15360 (scaled) ⊕ Checksum: 0x198b [validation disabled] ■ Data (20 bytes)



ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> o				
	ols <u>H</u> elp			
	业 🗐 🛢 ⊖, ⊝,	Q T	M M M M	
ilter: tcp	▼ Expression Clear	Apply		
o, Time Source	Destination	Protoco	Info	
	120.241.16.104	TCP		[ACK] Seq=276 Ack=22 Win=65516 Len=0
	64.233.189.188	TCP		ve] 57058 > hpvroom [ACK] Seq=1012 Ack=4550 Win=65048 Len=1
	192.168.1.5	TCP		ve ACK] hpvroom > 57058 [ACK] Seq=4550 Ack=1013 Win=67840 Len=0 SLE=1012 SRE=101.
	120.241.16.104	TCP		[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
	192.168.1.5	TCP		[SYN, ACK] Seq=0 Ack=1 Win=13600 Len=0 MSS=1360 SACK_PERM=1 WS=10
	120.241.16.104 120.241.16.104	TCP TCP		[ACK] Seq=1 Ack=1 Win=65536 Len=0 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=274
	192.168.1.5	TCP		[ACK] Seq=1 Ack=275 Win=15360 Len=0
	192.168.1.5	TCP		[PSH, ACK] Seq=1 Ack=275 Win=15360 Len=20
	120.241.16.104	TCP		[ACK] Seq=275 Ack=21 Win=65516 Len=0
	192.168.1.5	TCP		ission] 36688 > 57743 [PSH, ACK] Seq=1 Ack=275 Win=15360 Len=20
	120.241.16.104	TCP		15887#1] 57743 > 36688 [ACK] Seq=275 Ack=21 Win=65516 Len=0 SLE=1 SRE=21
	203.119.198.187	HTTP		or non-HTTP traffic
	192.168.1.5 192.168.1.5	TCP HTTP		[ACK] Seq=547 Ack=1226 Win=28096 Len=0 or non-HTTP traffic
13092 3407.34290 203.119.190.107	192.100.1.3	ппр	Concinuación	iii iiii-niie ti airi t
→ Differentiated Services Field: 0x00 (DSCP 0x00: Total Length: 40	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)	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]			688), Seq: 275,	Ack: 21, Len: 0



[This is an ACK to the segment in frame: 15886]
[The RTT to ACK the segment was: 0.199555000 seconds]

Microsoft - Wireshark									
<u>File Edit View Go Capture Analyze Statistics Telep</u>	hon <u>y T</u> ools <u>H</u> elp								
		⊋ ℚ ፫	T 🚉 🗵 🥦 🔆 💢						
Filter: tcp	▼ Expression Cle	ar Apply							
No. Time Source	Destination		tol Info						
15885 3487.01476120.241.16.104	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 15888 3487.25067 120.241.16.104	120.241.16.104 192.168.1.5	TCP TCP	57743 > 36688 [ACK] Seq=275 Ack=21 Win=65516 Len=0 [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						
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 15895 3488.25148 120.241.16.104	120.241.16.104 192.168.1.5	TCP TCP	57743 > 36688 [FIN, ACK] Seq=275 Ack=21 Win=65516 Len=0 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] 5eq=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						
< □			III						
Version: 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCF Total Length: 40 Identification: 0x231d (8989) Flags: 0x02 (bon'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 (120.241.16.1			86688), Seq: 275, Ack: 21, Len: 0						
Source port: 57743 (57743) Destination port: 36688 (36688) [Stream index: 1147] Sequence number: 275 (relative sequence Acknowledgement number: 21 (relative all 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]									



Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help 🖺 🕍 🖄 🕍 | 🗀 🔚 🗶 😂 🔠 | 🍳 👄 🐤 😜 📅 🛂 | 🗐 📴 | 🗨 🝳 🙊 📆 | 🖼 🖼 🛣 🥵 🎉 | Filter: tcp ▼ Expression... Clear Apply Time Destination Protocol Info Source 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 57743 > 36688 [ACK] Seq=275 Ack=21 Win=65516 Len=0 192.168.1.5 15890 3487.37655 192.168.1.5 203.119.198.187 HTTP Continuation or non-HTTP traffic http > 56963 [ACK] Seq=547 Ack=1226 Win=28096 Len=0 15891 3487, 45678 203, 119, 198, 187 192.168.1.5 15892 3487.54298 203.119.198.187 192,168,1,5 Continuation or non-HTTP traffic 15893 3487.74631 192.168.1.5 203.119.198.187 56963 > http [ACK] Seq=1226 Ack=929 Win=16445 Len=0 15894 3488, 21437 192, 168, 1, 5 120.241.16.104 57743 > 36688 [FIN, ACK] Seq=275 Ack=21 Win=65516 Len=0 15895 3488.25148 120.241.16.104 192.168.1.5 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=0 192.168.1.5 15899 3488.86929 192.168.1.5 183.192.200.4 15900 3490.01454 192.168.1.5 120, 241, 16, 104 57744 > 36688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1 Herame 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) Fragment offset: 0 Time to live: 54 Protocol: TCP (6) 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 set0.. = ECN-Echo: Not set0. = Urgent: Not set = Acknowledgement: Set 0... = Push: Not set0.. = Reset: Not set0. = Syn: Not 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;

