

西安交通大学

计算机网络大作业

实验报告

班级：计算机 86
姓名：常傲
学号：2182212573

(PS: 这次大作业的报告我在规定时间之前已经提交了，但是在考完试后老师在群里说可以在原来提交的基础上重新提交进行修改，为了让自己的报告尽善尽美一些，我就将报告再完善一下，希望能多得一些分数)

第一次实验

实验目的：

- 1、掌握路由器的基本知识
- 2、掌握路由器端口的配置
- 3、掌握路由协议的基本配置
- 4、熟悉使用 Boson Netsim 模拟器

实验内容：

- 1、使用 IOS 命令配置路由器
- 2、掌握静态路由和动态路由（RIP、OSPF）的配置方法

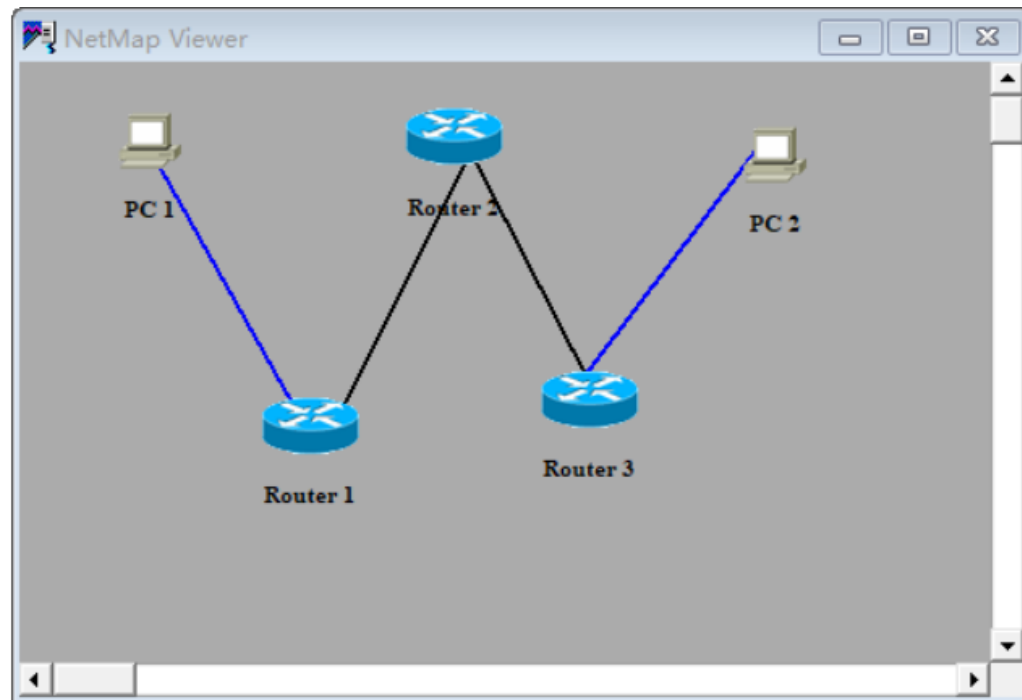
实验要求：

自行构建一个网络拓扑，要求包括 3 个以上路由器，用于连接两个以太网，每个以太网至少包括 1 台主机；

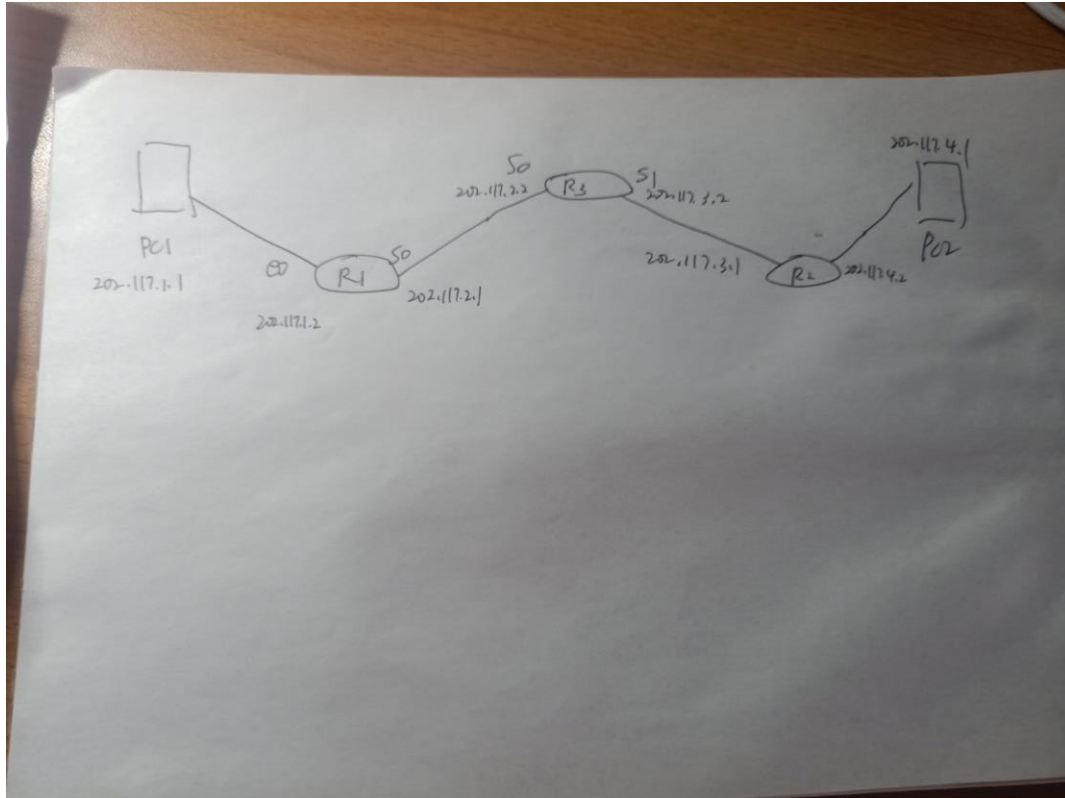
路由器配置 RIP 或 OSPF 来维护路由表；

任意两个主机之间通过 ping 命令能够连通

拓扑图：



自己画的全局图（包含 IP 地址）



先对路由器进行 ip 分配

R1:

enable

ip config

int e0

ip address 202.117.1.2 255.255.255.0

no shutdown

int s0

ip address 202.117.2.1 255.255.255.0

clock rate 64000

no shut

end

```

Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int e0
Router(config-if)#ip address 202.117.1.2 255.255.255.0
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
Router(config-if)#int s0
Router(config-if)#ip address 202.117.2.1
% Incomplete command.
Router(config-if)#ip address 202.117.2.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Router(config-if)#end
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route

Gateway of last resort is not set
C      202.117.1.0/24 is directly connected, Ethernet0
C      202.117.2.0/24 is directly connected, Serial0

Router#

```

R2:

enable

config terminal

int e0

ip address 202.117.4.2 255.255.255.0

no shut

int s0

ip address 202.117.3.1 255.255.255.0

clock rate 64000

no shut

end

```

Press Enter to Start

Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int e0
Router(config-if)#ip address 202.117.4.2 255.255.255.0
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
Router(config-if)#int s0
Router(config-if)#ip address 202.117.3.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Router(config-if)#end
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route

Gateway of last resort is not set
C      202.117.4.0/24 is directly connected, Ethernet0
C      202.117.3.0/24 is directly connected, Serial0

%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down

Router#

```

R3:
enable
config terminal
int s0
ip address 202.117.2.2 255.255.255.0
clock rate 64000
no shut
int s1
ip address 202.117.3.2 255.255.255.0
clock rate 64000
no shut
end

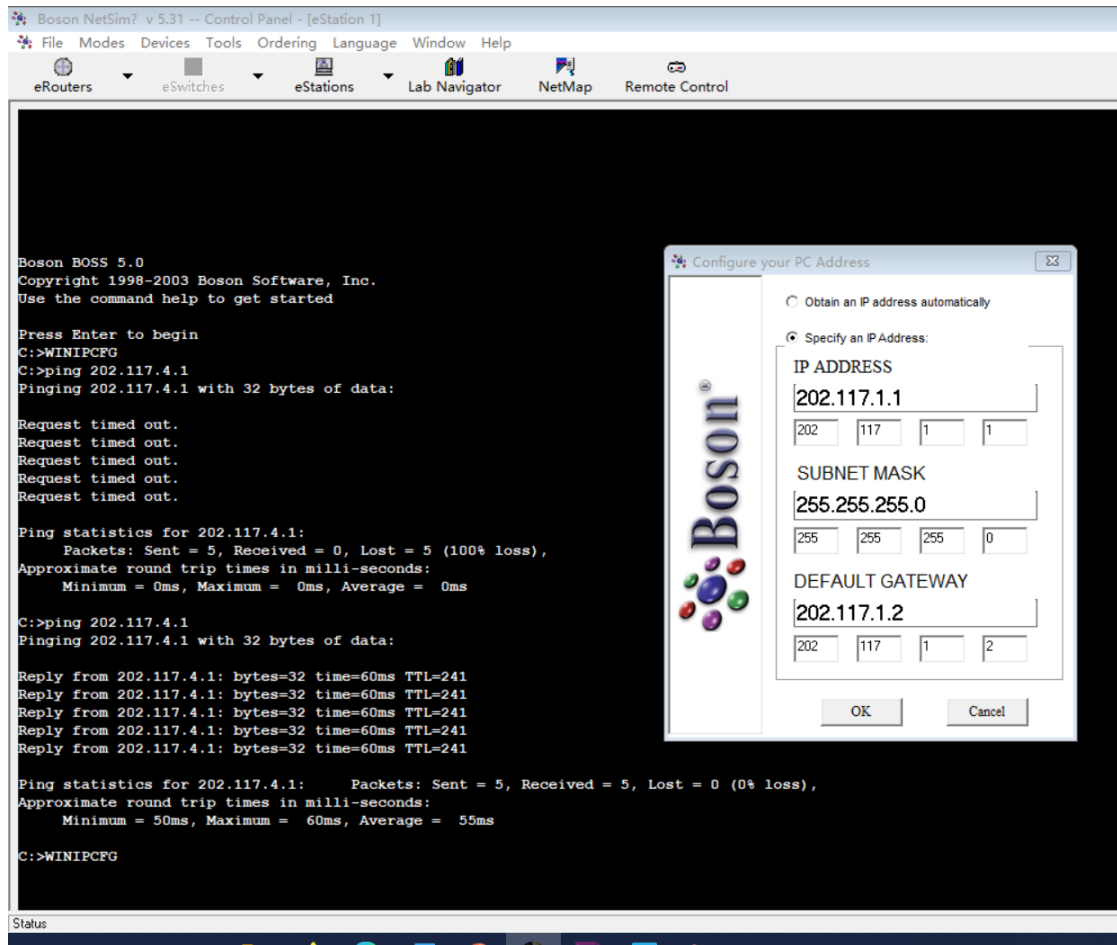
Press Enter to Start

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0
Router(config-if)#ip address 202.117.2.2 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Router(config-if)#int s1
Router(config-if)#ip address 202.117.3.2 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial1, changed state to up
Router(config-if)#end
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

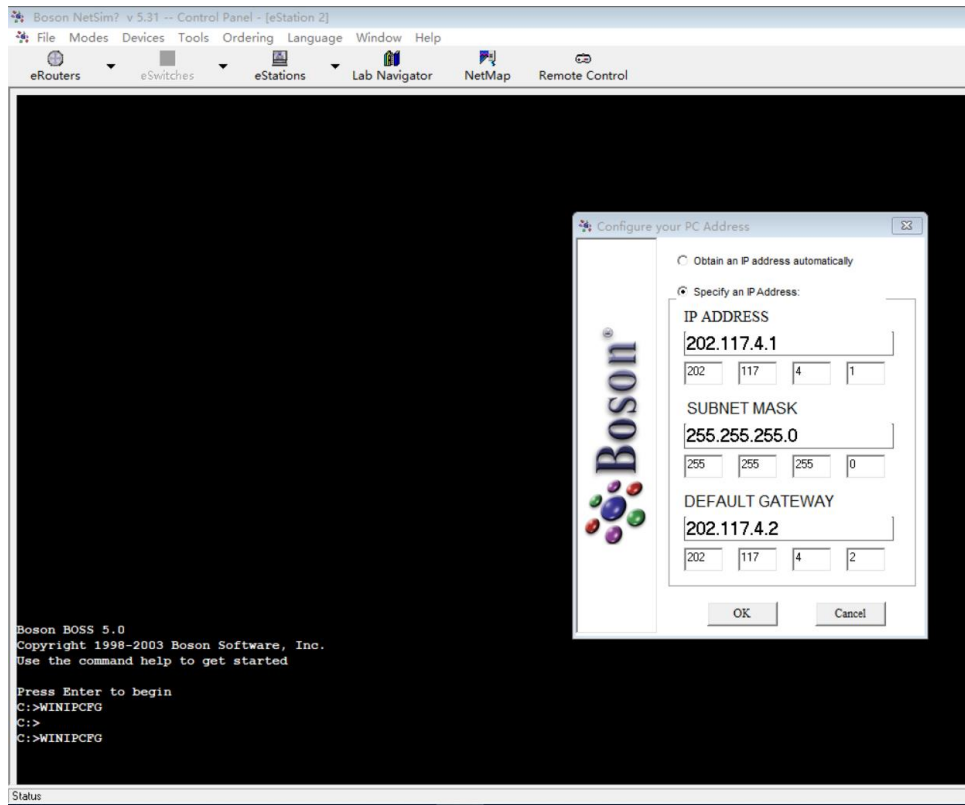
Gateway of last resort is not set
C      202.117.2.0/24 is directly connected, Serial0
C      202.117.3.0/24 is directly connected, Serial1

Router#
```

接下来是主机
PC1:



PC2:



众所周知，boson netsim 可以有两种分配 IP 地址的方法（RIP 和 OSPF），我将这两种方法都尝试了一下而且都成功了，如图：

静态：

R1:

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 202.117.3.0 255.255.255.0 202.117.2.2
Router(config)#ip route 202.117.4.0 255.255.255.0 202.117.2.2
Router(config)#end
```

R2:

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 202.117.1.0 255.255.255.0 202.117.3.2
Router(config)#ip route 202.117.2.0 255.255.255.0 202.117.3.2
Router(config)#end
```

R3:

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 202.117.1.0 255.255.255.0 202.117.2.1
Router(config)#ip route 202.117.4.0 255.255.255.0 202.117.3.1
Router(config)#end
```

结果：

```
C:>ping 202.117.4.1
Pinging 202.117.4.1 with 32 bytes of data:

Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241

Ping statistics for 202.117.4.1:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 60ms, Average = 55ms
```

动态：

R1:

```
Router#enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 202.117.1.0
Router(config-router)#network 202.117.2.0
Router(config-router)#end

Router#
```

R2:

```
Router#enable
Router#router rip
% Invalid input detected at '^' marker.

Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 202.117.3.0
Router(config-router)#network 202.117.4.0

Router(config-router)#
```

R3:

```
Router#enable
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 202.117.1.0 255.255.255.0 202.117.2.1
Router(config)#ip route 202.117.4.0 255.255.255.0 202.117.3.1
Router(config)#end
Router#enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 202.117.2.0
Router(config-router)#network 202.117.3.0
Router(config-router)#end

Router#
```

Status

结果:

```
C:>ping 202.117.4.1
Pinging 202.117.4.1 with 32 bytes of data:

Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241
Reply from 202.117.4.1: bytes=32 time=60ms TTL=241

Ping statistics for 202.117.4.1:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 60ms, Average = 55ms
```

心得体会:

路由器是工作在网络层的设备，隔绝了广播域。因此，路由器的每个端口号都连着不同的网路号（即连接不同的子网）。刚开始的我由于疏忽大意加上知识掌握不牢固，使得我走了很多的弯路。于是查找很多网上的资料什么的，才逐渐明白这次实验的精髓。由于我是在十一月份就做完了这次试验，所以也趁热打铁复习了关于掩码、网关等知识，对网络层和数据链路层的层次结构更加清晰了

实验二

实验目的：

- 利用 ethereal 软件分析 HTTP 及其下层协议（TCP 协议）
- 了解网络中数据封装的概念
- 掌握 HTTP 及 TCP 协议的工作过程。

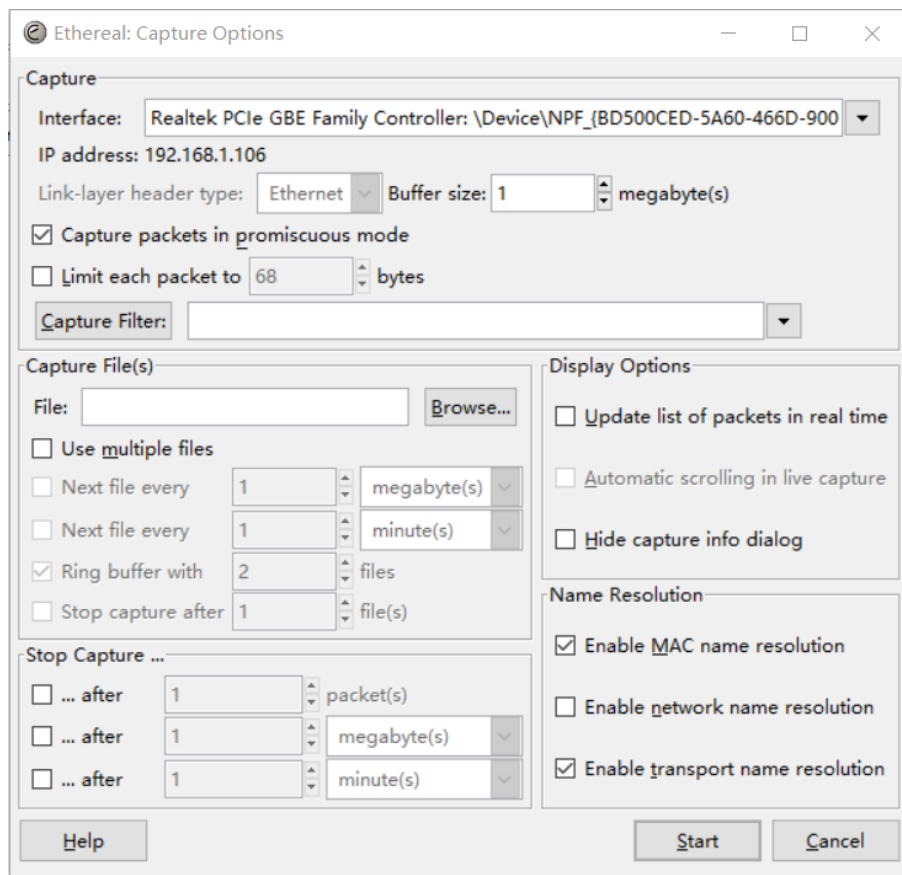
实验内容：

- 启动 ethereal 软件，进行报文截获
- 在浏览器访问 www.xjtu.edu.cn 页面。（打开网页，浏览并关闭页面）
- 停止 ethereal 的报文截获，将截获命名为“http—学号”
- 分析截获报文。

实验要求：

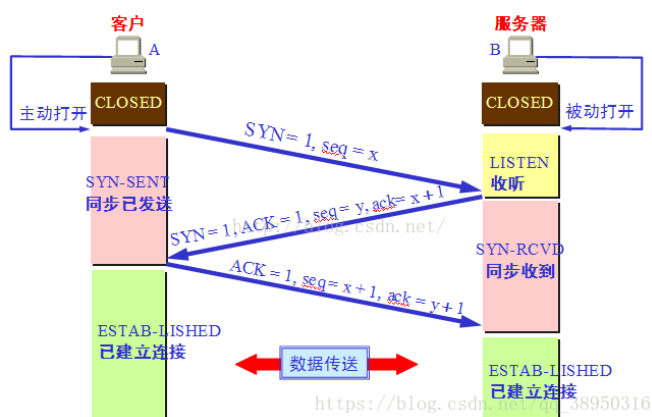
- 从截获的报文中选择 HTTP 请求报文（即 get 报文）和 HTTP 应答报文，并分析各字段的值；
- 综合分析截获的报文，概括 HTTP 协议的工作过程；
- 从截获报文中选择 TCP 建立连接和释放连接的报文，分析各个字段的值并概括 HTTP 协议的工作过程；

连接建立



4184	7.433422	2001:250:1001:2500	2600:1901:0:38d7::	HTTP	Continuation or non-HTTP traffic
4190	7.457144	115.154.93.157	202.117.19.114	TCP	55275 > http [SYN, ACK] Seq=0 Len=0 MSS=1440 WS=8
4191	7.457960	202.117.19.114	115.154.93.157	TCP	http > 55275 [SYN, ACK] Seq=0 Ack=1 win=3737600 Len=0 MSS=1460 WS=7
4192	7.458277	115.154.93.157	202.117.19.114	TCP	55275 > http [ACK] Seq=1 Ack=1 win=1059840 Len=0
4196	7.491552	2600:1901:0:38d7::	2001:250:1001:2500	TCP	http > 55207 [ACK] Seq=0 Ack=1 win=261 Len=0 SLE=0 SRE=1
4197	7.631158	115.154.93.157	117.18.237.29	HTTP	Continuation or non-HTTP traffic
4200	7.665112	2001:250:1001:2500	2600:1901:0:38d7::	HTTP	Continuation or non-HTTP traffic
4201	7.720050	2600:1901:0:38d7::	2001:250:1001:2500	TCP	http > 55212 [ACK] Seq=0 Ack=1 win=261 Len=0 SLE=0 SRE=1
4202	8.097506	115.154.93.157	34.107.221.82	HTTP	Continuation or non-HTTP traffic
4203	8.289569	115.154.93.157	117.18.237.29	TCP	55236 > http [FIN, ACK] Seq=0 Ack=0 win=517 Len=0
4204	8.313445	34.107.221.82	115.154.93.157	TCP	http > 55211 [ACK] Seq=0 Ack=1 win=261 Len=0 SLE=0 SRE=1
4205	8.470691	115.154.93.157	111.6.243.174	HTTP	Continuation or non-HTTP traffic
4206	8.482705	111.6.243.174	115.154.93.157	TCP	http > 55228 [ACK] Seq=0 Ack=1 win=60 Len=0 SLE=0 SRE=1

连接建立（三次握手）



第一步：客户机的 TCP 向服务器的 TCP 发送一个连接请求报文，这个报文段有几个特殊字段。首部 SYN=1，表示同步，seq=0 表示起始符号。

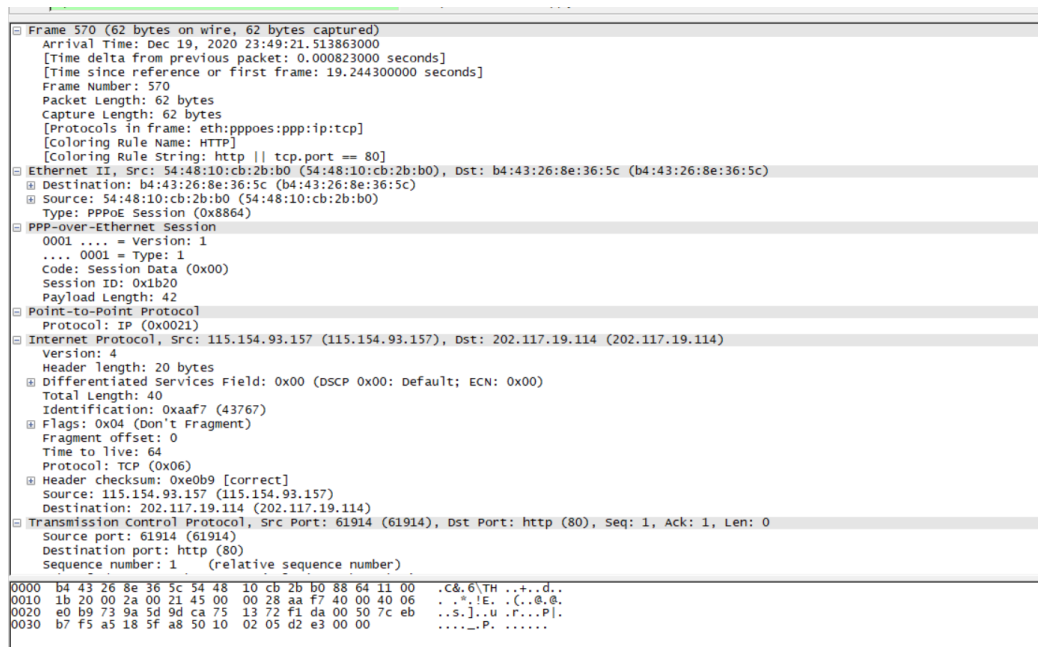
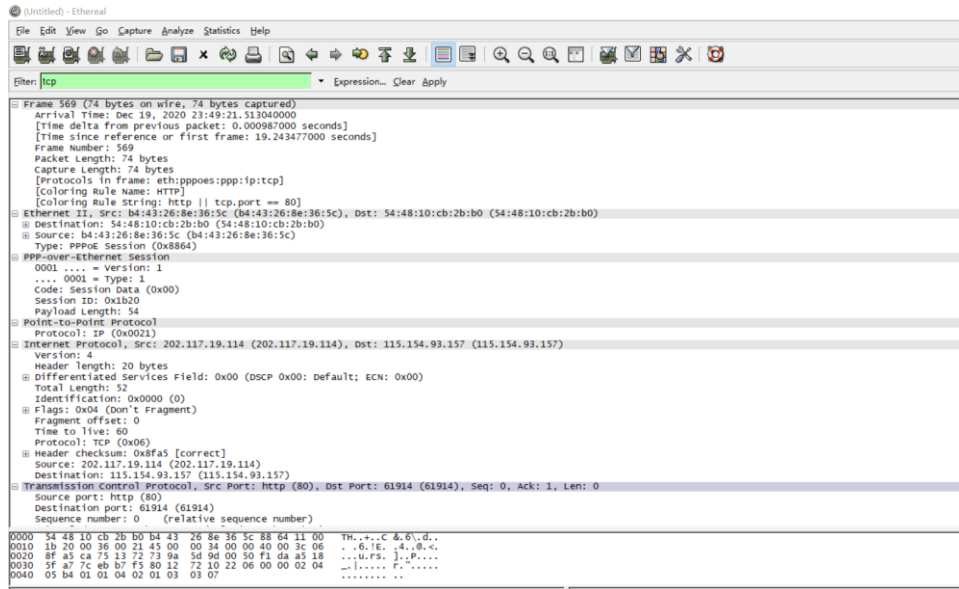
第二步：服务器收到请求报文后，如同意则回复一个确认报文。确认段中，SYN 和 ACK 均为 1，ACK 表示确认位且 ACK=seq+1；

第三步：ACK=1，Seq=1，向服务器发送确认包 ACK(ack=y+1)，此包发送完毕，客户端和服务端进入（TCP 连接成功）状态，完成三次握手。

http 报文段分析：

Frame 568 (74 bytes on wire, 74 bytes captured)	
Arrival Time: Dec 19, 2020 23:49:21.512053000	
[Time delta from previous packet: 0.106551000 seconds]	
[Time since reference or first frame: 19.242490000 seconds]	
Frame Number: 568	
Packet Length: 74 bytes	
Capture Length: 74 bytes	
Protocols in frame: eth:pppoe:ppp:ip:tcp	
[Coloring Rule Name: HTTP]	
[Coloring Rule String: http tcp.port == 80]	
Ethernet II, Src: 54:84:10:cb:2b:b0 (54:84:10:cb:2b:b0), Dst: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)	
Destination: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)	
Source: 54:84:10:cb:2b:b0 (54:84:10:cb:2b:b0)	
Type: PPPoE Session (0x864)	
PPP-over-Ethernet Session	
0001 = Version: 1	
.... 0001 = Type: 1	
Code: Session Data (0x00)	
Session ID: 0x1b20	
Payload Length: 54	
Point-to-Point Protocol	
Protocol: IP (0x0021)	
Internet Protocol, Src: 115.154.93.157 (115.154.93.157), Dst: 202.117.19.114 (202.117.19.114)	
Version: 4	
Header length: 20 bytes	
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)	
Total Length: 52	
Identification: 0xaa66 (43766)	
Flags: 0x04 (Don't Fragment)	
Fragment offset: 0	
Time to live: 64	
Protocol: TCP (0x06)	
Header checksum: 0x0aae [correct]	
Source: 115.154.93.157 (115.154.93.157)	
Destination: 202.117.19.114 (202.117.19.114)	
Transmission Control Protocol, Src Port: 61914 (61914), Dst Port: http (80), Seq: 0, Len: 0	
Source port: 61914 (61914)	
Destination port: http (80)	
Sequence number: 0 (relative sequence number)	
<pre> 0000 04 43 26 8e 36 5c 24 48 10 c9 20 00 00 11 00 .C&6\H...+... 0010 1b 20 00 36 00 21 45 00 00 34 aa f6 40 00 40 06 .6\E...A...S. 0020 e0 ae 73 9a 5d 9d ca 75 13 72 f1 da 00 50 7c eb .s].u...P . 0030 b7 f4 05 00 50 00 80 02 fd 20 9b d9 00 00 02 04 0040 05 a0 01 03 08 01 01 04 02 </pre>	

可以看出，报文的客户端是 115.154.93.157，目的是 202.117.19.114，使用的是 IPV4 协议，源端口号是 61914（49152~65535 是客户端的端口号），服务器端口号是 80（http 端口号，服务器端口号范围是 0~49151，其中 0~1023 是常用的）等等，在此不赘述。

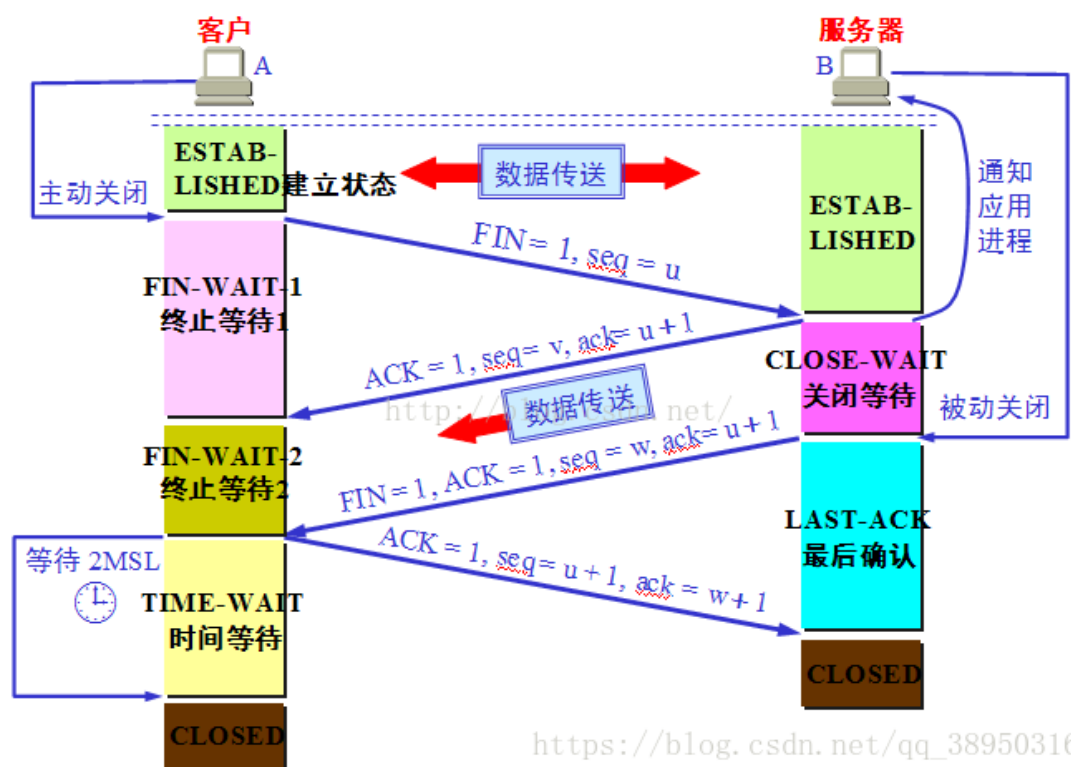


连接释放

天下没有不散的宴席，所以连接有建立就要有释放。连接的释放则是四次握手。

4789	12.484724	115.154.93.157	111.19.223.35	SSL	Continuation Data
4790	12.484738	115.154.93.157	202.117.19.114	TCP	55275 > http [FIN, ACK] Seq=1 Ack=1 win=1059840 Len=0
4791	12.484805	115.154.93.157	111.19.223.35	TCP	55278 > https [ACK] Seq=2739 Ack=10473 win=131072 Len=0
4792	12.484860	115.154.93.157	111.19.223.35	TCP	55278 > https [ACK] Seq=2739 Ack=11793 win=129792 Len=0
4853	12.495967	111.19.223.35	115.154.93.157	SSL	Continuation Data
4854	12.495967	202.117.19.114	115.154.93.157	TCP	http > 55275 [ACK] Seq=1 Ack=2 win=29312 Len=0
4855	12.495967	202.117.19.114	115.154.93.157	TCP	http > 55275 [FIN, ACK] Seq=1 Ack=2 win=29312 Len=0
4856	12.495967	111.19.223.35	115.154.93.157	TCP	[TCP segment of a reassembled PDU]
4857	12.495968	111.19.223.35	115.154.93.157	TCP	[TCP segment of a reassembled PDU]
4858	12.495969	111.19.223.35	115.154.93.157	TCP	[TCP segment of a reassembled PDU]

还有一次的分手报文不知道为什么找不到了……



第一步：客户机打算释放连接，于是发出连接释放报文，并且停止发送数据。释放数据报文首部，FIN=1，其序列号为 seq=u，它等于前面已经传送过来的数据的最后一个字节的序号加 1，此时，客户端进入 FIN-WAIT-1（终止等待 1）状态。TCP 规定，FIN 报文段即使不携带数据，也要消耗一个序号。TCP 是全双工的，所以一条连接等效有两条通路

第二步：服务器收到连接释放报文，发出确认报文，ACK=1，ack=u+1，并且带上自己的序列号 seq=v，此时，服务端就进入了 CLOSE-WAIT（关闭等待）状态。TCP 服务器通知高层的应用进程，客户端向服务器的方向就释放了，这时候处于半关闭状态，即客户端已经没有数据要发送了，但是服务器若发送数据，客户端依然要接受。这个状态还要持续一段时间，也就是整个 CLOSE-WAIT 状态持续的时间。客户端收到服务器的确认请求后，此时，客户端就进入 FIN-WAIT-2（终止等待 2）状态，等待服务器发送连接释放报文（在这之前还需要接受服务器发送的最后的的数据）。

第三步：服务器将最后的数据发送完毕后，就向客户端发送连接释放报文，FIN=1，ack=u+1，由于在半关闭状态，服务器很可能又发送了一些数据，假定此时的序列号为 seq=w，此时，服务器就进入了 LAST-ACK（最后确认）状态，等待客户端的确认。

第四步：客户端收到服务器的连接释放报文后，必须发出确认，ACK=1，ack=w+1，而自己的序列号是 seq=u+1，此时，客户端就进入了 TIME-WAIT（时间等待）状态。注意此时 TCP 连接还没有释放，必须经过 $2 \times \text{MSL}$ （最长报文段寿命）的时间后，当客户端撤销相应的 TCB 后，才进入 CLOSED 状态。服务器只要收到了客户端发出的确认，立即进入 CLOSED 状态。同样，撤销 TCB 后，就结束了这次的 TCP 连接。可以看到，服务器结束 TCP 连接的时间要比客户端早一些。

http 报文段分析:

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: tcp Expression... Clear Apply

Frame 596 (62 bytes on wire, 62 bytes captured)
Arrival Time: Dec 19, 2020 23:49:24.784007000
[Time delta from previous packet: 0.000117000 seconds]
[Time since reference or first frame: 22.514444000 seconds]
Frame Number: 596
Packet Length: 62 bytes
Capture Length: 62 bytes
[Protocols in frame: eth:pppoe:ppp:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0), Dst: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)
Destination: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)
Source: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0)
Type: PPPoE Session (0x8864)
PPPoE-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x1b20
Payload Length: 42
Point-to-Point Protocol
Protocol: IP (0x0021)
Internet Protocol, Src: 115.154.93.157 (115.154.93.157), Dst: 117.18.237.29 (117.18.237.29)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 40
Identification: 0x3df8 (15864)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0xc970 [correct]
Source: 115.154.93.157 (115.154.93.157)
Destination: 117.18.237.29 (117.18.237.29)
Transmission Control Protocol, Src Port: 61904 (61904), Dst Port: http (80), Seq: 1, Ack: 0, Len: 0
Source port: 61904 (61904)
Destination port: http (80)
Sequence number: 1 (calculated sequence number)
0000 b4 43 26 8e 36 5c 54 48 10 cb 2b b0 88 64 11 00 .C&.6\TH .+.d..
0010 1b 20 00 2a 00 21 45 00 00 28 3d f8 40 00 40 06 .*.!E. .(B.@.<.
0020 c9 70 73 9a 5d 9d 75 12 ed 1d f1 00 00 50 62 c2 .ps.]u.pb.
0030 08 46 56 df 8c 47 50 11 02 02 3a 1a 00 00 .FV.GP.

No..	Time	Source	Destination	Protocol	Info
Frame 601 (68 bytes on wire, 68 bytes captured) Arrival Time: Dec 19, 2020 23:49:24.784830000 [Time delta from previous packet: 0.000382000 seconds] [Time since reference or first frame: 22.515267000 seconds] Frame Number: 601 Packet Length: 68 bytes Capture Length: 68 bytes [Protocols in frame: eth:pppoe:ppp:ip:tcp] [Coloring Rule Name: HTTP] [Coloring Rule String: http tcp.port == 80]					
Ethernet II, Src: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c), Dst: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0)					
Destination: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0)					
Source: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)					
Type: PPPoE Session (0x8864)					
PPPoE-over-Ethernet Session					
0001 = Version: 1					
.... 0001 = Type: 1					
Code: Session Data (0x00)					
Session ID: 0x1b20					
Payload Length: 42					
Point-to-Point Protocol					
Protocol: IP (0x0021)					
Internet Protocol, Src: 202.117.19.114 (202.117.19.114), Dst: 115.154.93.157 (115.154.93.157)					
Version: 4					
Header length: 20 bytes					
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)					
Total Length: 40					
Identification: 0x42d4 (17108)					
Flags: 0x04 (Don't Fragment)					
Fragment offset: 0					
Time to live: 60					
Protocol: TCP (0x06)					
Header checksum: 0x4cdd [correct]					
Source: 202.117.19.114 (202.117.19.114)					
Destination: 115.154.93.157 (115.154.93.157)					
Transmission Control Protocol, Src Port: http (80), Dst Port: 61914 (61914), Seq: 1, Ack: 2, Len: 0					
Source port: http (80)					
Destination port: 61914 (61914)					
0000 54 48 10 cb 2b b0 b4 43 26 8e 36 5c 88 64 11 00 TH..+.C &.6\d.. 0010 1b 20 00 2a 00 21 45 00 00 28 42 d4 40 00 3c 06 .*.!E. .(B.@.<. 0020 4c dd ca 75 13 72 73 9a 5d 9d 00 50 f1 da a5 18 L..u.rs.]..P.... 0030 5f a8 7c eb b7 f6 50 11 00 e5 d4 01 00 00 00 00 -- ...P. 0040 00 00 00 00					

Frame 629 (62 bytes on wire, 62 bytes captured)
 Arrival Time: Dec 19, 2020 23:49:25.198068000
 [Time delta from previous packet: 0.076801000 seconds]
 [Time since reference or first frame: 22.928505000 seconds]
 Frame Number: 629
 Packet Length: 62 bytes
 Capture Length: 62 bytes
 [Protocols in frame: eth:pppoe:ppp:ip:tcp]
 [Coloring Rule Name: HTTP]
 [Coloring Rule String: http || tcp.port == 80]

Ethernet II, Src: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0), Dst: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)
 Destination: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)
 Source: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0)
 Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x1b20
 Payload Length: 42

Point-to-Point Protocol
 Protocol: IP (0x0021)

Internet Protocol, Src: 115.154.93.157 (115.154.93.157), Dst: 117.18.237.29 (117.18.237.29)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 40
 Identification: 0x3df9 (15865)
 Flags: 0x04 (Don't Fragment)
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (0x06)
 Header checksum: 0xc96f [correct]
 Source: 115.154.93.157 (115.154.93.157)
 Destination: 117.18.237.29 (117.18.237.29)

Transmission Control Protocol, Src Port: 61904 (61904), Dst Port: http (80), Seq: 1, Ack: 0, Len: 0
 Source port: 61904 (61904)
 Destination port: http (80)
 Sequence number: 1 (relative sequence number)

0000	b4 43 26 8e 36 5c 54 48 10 cb 2b b0 88 64 11 00	.C&6\TH ..+.d..
0010	1b 20 00 2a 00 21 45 00 00 28 3d f9 40 00 40 06	. .*.!E. .(=.@.@.
0020	c9 6f 73 9a 5d 9d 75 12 ed 1d f1 d0 00 50 62 c2	.os.]u.Pb.
0030	08 46 56 df 8c 47 50 11 02 02 3a 1a 00 00	.FV..GP.

File: "C:\Users\DELL\AppData\Local\Temp\etherXXXXB3OTV0" 267 KB 00:00:23 | P: 633 D: 346

File Edit View Go Capture Analyze Statistics Help

Filter: tcp Expression: Clear Apply

Frame 601 (68 bytes on wire, 68 bytes captured)
 Arrival Time: Dec 19, 2020 23:49:24.784830000
 [Time delta from previous packet: 0.000382000 seconds]
 [Time since reference or first frame: 22.915267000 seconds]
 Frame Number: 601
 Packet Length: 68 bytes
 Capture Length: 68 bytes
 [Protocols in frame: eth:pppoe:ppp:ip:tcp]
 [Coloring Rule Name: HTTP]
 [Coloring Rule String: http || tcp.port == 80]

Ethernet II, Src: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c), Dst: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0)
 Destination: 54:48:10:cb:2b:b0 (54:48:10:cb:2b:b0)
 Source: b4:43:26:8e:36:5c (b4:43:26:8e:36:5c)
 Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x1b20
 Payload Length: 42

Point-to-Point Protocol
 Protocol: IP (0x0021)

Internet Protocol, Src: 202.117.19.114 (202.117.19.114), Dst: 115.154.93.157 (115.154.93.157)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 40
 Identification: 0x42d4 (17108)
 Flags: 0x04 (Don't Fragment)
 Fragment offset: 0
 Time to live: 60
 Protocol: TCP (0x06)
 Header checksum: 0x4cdd [correct]
 Source: 202.117.19.114 (202.117.19.114)
 Destination: 115.154.93.157 (115.154.93.157)

Transmission Control Protocol, Src Port: http (80), Dst Port: 61914 (61914), Seq: 1, Ack: 2, Len: 0
 Source port: http (80)
 Destination port: 61914 (61914)
 Sequence number: 1 (relative sequence number)

000	54 48 10 cb 2b b0 b4 43 26 8e 36 5c 88 64 11 00	TH..+.C &6\d..
010	1b 20 00 2a 00 21 45 00 00 28 42 d4 40 00 3c 06	. .*.!E. .(B.@.<.
020	4c dd ca 75 13 72 73 9a 5d 9d 00 50 f1 da a5 18	L..u.r.s.]..P....
030	5f a8 7c eb b7 f6 50 11 00 e5 d4 01 00 00 00 00P.
040	00 00 00 00


```

Hypertext Transfer Protocol
GET /images/18/01/23/1ay37aq43t/icon_r_1.png HTTP/1.1\r\n
Request Method: GET
Request URI: /images/18/01/23/1ay37aq43t/icon_r_1.png
Request Version: HTTP/1.1
Host: www.xjtu.edu.cn\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0\r\n
Accept: image/webp,*/*\r\n
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Referer: http://www.xjtu.edu.cn/\r\n
\r\n

```

Get 报文分析:

可以看出，网站的服务器是"www.xjtu.edu.cn/";

使用的是 http1.1 连续连接协议，

URI 是网站中的某个图片

使用的浏览器是火狐浏览器 83.0 版本

接受网站是中国境内的

Keep-active 意思是持久连接

等等

http 响应报文

```

... .. = urgent: not set
... .. = Acknowledgment: Set
... .. = Push: Set
... .. = Reset: Not set
... .. = Syn: Not set
... .. = Fin: Not set
window size: 16640 (scaled)
checksum: 0x71b9 [correct]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Request Version: HTTP/1.1
Response code: 200
Date: Sat, 19 Dec 2020 15:49:13 GMT\r\n
Server: VwebServer\r\n
X-Frame-Options: SAMEORIGIN\r\n
Last-Modified: Thu, 24 Aug 2017 03:18:31 GMT\r\n
ETag: "3e5-5577748672fc0"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 997\r\n
Cache-Control: max-age=3600\r\n
Expires: Sat, 19 Dec 2020 16:49:13 GMT\r\n
Keep-Alive: timeout=5, max=199\r\n
Connection: Keep-Alive\r\n
Content-Type: image/png\r\n
Content-Language: zh-CN\r\n
\r\n
Media Type: image/png (997 bytes)

```

协议仍然是 http1.1 协议

Date: Tue, 12 Nov 2019 03: 05: 59 GMT 指当前日期

Content-Length: 997，报文主题的长度为 56542 字节

Connection keep-alive，表示是持久连接

Last-Modified: Tue, 12 Nov 2019 02: 51: 31 GMT，源头服务器认定的资源做出修改的日期及时间。

ETag:"3e5-5577748672fc0"，资源的特定版本的标识符。这可以让缓存更高效，并节省带宽，因为如果内容没有改变，Web 服务器不需要发送完整的响应。而如果内容发生了变化，使用 ETag 有助于防止资源的同时更新相互覆盖。

Accept-Ranges: bytes，范围请求的单位是 bytes（字节）。

Content-Language: zh-CN，所使用的语言为中文

等等

心得体会：

这次实验让我对于 tcp 连接的三次握手四次握手有了更加深刻的了解。我也开始对 http 有了更加具体的印象而非抽象的概念。Tcp 工作在传输层而 http 工作在应用层，所以两者之间有着 SAP 的联系使得二者某种程度上是密不可分的。无论如何也学不懂的知识也在实验结束的一瞬间豁然开朗。