计算机网络大作业（实验）

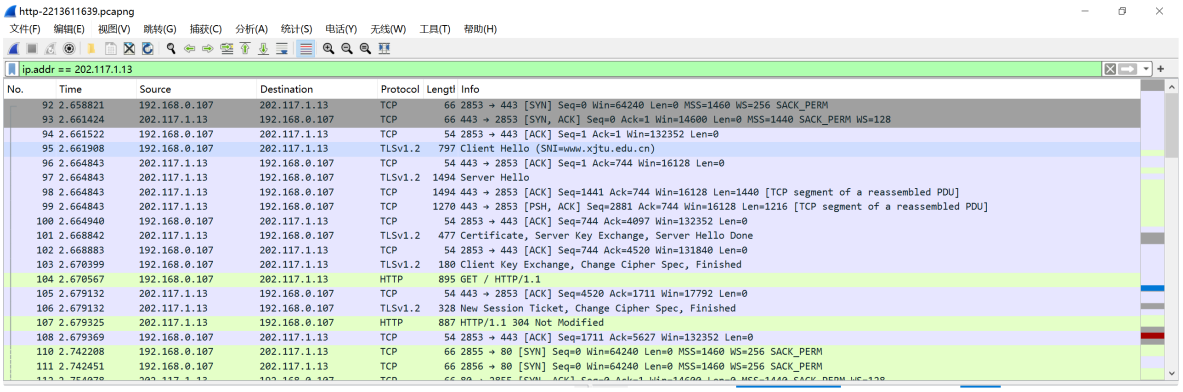
wireshark抓包

```
PS C:\Users\learningyu> ping www.xjtu.edu.cn

正在 Ping www.xjtu.edu.cn [202.117.1.13] 具有 32 字节的数据:
来自 202.117.1.13 的回复: 字节=32 时间=23ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=24ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=7ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=48ms TTL=60

202.117.1.13 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 7ms, 最长 = 48ms, 平均 = 25ms
PS C:\Users\learningyu>
```

通过Ping查出www.xjtu.end.cn的ip地址为

www.xjtu.edu.cn 的IP:202.117.1.13

抓到的包



Http分析

HTTP请求报文

物理层的数据帧详细概要

```
Frame 104: 895 bytes on wire (7160 bits), 895 bytes captured (7160 bits) on interface \Device\NP
   Section number: 1
   Interface id: 0 (\Device\NPF_{1A827331-F875-4CCC-82E9-6A2496560E55})
      Interface name: \Device\NPF_{1A827331-F875-4CCC-82E9-6A2496560E55}
      Interface description: WLAN
   Encapsulation type: Ethernet (1)
   Arrival Time: Dec 24, 2023 22:09:12.101457000 中国标准时间
   UTC Arrival Time: Dec 24, 2023 14:09:12.101457000 UTC
   Epoch Arrival Time: 1703426952.101457000
   [Time shift for this packet: 0.000000000 seconds]
   [Time delta from previous captured frame: 0.000168000 seconds]
   [Time delta from previous displayed frame: 0.000168000 seconds]
   [Time since reference or first frame: 2.670567000 seconds]
   Frame Number: 104
   Frame Length: 895 bytes (7160 bits)
   Capture Length: 895 bytes (7160 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:ethertype:ip:tcp:tls:http]
   [Coloring Rule Name: HTTP]
   [Coloring Rule String: http || tcp.port == 80 || http2]
```

可以看出以下信息：为104号帧、线路字节7160字节，实际捕获895字节。端口为0号端口，端口在计算机中命名为WALN。采取的封装方式为Ethernet（与wireshark版本有关）。捕获的时间和日期为2023年11月24日 22：09：12秒左右。以及一些和帧有关的时间信息。该帧没有被标记，也没有被忽略。该帧的协议为HTTP,tcp端口号80

数据链路层以太网帧的头部信息

```
Ethernet II, Src: Intel_49:8b:03 (4c:79:6e:49:8b:03), Dst: TendaTechnol_81:7f:70 (58:d9:d5:81:7f:70
   Destination: TendaTechnol_81:7f:70 (58:d9:d5:81:7f:70)
      Address: TendaTechnol_81:7f:70 (58:d9:d5:81:7f:70)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Source: Intel_49:8b:03 (4c:79:6e:49:8b:03)
      Address: Intel_49:8b:03 (4c:79:6e:49:8b:03)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
```

两个信息：目的的MAC地址和源的MAC地址

网络层IP头部包信息

```
Internet Protocol Version 4, Src: 192.168.0.107, Dst: 202.117.1.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 881
    Identification: 0x4a12 (18962)
  010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.107
    Destination Address: 202.117.1.13
```

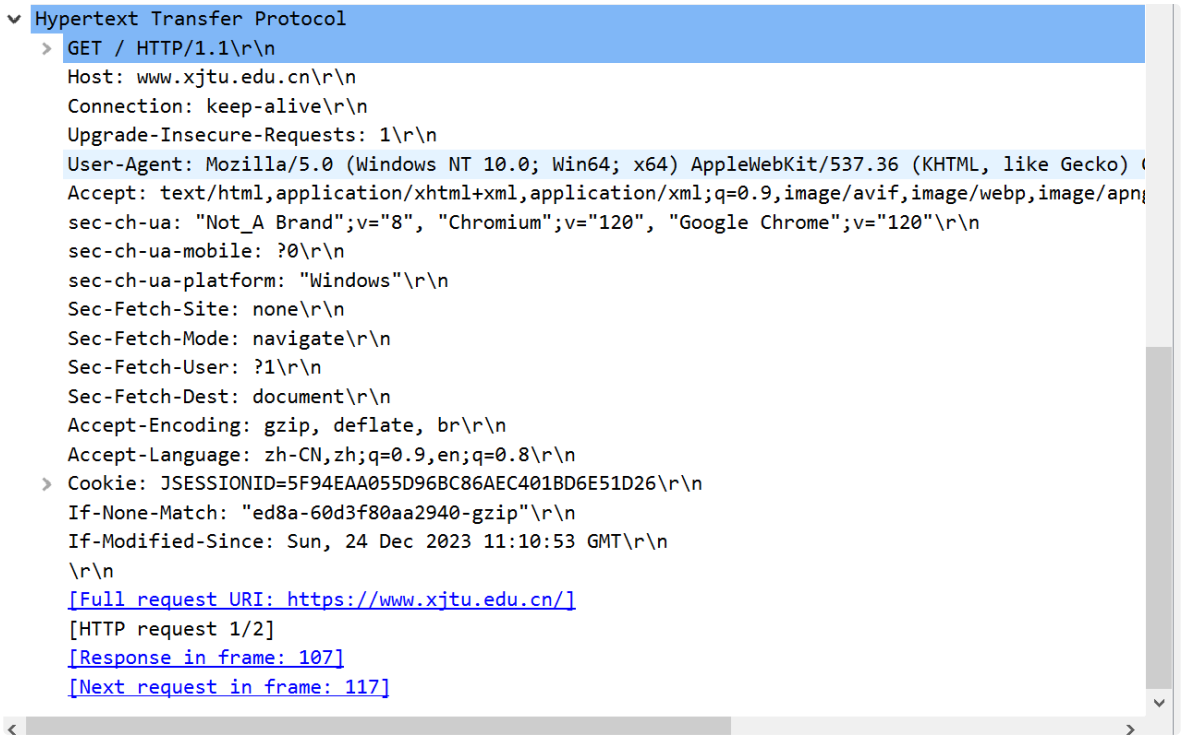
可以看出：使用了IPV4协议，ip包头长20字节。IP包共长881字节，标记字段为18962.生存周期64。源IP地址192.168.0.107，目的IP地址202.117.1.13(学校官网)

传输层数据包头部信息

```
Transmission Control Protocol, Src Port: 2853, Dst Port: 443, Seq: 870, Ack: 4520, Len: 841
    Source Port: 2853
    Destination Port: 443
    [Stream index: 18]
  [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 841]
    Sequence Number: 870    (relative sequence number)
    Sequence Number (raw): 4294410742
    [Next Sequence Number: 1711    (relative sequence number)]
    Acknowledgment Number: 4520    (relative ack number)
    Acknowledgment number (raw): 4219520484
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    Window: 515
    [Calculated window size: 131840]
    [Window size scaling factor: 256]
    Checksum: 0x8ff9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
    TCP payload (841 bytes)
```

可以看出以下信息：源端口为2853，目的端口为443.流量控制端口大小为131840

应用层分析



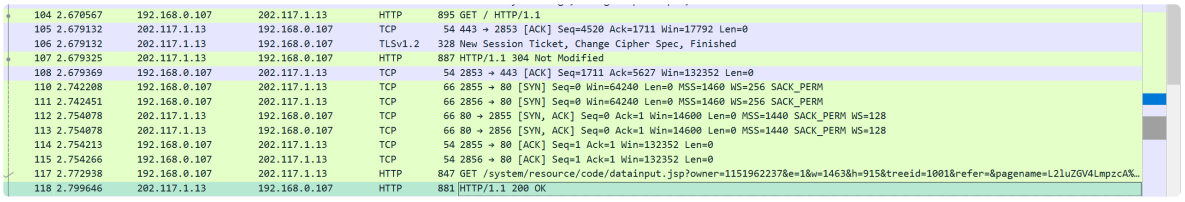
就是具体的http报文.给出了请求主机的名字，还给出了自身的一些信息，比如浏览器是chromium,系统是windows,能接受的语言是中文简体，cookie等等

HTTP应答报文

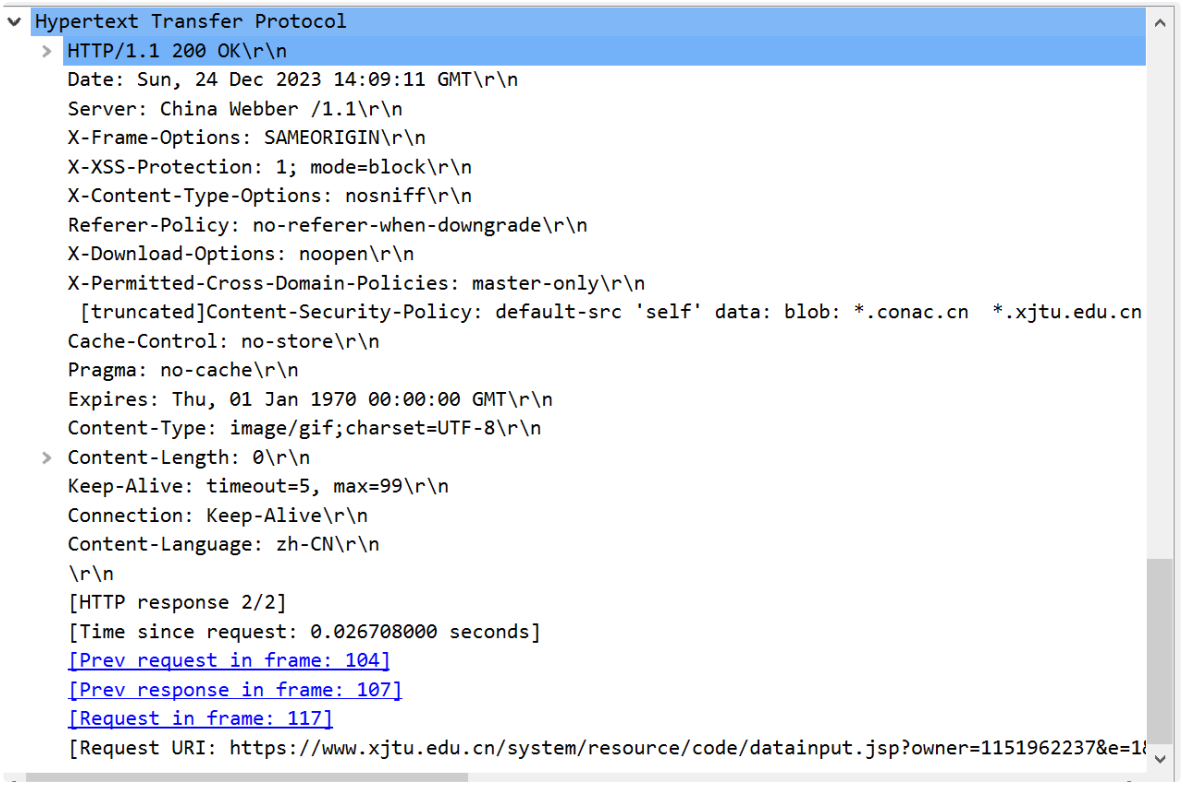
前面的物理层、数据链路层、网络层、传输层和HTTP请求报文大同小异。看看应用具体的HTTP报文。

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Sun, 24 Dec 2023 14:09:12 GMT\r\n
  Server: *********\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  X-XSS-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  Referer-Policy: no-referer-when-downgrade\r\n
  X-Download-Options: noopen\r\n
  X-Permitted-Cross-Domain-Policies: master-only\r\n
   [truncated]Content-Security-Policy: default-src 'self' data: blob: *.conac.cn  *.xjtu.edu.cn
  Last-Modified: Sun, 24 Dec 2023 11:10:53 GMT\r\n
  Accept-Ranges: bytes\r\n
  Cache-Control: max-age=600\r\n
  Expires: Sun, 24 Dec 2023 14:19:12 GMT\r\n
  ETag: "ed8a-60d3f80aa2940-gzip"\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.008758000 seconds]
  [Request in frame: 104]
  [Next request in frame: 117]
  [Next response in frame: 118]
  [Request URI: https://www.xjtu.edu.cn/]
```

第一行给出的是相关的状态，此处可以发现Host还没有准备好。



观察到后面有成功的一次http请求和应答。不妨在看看这个的http报文



第一行表示准备好了，后面是一些相关的设定，应该和请求报文中的内容想呼应。

HTTP协议的工作过程

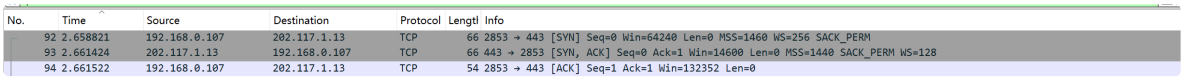
1. 客户端发起请求：
    - 客户端通常是Web浏览器，但也可以是其他HTTP客户端应用程序。
    - 客户端构建一个HTTP请求，其中包括：
        - 请求方法（如GET、POST、PUT、DELETE等），表示客户端的意图。
        - 请求URL（Uniform Resource Locator），指定要访问的资源的地址。
        - 请求头部，包含有关请求的元信息，如User-Agent（客户端的标识）、Accept（接受的内容类型）等。
        - 请求正文（对于POST请求等情况）。
2. 服务器接收请求：
    - 服务器是Web服务器，它接收到客户端的HTTP请求。
    - 服务器解析请求，理解客户端的意图，并准备回应。
3. 服务器处理请求：
    - 根据请求的URL和方法，服务器执行相应的操作，通常是查找、生成或修改资源。

- 服务器可能需要访问数据库、文件系统或其他资源来满足请求。

4. 服务器发送响应：
   - 服务器构建一个HTTP响应，其中包括：
     - 响应状态行，包含HTTP版本和状态码（例如200表示成功，404表示资源未找到，500表示服务器内部错误）。
     - 响应头部，包含有关响应的元信息，如Server（服务器的标识）、Content-Type（响应的内容类型）等。
     - 响应正文，包含实际的数据或资源内容。
5. 客户端接收响应：
   - 客户端接收服务器的HTTP响应。
   - 客户端解析响应，根据状态码判断请求是否成功，并提取响应中的数据。
6. 客户端呈现或处理响应：
   - 如果响应包含HTML内容，客户端会呈现网页，用户可以看到页面内容。
   - 如果响应包含其他类型的数据，客户端可能会将数据用于不同的用途，如下载文件、渲染图像等。
7. 连接的关闭：
   - 一旦HTTP通信完成，客户端和服务器通常会关闭连接。

TCP分析

TCP建立连接



No.	Time	Source	Destination	Protocol	Lengtl	Info
92	2.658821	192.168.0.107	202.117.1.13	TCP	66	2853 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
93	2.661424	202.117.1.13	192.168.0.107	TCP	66	443 → 2853 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=128
94	2.661522	192.168.0.107	202.117.1.13	TCP	54	2853 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0

tcp建立时由客户端端口662853发现主机443端口内容为SYN=1 seq=0

主机端返回一个SYN=1 ACK=1 seq=0 ack=1 的包

客户端收到后回复一个ACK=1，seq=1，ack=1的包

至此，tcp成功建立连接

TCP断开连接

106	24.318233	202.117.1.13	192.168.0.107	TCP	54 443 → 14595 [FIN, ACK] Seq=184 Ack=859 Win=16256 Len=0
107	24.318314	192.168.0.107	202.117.1.13	TCP	54 14595 → 443 [ACK] Seq=859 Ack=185 Win=132096 Len=0
117	25.288512	192.168.0.107	202.117.1.13	TCP	54 14595 → 443 [FIN, ACK] Seq=859 Ack=185 Win=132096 Len=0
119	25.290403	202.117.1.13	192.168.0.107	TCP	54 443 → 14595 [ACK] Seq=185 Ack=860 Win=16256 Len=0

主机发起请求FIN,ACK（第一次挥手），本机接收到并返回两个包，一个为ACK（第二次挥手），另一个为FIN,ACK（第三次挥手，最后主机发一个ACK返回给本机（第四次挥手）然后结束，

TCP过程

经过三次握手建立连接。中间保持active，最后4次握手断开连接

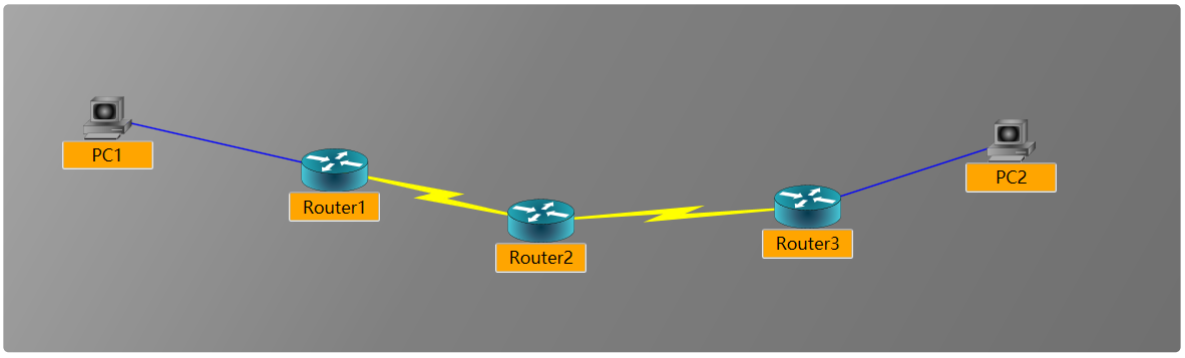
具体而言：

1. 建立连接：
    - 在通信的两端，分别有一个TCP协议的实体，一个充当客户端，一个充当服务器。为了建立连接，客户端首先向服务器发送一个TCP连接请求报文（SYN）。
2. 服务器响应：
    - 服务器收到客户端的连接请求后，如果愿意接受连接，就会发送一个TCP连接响应报文（SYN-ACK）。
3. 客户端确认：
    - 客户端接收到服务器的响应后，会发送一个确认报文（ACK），这表示连接已建立。此时，连接处于已建立状态（ESTABLISHED）。
4. 数据传输：
    - 一旦连接建立，客户端和服务器之间可以开始传输数据。数据被分成小块（通常称为数据段或数据包）并通过TCP协议进行传输。
5. 数据分段：
    - TCP会将应用程序发送的数据划分为适当大小的数据段。这些数据段通常包括数据部分、序列号（用于排序和重组数据段）、校验和（用于检测数据的完整性）等。
6. 数据可靠性：
    - TCP通过使用确认机制来确保数据的可靠传输。每当接收方成功接收并验证了数据段后，会发送确认报文，通知发送方数据已成功到达。如果发送方在一定时间内未收到确认，它将重新发送数据段，以确保数据不会丢失或损坏。
7. 流量控制：
    - TCP还实施了流量控制机制，以确保发送方不会发送太多数据，超出接收方的处理能力。这是通过使用滑动窗口机制来实现的。
8. 连接终止：

- 当数据传输完成时，双方中的任何一方都可以发送一个连接终止请求。这通常涉及发送一个FIN（Finish）报文。
- 接收到FIN后，接收方可以发送一个ACK报文作为确认，然后终止连接，或者也可以发送自己的FIN报文，然后接收方发送ACK报文。
- 当双方都发送了FIN和ACK，连接将进入终止状态，并最终关闭。

boson模拟组网

拓扑



相应的路由表配置

Router1

```
     172.15.0.0/24 is subnetted, 1 subnets
C       172.15.1.0 is directly connected, Ethernet0/0
C    202.10.10.0 is directly connected, Serial0/0
R    189.144.0.0 [120/1] via 202.10.10.8, 00:09:41, Serial0/0
R    192.169.10.0 [120/2] via 202.10.10.8, 00:03:38, Serial0/0
```

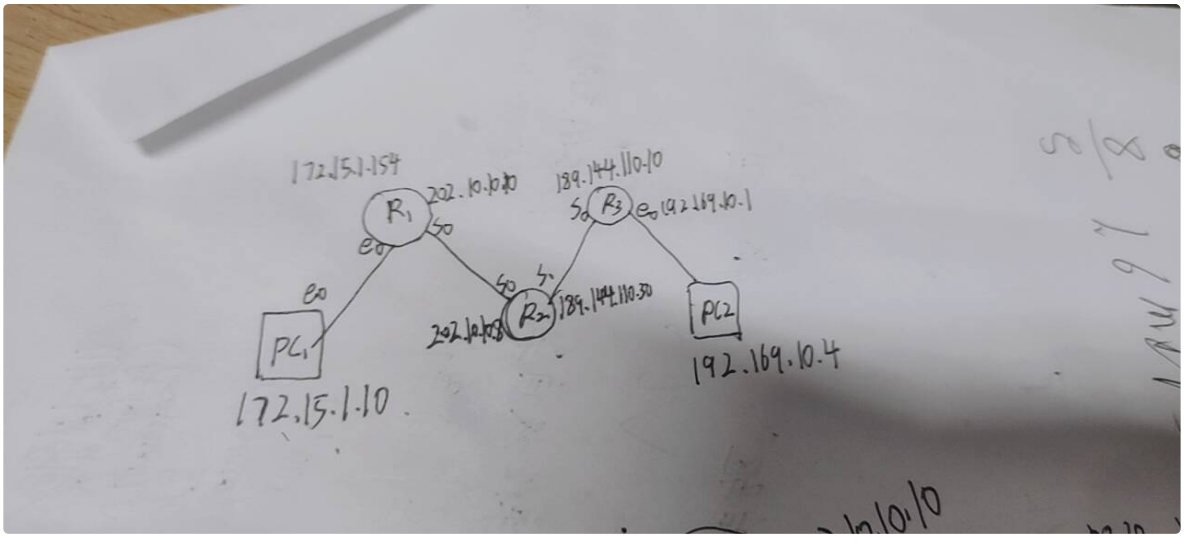
Router2

```
C    202.10.10.0 is directly connected, Serial0/0
     189.144.0.0/24 is subnetted, 1 subnets
C       189.144.110.0 is directly connected, Serial0/1
R    172.15.0.0 [120/1] via 202.10.10.10, 00:08:18, Serial0/0
R    192.169.10.0 [120/1] via 189.144.110.10, 00:05:23, Serial0/1
```

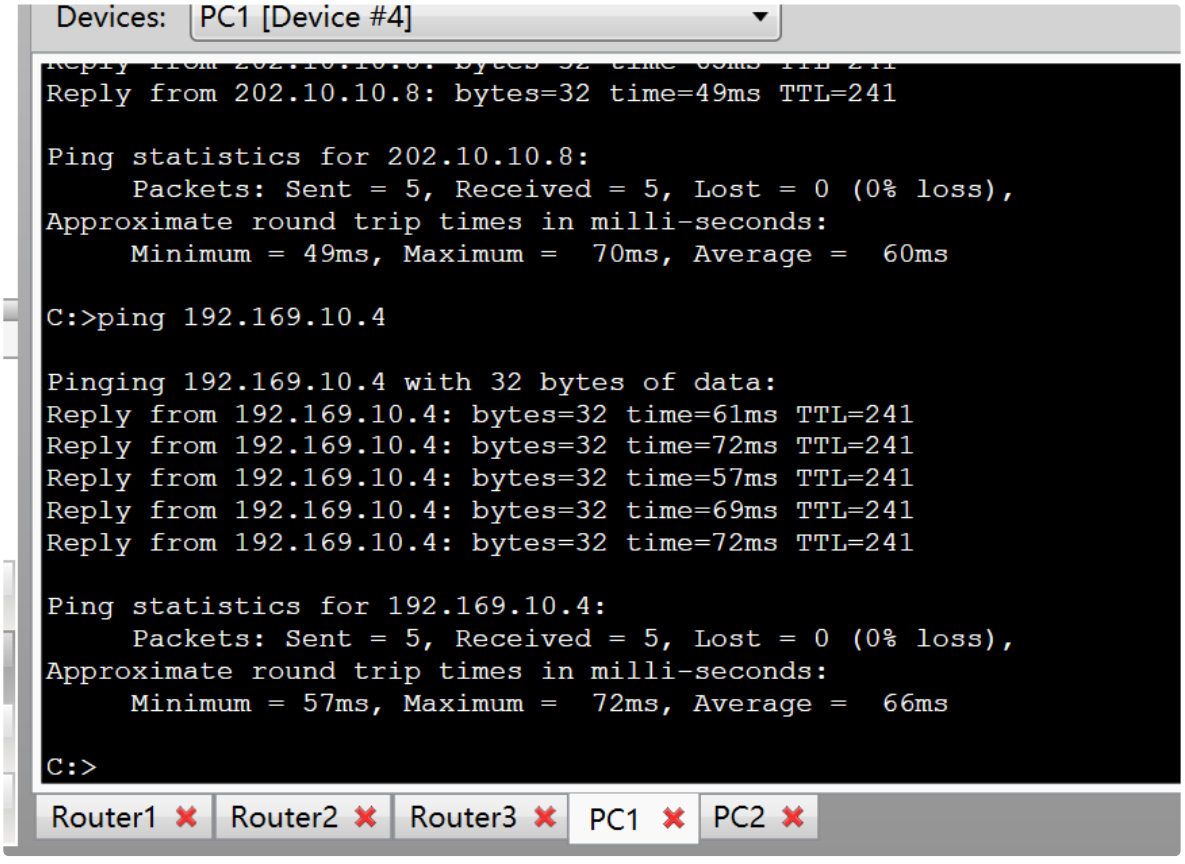
Router3

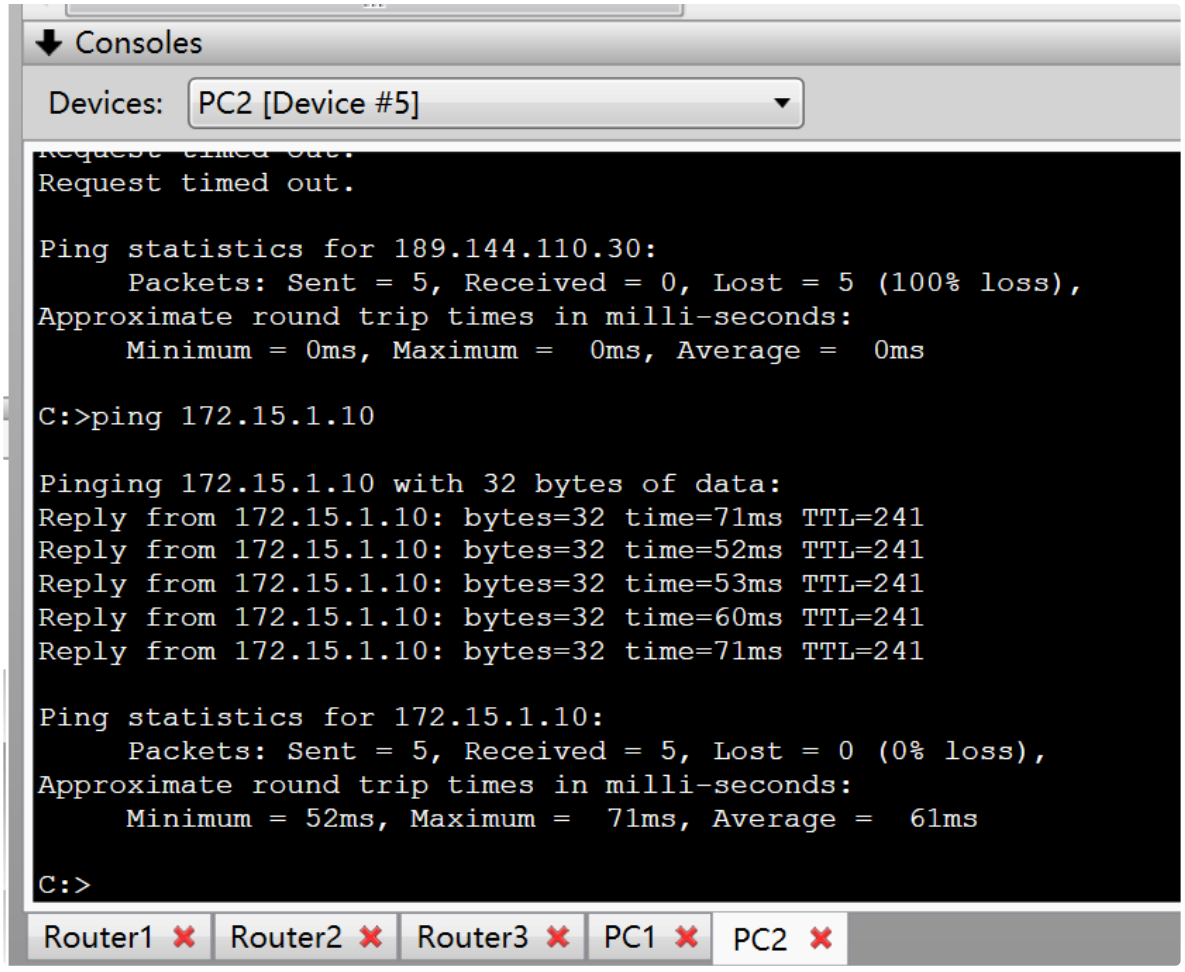
```
C    192.169.10.0 is directly connected, Ethernet0/0
     189.144.0.0/24 is subnetted, 1 subnets
C       189.144.110.0 is directly connected, Serial0/0
R    202.10.10.0 [120/1] via 189.144.110.30, 00:07:25, Serial0/0
R    172.15.0.0 [120/2] via 189.144.110.30, 00:04:25, Serial0/0
```

各端口的ip



PC1和PC2可以相互ping通




Consoles
Devices: PC2 [Device #5]
Request timed out.
Ping statistics for 189.144.110.30:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:>ping 172.15.1.10
Pinging 172.15.1.10 with 32 bytes of data:
Reply from 172.15.1.10: bytes=32 time=71ms TTL=241
Reply from 172.15.1.10: bytes=32 time=52ms TTL=241
Reply from 172.15.1.10: bytes=32 time=53ms TTL=241
Reply from 172.15.1.10: bytes=32 time=60ms TTL=241
Reply from 172.15.1.10: bytes=32 time=71ms TTL=241
Ping statistics for 172.15.1.10:
Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 52ms, Maximum = 71ms, Average = 61ms
C:>
Router1
Router2
Router3
PC1
PC2