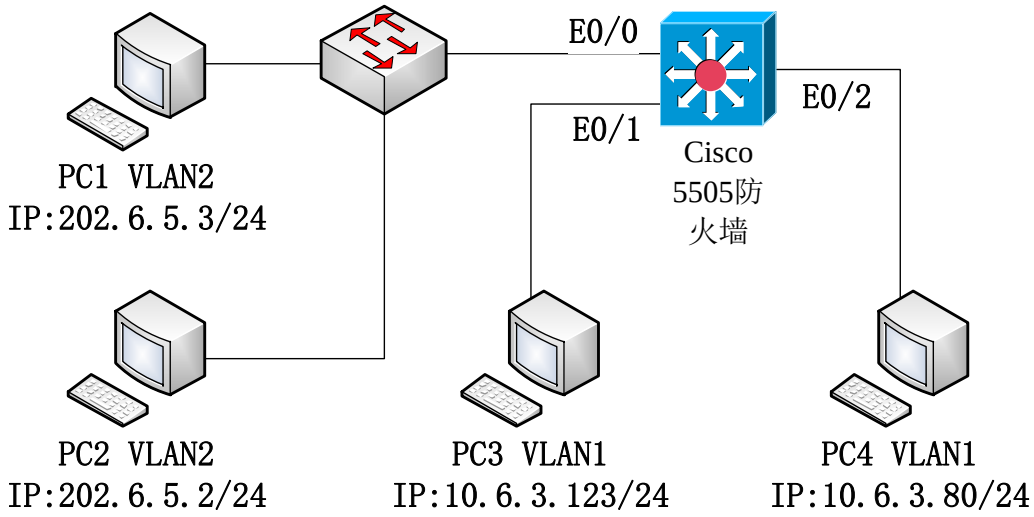
计算机网络专题实验现场检查单 7

实验名称：**防火墙与 SSLVPN 实验**　　时间：　2021 年 4 月 23 日　早□ 午□　晚 √

组号	5-6	实验位	6	控制器地址	192.168.160
姓名	施炎江	高浩翔		薛杰锋	贾星辰

实验组网图

【可以手画拍照。拓扑图中，请标明设备编号、端口号、vlan 号、IP 地址、掩码等】



验果

1、本组 CISCO ASA5505 中 Vlan 的划分、命名及端口分配方案是：

VLAN 划分：本组 CISCO ASA5505 中的 VLAN 划分为 VLAN1 和 VLAN2。

命名：其中 PC1（IP:202.6.5.3/24）和 PC2（IP:202.6.5.2/24）在 VLAN2 内。PC3（IP:10.6.3.123/24）和 PC4（IP:10.6.3.80/24）在 VLAN1 内。

端口分配方案：CISCO ASA5505 的 E0/0 端口连接交换机，该交换机与 PC1、PC2 相连；E0/1 端口连接 PC3；E0/2 端口连接 PC4。

2、CISCO ASA5505 内网 DHCP 服务器的 IP 范围是：

10.1.3.2-10.1.3.33

3、SSL VPN 用户地址池的名称和地址范围是：

名称：ssluser

地址范围：10.10.10.1-10.10.10.10

4、创建的 SSL VPN 用户名是：

创建的用户名是 vpnuser1 和 vpnuser2。

5、所配置的防火墙测试方案及结果是：

步骤 8：启动 HFS（http file server)，添加共享文件资源，设置内部 IP（10.6.3.80）和端口（80），构建一个可以供外部 VPN 用户访问的 Web 服务。

在 PC3 上用浏览器测试访问 PC4 结果：

测试结果说明能够实现共享文件资源。

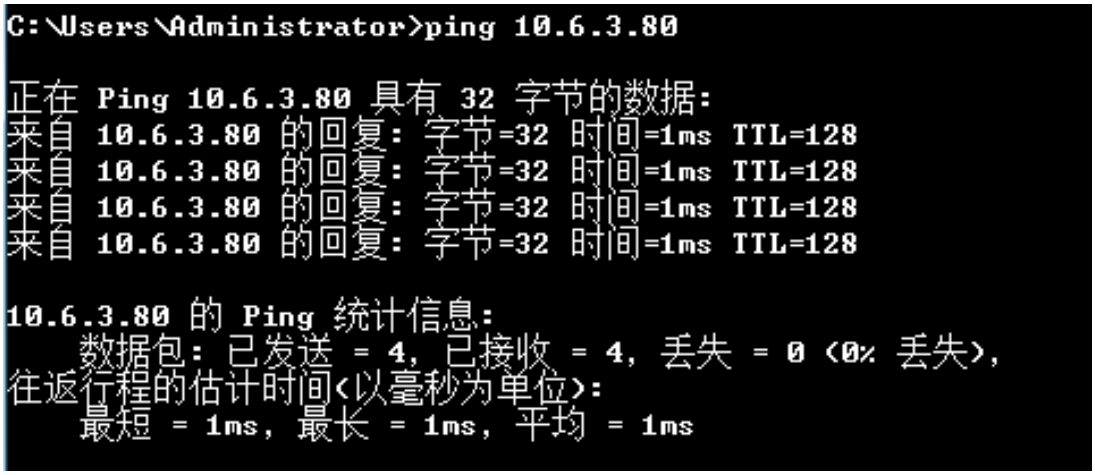
步骤 9：在外网 PC1 和 PC2 用 SSLVPN 接入并下载内部 Web 资源。

1）在浏览器中输入 https://202.6.5.1 访问 WEB VPN，在随后弹出的对话框中输入用户名和密码单击登陆。两个 PC 的用户名不能取同一个。

系统会弹出要求安装 SSL VPN CLIENT 程序，单击“YES”，系统自动安装并连接 SSLVPN。

在 VPN 软件环境下，分别以客户端模式和 web 模式访问内部 Web 资源服务器，并运行 ping 测试网络连通性。

客户端模式和 web 模式均能访问内部 Web 资源服务器，执行 PC1 ping PC3 的结果如下：



四个报文都接收成功丢包率为 0，能够成功连接。

2）查看本地网卡配置，参考路由表信息，分析外部 PC 如何通过 VPN 安全访问 10.6.3.x 上的资源。

（1）web 模式

PC1 本地网卡配置如下：

通过 web 模式连接 vpn 时，PC 是通过原先使用的网卡进行连接的，因此在网卡配置里没有多余的虚拟显卡。

```
C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : 6-PC1
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 6-1 exp:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . . . . . . . . . : 00-E0-4C-68-46-00
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::ac25:fa72:b564:7f87%14(首选)
   IPv4 地址 . . . . . . . . . . . . : 202.6.5.3(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 202.6.5.1
   DHCPv6 IAID . . . . . . . . . . . : 436265036
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-24-A7-91-D3-00-E0-4C-70-70-59

   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

PC1 本地路由信息如下：

```
C:\Users\Administrator>netstat -r
===========================================================================
接口列表
 14...00 e0 4c 68 46 00 ......Realtek PCIe GBE Family Controller
 13...48 4d 7e a8 1b 7d ......Intel(R) Ethernet Connection (2) I219-LM
 12...00 19 e0 87 ce b7 ......Atheros AR5005GS Wireless Network Adapter
  1...........................Software Loopback Interface 1
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 15...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
 18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 38...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      202.6.5.1      202.6.5.3    276
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
      192.168.0.0      255.255.0.0     192.168.0.1    192.168.0.61    276
      192.168.0.0    255.255.255.0         在链路上      192.168.0.61    276
     192.168.0.61  255.255.255.255         在链路上      192.168.0.61    276
    192.168.0.255  255.255.255.255         在链路上      192.168.0.61    276
        202.6.5.0    255.255.255.0         在链路上         202.6.5.3    276
        202.6.5.3  255.255.255.255         在链路上         202.6.5.3    276
      202.6.5.255  255.255.255.255         在链路上         202.6.5.3    276
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0         在链路上         202.6.5.3    276
        224.0.0.0        240.0.0.0         在链路上      192.168.0.61    276
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255         在链路上         202.6.5.3    276
  255.255.255.255  255.255.255.255         在链路上      192.168.0.61    276
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址  跃点数
      192.168.0.0      255.255.0.0     192.168.0.1     默认
          0.0.0.0          0.0.0.0       202.6.5.1     默认
===========================================================================
```

Web 模式里，PC 和防火墙进行认证后，PC 向内网发送数据时无需知道内网 PC 的地址，只需要向防火墙发送数据包即可，防火墙会根据数据包内的 SSL 加密信息转发给内网的 PC。

（2）客户端模式：

PC1 本地网卡配置如下：

通过客户端连接 VPN 时，会产生一个虚拟网卡，即下图中的以太网适配器 本地连接 2，通过该网卡获得一个内网的 VPN 用户地址，即网卡内的 IP 地址 10.10.10.1。

```
C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : 6-PC1
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 本地连接 2:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Cisco AnyConnect VPN Virtual Miniport Ada
pter for Windows x64
   物理地址. . . . . . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::bd34:d245:31b0:4e59%37(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.10.10.1(首选)
   子网掩码 . . . . . . . . . . . . : 255.0.0.0
   默认网关. . . . . . . . . . . . . : 10.0.0.1
   DHCPv6 IAID . . . . . . . . . . . : 620758426
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-24-A7-91-D3-00-E0-4C-70-70-59

   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

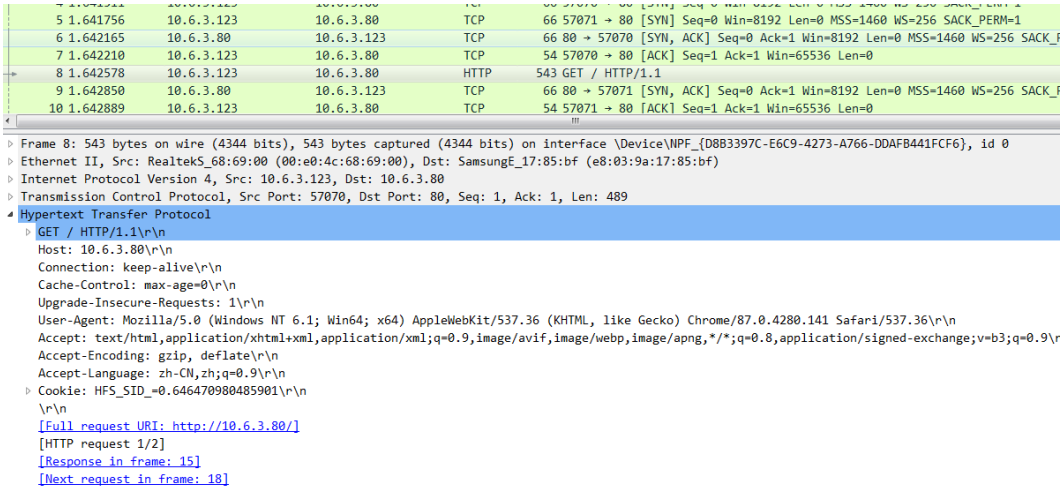
PC1 本地路由信息如下：

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0       202.6.5.1       202.6.5.3    276
          0.0.0.0          0.0.0.0     192.168.3.1    192.168.3.105     25
          0.0.0.0          0.0.0.0      10.0.0.1      10.10.10.1      2
         10.0.0.0        255.0.0.0         在链路上        10.10.10.1    257
       10.10.10.1  255.255.255.255         在链路上        10.10.10.1    257
   10.255.255.255  255.255.255.255         在链路上        10.10.10.1    257
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
        202.6.5.1  255.255.255.255       202.6.5.1       202.6.5.3     21
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0         在链路上         202.6.5.3    276
        224.0.0.0        240.0.0.0         在链路上       192.168.0.61    276
        224.0.0.0        240.0.0.0         在链路上     192.168.3.105    281
        224.0.0.0        240.0.0.0         在链路上        10.10.10.1    257
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255         在链路上         202.6.5.3    276
  255.255.255.255  255.255.255.255         在链路上       192.168.0.61    276
  255.255.255.255  255.255.255.255         在链路上     192.168.3.105    281
  255.255.255.255  255.255.255.255         在链路上        10.10.10.1    257
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址  跃点数
      192.168.0.0    255.255.0.0     192.168.0.1     默认
          0.0.0.0          0.0.0.0       202.6.5.1     默认
          0.0.0.0          0.0.0.0        10.0.0.1       1
```

客户端连接 VPN 时，会产生一个虚拟网卡，通过该网卡获得一个内网的 VPN 用户地址。此时，可以认为外网 PC 与内网 PC 在同一个虚拟局域网内，因此，路由表里有该局域网网关地址。

6、分析步骤 10 完成捕获的报文，分析两台 PC 上报文的差别（可选）。

内网：PC3 抓包

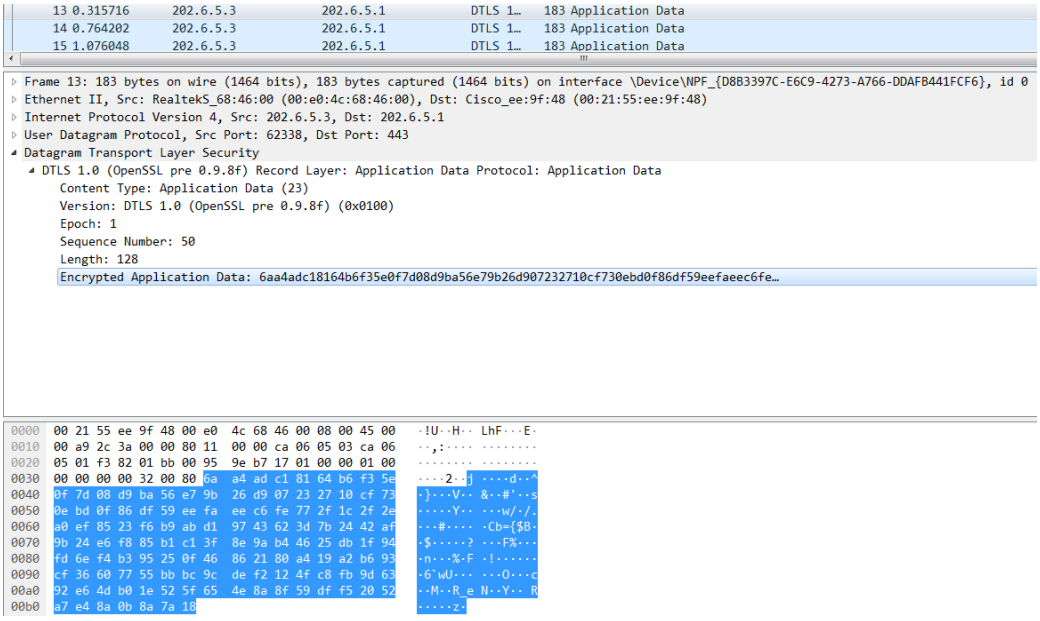


通过内网访问，两台 PC 可以没有阻碍地连通。

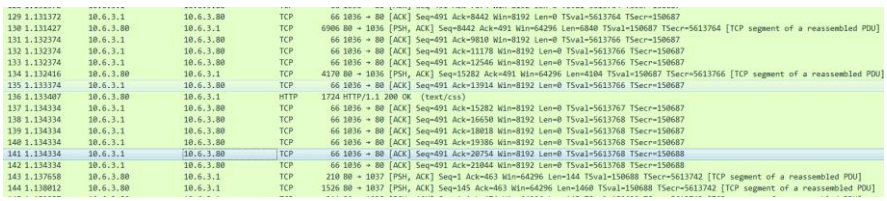
外网：

通过 web 方式：

PC1 访问 PC4 的报文



PC4 抓包

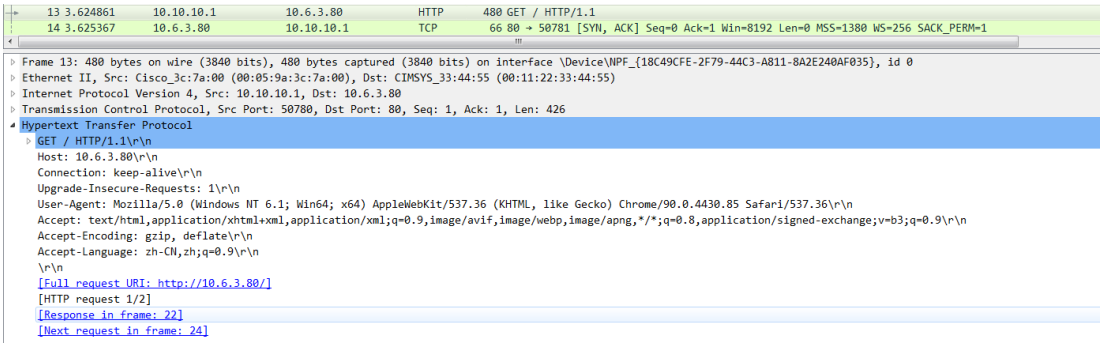


通过 web 方式连接 VPN，在外网 PC 上只能看见本机到防火墙的报文，且报文协议为 DTLS 1.0(OpenSSL pre 0.9.8f)，说明该报文需要经由防火墙处理后转发给内网 PC，即报文先由外网 PC 发送给防火墙，再由防火墙转发给内部服务器；在内网 PC

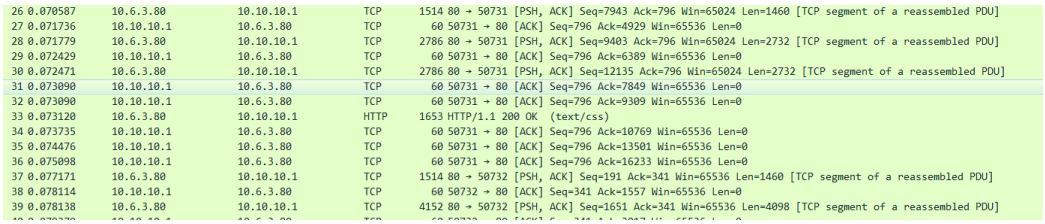
上看到的数据，来源都是防火墙 10.6.3.1，这也说明了服务器发送的响应数据是先发送给防火墙，然后由防火墙抓发给外网 PC。

通过客户端方式：

外网客户端 VPN 抓包



PC4 抓包



通过客户端连接 VPN，客户端会被分配一个 VPN 地址，即报文地址中的 10.10.10.1。客户端可以看到内网 PC 的 IP 地址，穿过防火墙直接地进行通信，因此，在 PC1 抓包看到的目的地就是内网 PC 的 IP 地址 10.6.3.80，在内网 PC 上看到的来源是 10.10.10.1，即外网 PC 所使用的 VPN 用户地址。

报文的主要差异是 IP 地址的不同，WEB 下 IP 地址是防火墙的 IP，客户端情况下 IP 是内网服务器的 IP。

进阶自设计

分别在校园网和外网（通过校园 VPN 服务 http://vpn.xjtu.edu.cn/）访问校内资源（可自己架设服务器），分析对比三种模式（内网访问、外网 WebVPN 访问和外网 SSLVPN 访问）的访问过程及相关参数。

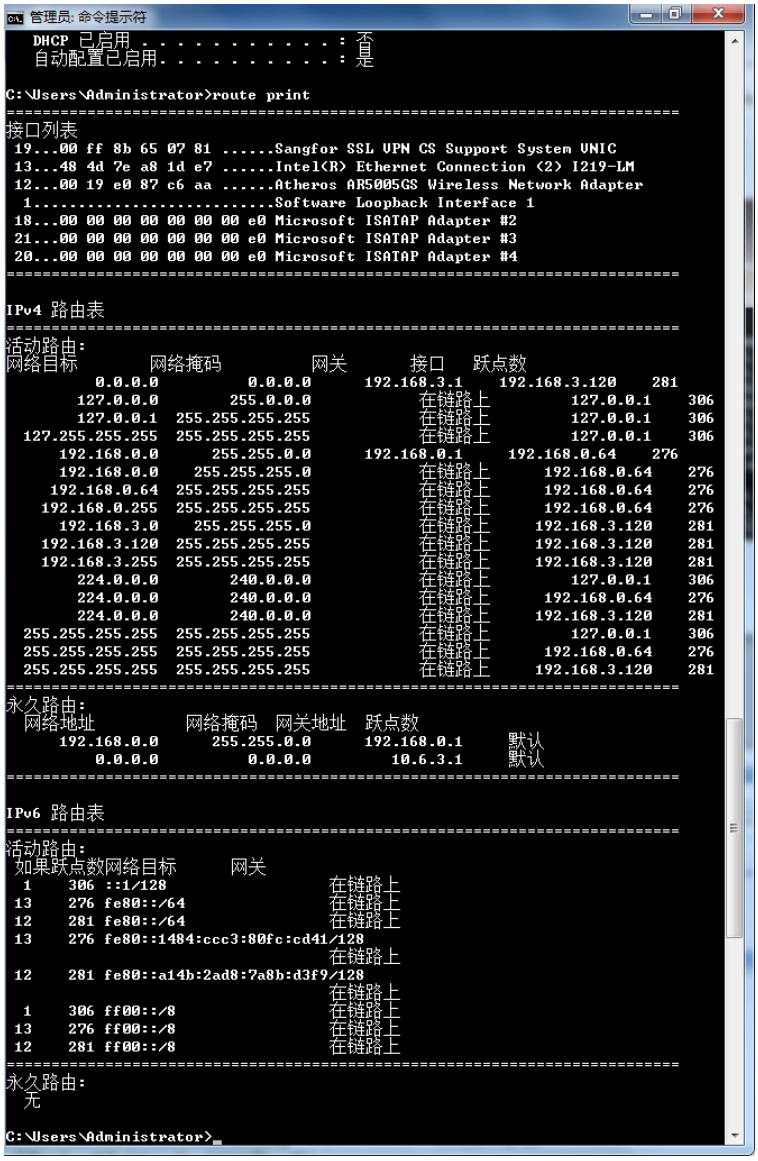
均以访问本科考勤网页为例：bkkq.xjtu.edu.cn[本地地址：10.32.129.60]

内网访问：

物理网卡：

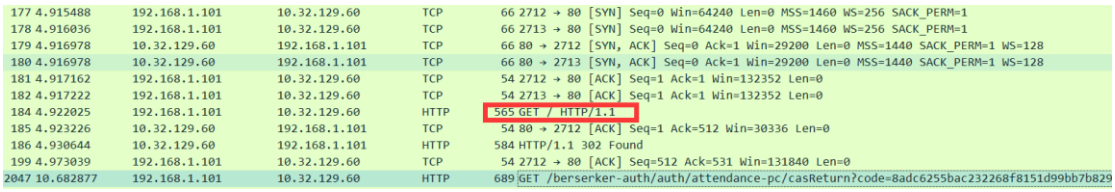
```
无线局域网适配器 无线网络连接:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Atheros AR5005GS Wireless Network Adapter

   物理地址. . . . . . . . . . . . . : 00-19-E0-87-C6-AA
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::a14b:2ad8:7a8b:d3f9%12(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.3.120(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2021年4月23日 18:50:23
   租约过期的时间  . . . . . . . . . : 2021年4月23日 20:50:23
   默认网关. . . . . . . . . . . . . : 192.168.3.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.3.1
   DHCPv6 IAID . . . . . . . . . . . : 218110432
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-24-A7-91-D3-00-E0-4C-70-70-59

   DNS 服务器  . . . . . . . . . . . : 202.117.0.20
                                       192.168.3.1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

本地路由表信息：



```
管理员: 命令提示符
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是

C:\Users\Administrator>route print
===========================================================================
接口列表
 19...00 ff 8b 65 07 81 ......Sangfor SSL VPN CS Support System VNIC
 13...48 4d 7e a8 1d e7 ......Intel(R) Ethernet Connection (2) I219-LM
 12...00 19 e0 87 c6 aa ......Atheros AR5005GS Wireless Network Adapter
  1...........................Software Loopback Interface 1
 18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.3.1   192.168.3.120    281
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    306
      192.168.0.0      255.255.0.0      192.168.0.1     192.168.0.64    276
      192.168.0.0    255.255.255.0            在链路上      192.168.0.64    276
     192.168.0.64  255.255.255.255            在链路上      192.168.0.64    276
    192.168.0.255  255.255.255.255            在链路上      192.168.0.64    276
      192.168.3.0    255.255.255.0            在链路上     192.168.3.120    281
    192.168.3.120  255.255.255.255            在链路上     192.168.3.120    281
    192.168.3.255  255.255.255.255            在链路上     192.168.3.120    281
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0            在链路上      192.168.0.64    276
        224.0.0.0        240.0.0.0            在链路上     192.168.3.120    281
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255            在链路上      192.168.0.64    276
  255.255.255.255  255.255.255.255            在链路上     192.168.3.120    281
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址  跃点数
      192.168.0.0      255.255.0.0     192.168.0.1     默认
        0.0.0.0          0.0.0.0       10.6.3.1      默认
===========================================================================

IPv6 路由表
===========================================================================
活动路由:
 如果跃点数网络目标       网关
  1    306 ::1/128                  在链路上
 13    276 fe80::/64                在链路上
 12    281 fe80::/64                在链路上
 13    276 fe80::1484:ccc3:80fc:cd41/128
                                    在链路上
 12    281 fe80::a14b:2ad8:7a8b:d3f9/128
                                    在链路上
  1    306 ff00::/8                 在链路上
 13    276 ff00::/8                 在链路上
 12    281 ff00::/8                 在链路上
===========================================================================
永久路由:
  无

C:\Users\Administrator>_
```

遵循未加密的 HTTP 协议，如图所示：



177	4.915488	192.168.1.101	10.32.129.60	TCP	66	2712 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
178	4.916036	192.168.1.101	10.32.129.60	TCP	66	2713 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
179	4.916978	10.32.129.60	192.168.1.101	TCP	66	80 → 2712 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
180	4.916978	10.32.129.60	192.168.1.101	TCP	66	80 → 2713 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
181	4.917162	192.168.1.101	10.32.129.60	TCP	54	2712 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
182	4.917222	192.168.1.101	10.32.129.60	TCP	54	2713 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
184	4.922025	192.168.1.101	10.32.129.60	HTTP	565	GET / HTTP/1.1
185	4.923226	10.32.129.60	192.168.1.101	TCP	54	80 → 2712 [ACK] Seq=1 Ack=512 Win=30336 Len=0
186	4.930644	10.32.129.60	192.168.1.101	HTTP	584	HTTP/1.1 302 Found
199	4.973039	192.168.1.101	10.32.129.60	TCP	54	2712 → 80 [ACK] Seq=512 Ack=531 Win=131840 Len=0
2047	10.682877	192.168.1.101	10.32.129.60	HTTP	689	GET /berserker-auth/auth/attendance-pc/casReturn?code=8adc6255bac232268f8151d99bb7b829

分析 HTTP 报文数据：

请求报文如下：

```
Hypertext Transfer Protocol
> GET /berserker-auth/auth/attendance-pc/casReturn?code=8adc6255bac232268f8151d99bb7b829&state=1234&userType=1&employeeNo=2181411962 HTTP/1.1\r\n
  Host: bkkq.xjtu.edu.cn\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Referer: http://org.xjtu.edu.cn/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9\r\n
> Cookie: _ga=GA1.3.1052594854.1608208627\r\n
  \r\n
  [Full request URI: http://bkkq.xjtu.edu.cn/berserker-auth/auth/attendance-pc/casReturn?code=8adc6255bac232268f8151d99bb7b829&state=1234&userType=1&employeeNo=2181411962]
  [HTTP request 2/6]
  [Prev request in frame: 184]
  [Response in frame: 2052]
  [Next request in frame: 2054]
```

应答报文如下：

```
Hypertext Transfer Protocol
v HTTP/1.1 200 OK\r\n
  v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Server: nginx/1.16.0\r\n
  Date: Wed, 21 Apr 2021 14:04:04 GMT\r\n
  Content-Type: text/html\r\n
v Content-Length: 582\r\n
    [Content length: 582]
  Last-Modified: Tue, 06 Apr 2021 09:15:36 GMT\r\n
  Connection: keep-alive\r\n
  ETag: "606c26b8-246"\r\n
  Accept-Ranges: bytes\r\n
  \r\n
  [HTTP response 3/6]
  [Time since request: 0.044651000 seconds]
  [Prev request in frame: 2047]
  [Prev response in frame: 2052]
  [Request in frame: 2054]
  [Next request in frame: 2061]
  [Next response in frame: 3034]
  [Request URI: http://bkkq.xjtu.edu.cn/attendance-student/kqtj/getKqtjByTermGroupSub]
  File Data: 582 bytes
Line-based text data: text/html (1 lines)
  [truncated]<!DOCTYPE html><html><head><meta charset=utf-8><meta name=viewport content="width=device-width,initial-scale=1,user-scalable=0"><title>Webpack App</title><li
```

追踪字节流可以查看到传输的 http 页面代码，均未加密：

```
GET /attendance-student-pc/ HTTP/1.1
Host: bkkq.xjtu.edu.cn
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/
537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9
Referer: http://org.xjtu.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.3.1052594854.1608208627

HTTP/1.1 200 OK
Server: nginx/1.16.0
Date: Wed, 21 Apr 2021 14:04:04 GMT
Content-Type: text/html
Content-Length: 582
Last-Modified: Tue, 06 Apr 2021 09:15:36 GMT
Connection: keep-alive
ETag: "606c26b8-246"
Accept-Ranges: bytes

<!DOCTYPE html><html><head><meta charset=utf-8><meta name=viewport content="width=device-width,initial-scale=1,user-
scalable=0"><title>Webpack App</title><link rel="shortcut icon" href=./favicon.ico><link href=./static/css/app.
27aab9544ca8b2e41d4094aabd8e4891.css rel=stylesheet></head><body><div id=app-box></div><script type=text/javascript src=./
static/js/manifest.3ad1d5771e9b13dbdad2.js></script><script type=text/javascript src=./static/js/
vendor.acaaa3cecb37891d7495.js></script><script type=text/javascript src=./static/js/app.fd52a691b06d7f353bf5.js></
```

外网 sslVPN 访问:

ip.add r == 222.90.111.20 && ssl

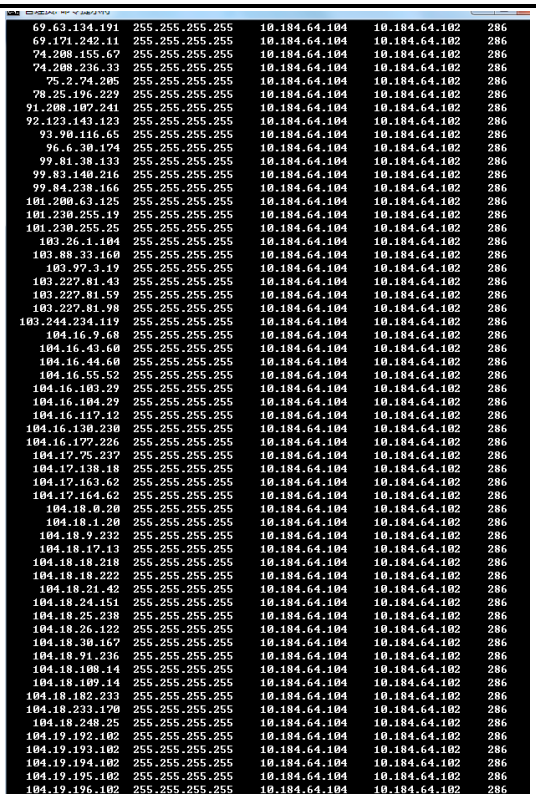
虚拟网卡

```
以太网适配器 本地连接 2:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Sangfor SSL VPN CS Support System VNIC
   物理地址. . . . . . . . . . . . . : 00-FF-8B-65-07-81
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::1cf4:ba69:d574:a7f2%19(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.184.64.102(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
   DNS 服务器 . . . . . . . . . . . : 127.0.0.1
   TCPIP 上的 NetBIOS . . . . . . . : 已启用
```

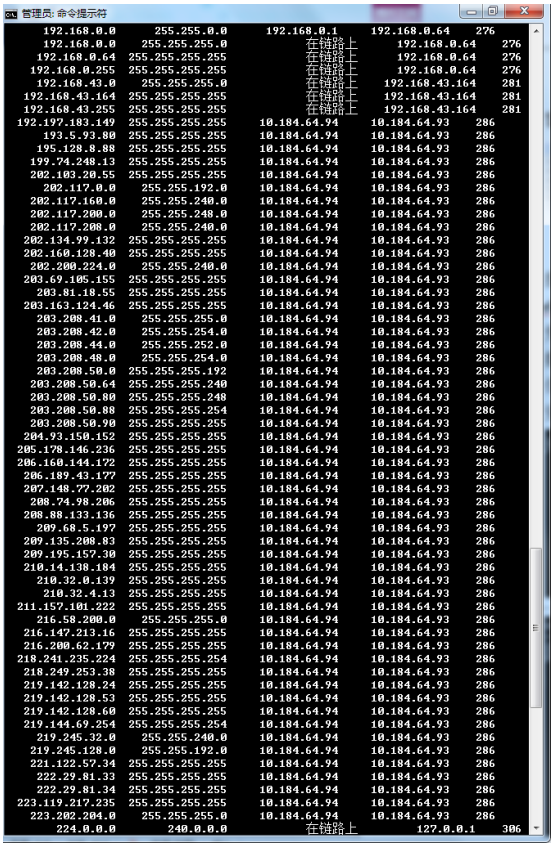
本地物理网卡配置

```
无线局域网适配器 无线网络连接:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Atheros AR5005GS Wireless Network Adapter

   物理地址. . . . . . . . . . . . . : 00-19-E0-87-C6-AA
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 240e:454:1dc:7de7:a14b:2ad8:7a8b:d3f9(首
选)
   临时 IPv6 地址. . . . . . . . . . : 240e:454:1dc:7de7:513f:7e75:b8f0:aa8c(首
选)
   本地链接 IPv6 地址. . . . . . . . : fe80::a14b:2ad8:7a8b:d3f9%12(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.43.164(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2021年4月23日 19:31:11
   租约过期的时间  . . . . . . . . . : 2021年4月23日 20:31:10
   默认网关. . . . . . . . . . . . . : fe80::2a1:db2c:f524:cc90%12
                                       192.168.43.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.43.1
   DNS 服务器 . . . . . . . . . . . : 127.0.0.1
                                       192.168.43.1
   TCPIP 上的 NetBIOS . . . . . . . : 已启用
```

本地路由表信息：



69.63.134.191	255.255.255.255	10.184.64.104	10.184.64.102	286
69.171.242.11	255.255.255.255	10.184.64.104	10.184.64.102	286
74.208.155.67	255.255.255.255	10.184.64.104	10.184.64.102	286
74.208.236.33	255.255.255.255	10.184.64.104	10.184.64.102	286
75.2.74.205	255.255.255.255	10.184.64.104	10.184.64.102	286
78.25.196.229	255.255.255.255	10.184.64.104	10.184.64.102	286
91.208.107.241	255.255.255.255	10.184.64.104	10.184.64.102	286
92.123.143.123	255.255.255.255	10.184.64.104	10.184.64.102	286
93.90.116.65	255.255.255.255	10.184.64.104	10.184.64.102	286
96.6.30.174	255.255.255.255	10.184.64.104	10.184.64.102	286
99.81.38.133	255.255.255.255	10.184.64.104	10.184.64.102	286
99.83.140.216	255.255.255.255	10.184.64.104	10.184.64.102	286
99.84.238.166	255.255.255.255	10.184.64.104	10.184.64.102	286
101.200.63.125	255.255.255.255	10.184.64.104	10.184.64.102	286
101.230.255.19	255.255.255.255	10.184.64.104	10.184.64.102	286
101.230.255.25	255.255.255.255	10.184.64.104	10.184.64.102	286
103.26.1.104	255.255.255.255	10.184.64.104	10.184.64.102	286
103.88.33.160	255.255.255.255	10.184.64.104	10.184.64.102	286
103.97.3.19	255.255.255.255	10.184.64.104	10.184.64.102	286
103.227.81.43	255.255.255.255	10.184.64.104	10.184.64.102	286
103.227.81.59	255.255.255.255	10.184.64.104	10.184.64.102	286
103.227.81.98	255.255.255.255	10.184.64.104	10.184.64.102	286
103.244.234.119	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.9.68	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.43.60	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.44.60	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.55.52	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.103.29	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.104.29	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.117.12	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.130.230	255.255.255.255	10.184.64.104	10.184.64.102	286
104.16.177.226	255.255.255.255	10.184.64.104	10.184.64.102	286
104.17.75.237	255.255.255.255	10.184.64.104	10.184.64.102	286
104.17.138.18	255.255.255.255	10.184.64.104	10.184.64.102	286
104.17.163.62	255.255.255.255	10.184.64.104	10.184.64.102	286
104.17.164.62	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.0.20	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.1.20	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.9.232	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.17.13	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.18.218	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.18.222	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.21.42	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.24.151	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.25.230	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.26.122	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.30.167	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.91.236	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.108.14	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.109.14	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.182.233	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.233.170	255.255.255.255	10.184.64.104	10.184.64.102	286
104.18.248.25	255.255.255.255	10.184.64.104	10.184.64.102	286
104.19.192.102	255.255.255.255	10.184.64.104	10.184.64.102	286
104.19.193.102	255.255.255.255	10.184.64.104	10.184.64.102	286
104.19.194.102	255.255.255.255	10.184.64.104	10.184.64.102	286
104.19.195.102	255.255.255.255	10.184.64.104	10.184.64.102	286
104.19.196.102	255.255.255.255	10.184.64.104	10.184.64.102	286



管理员: 命令提示符

192.168.0.0	255.255.0.0	192.168.0.1	192.168.0.64	276
192.168.0.0	255.255.255.0	在链路上	192.168.0.64	276
192.168.0.64	255.255.255.255	在链路上	192.168.0.64	276
192.168.0.255	255.255.255.255	在链路上	192.168.0.64	276
192.168.43.0	255.255.255.0	在链路上	192.168.43.164	281
192.168.43.164	255.255.255.255	在链路上	192.168.43.164	281
192.168.43.255	255.255.255.255	在链路上	192.168.43.164	281
192.197.183.149	255.255.255.255	10.184.64.94	10.184.64.93	286
193.5.93.80	255.255.255.255	10.184.64.94	10.184.64.93	286
195.128.8.88	255.255.255.255	10.184.64.94	10.184.64.93	286
199.74.248.13	255.255.255.255	10.184.64.94	10.184.64.93	286
202.103.20.55	255.255.255.255	10.184.64.94	10.184.64.93	286
202.117.0.0	255.255.192.0	10.184.64.94	10.184.64.93	286
202.117.160.0	255.255.240.0	10.184.64.94	10.184.64.93	286
202.117.200.0	255.255.248.0	10.184.64.94	10.184.64.93	286
202.117.208.0	255.255.240.0	10.184.64.94	10.184.64.93	286
202.134.99.132	255.255.255.255	10.184.64.94	10.184.64.93	286
202.160.128.40	255.255.255.255	10.184.64.94	10.184.64.93	286
202.200.224.0	255.255.240.0	10.184.64.94	10.184.64.93	286
203.69.105.155	255.255.255.255	10.184.64.94	10.184.64.93	286
203.81.18.55	255.255.255.255	10.184.64.94	10.184.64.93	286
203.163.124.46	255.255.255.255	10.184.64.94	10.184.64.93	286
203.208.41.0	255.255.255.0	10.184.64.94	10.184.64.93	286
203.208.42.0	255.255.254.0	10.184.64.94	10.184.64.93	286
203.208.44.0	255.255.252.0	10.184.64.94	10.184.64.93	286
203.208.48.0	255.255.254.0	10.184.64.94	10.184.64.93	286
203.208.50.0	255.255.255.192	10.184.64.94	10.184.64.93	286
203.208.50.64	255.255.255.240	10.184.64.94	10.184.64.93	286
203.208.50.80	255.255.255.248	10.184.64.94	10.184.64.93	286
203.208.50.88	255.255.255.254	10.184.64.94	10.184.64.93	286
203.208.50.90	255.255.255.255	10.184.64.94	10.184.64.93	286
204.93.150.152	255.255.255.255	10.184.64.94	10.184.64.93	286
205.178.146.226	255.255.255.255	10.184.64.94	10.184.64.93	286
206.160.144.172	255.255.255.255	10.184.64.94	10.184.64.93	286
206.189.43.177	255.255.255.255	10.184.64.94	10.184.64.93	286
207.148.77.202	255.255.255.255	10.184.64.94	10.184.64.93	286
208.74.98.206	255.255.255.255	10.184.64.94	10.184.64.93	286
208.88.133.136	255.255.255.255	10.184.64.94	10.184.64.93	286
209.68.5.197	255.255.255.255	10.184.64.94	10.184.64.93	286
209.135.208.83	255.255.255.255	10.184.64.94	10.184.64.93	286
209.195.157.30	255.255.255.255	10.184.64.94	10.184.64.93	286
210.14.138.184	255.255.255.255	10.184.64.94	10.184.64.93	286
210.32.0.139	255.255.255.255	10.184.64.94	10.184.64.93	286
210.32.4.13	255.255.255.255	10.184.64.94	10.184.64.93	286
211.157.101.222	255.255.255.255	10.184.64.94	10.184.64.93	286
216.58.200.0	255.255.255.0	10.184.64.94	10.184.64.93	286
216.147.213.16	255.255.255.255	10.184.64.94	10.184.64.93	286
216.200.62.179	255.255.255.255	10.184.64.94	10.184.64.93	286
218.241.235.224	255.255.255.254	10.184.64.94	10.184.64.93	286
218.249.253.38	255.255.255.255	10.184.64.94	10.184.64.93	286
219.142.128.24	255.255.255.255	10.184.64.94	10.184.64.93	286
219.142.128.53	255.255.255.255	10.184.64.94	10.184.64.93	286
219.142.128.60	255.255.255.255	10.184.64.94	10.184.64.93	286
219.144.69.254	255.255.255.254	10.184.64.94	10.184.64.93	286
219.245.32.0	255.255.240.0	10.184.64.94	10.184.64.93	286
219.245.128.0	255.255.192.0	10.184.64.94	10.184.64.93	286
221.122.57.34	255.255.255.255	10.184.64.94	10.184.64.93	286
222.29.81.33	255.255.255.255	10.184.64.94	10.184.64.93	286
222.29.81.34	255.255.255.255	10.184.64.94	10.184.64.93	286
223.119.217.235	255.255.255.255	10.184.64.94	10.184.64.93	286
223.202.204.0	255.255.255.0	10.184.64.94	10.184.64.93	286
224.0.0.0	240.0.0.0	在链路上	127.0.0.1	306

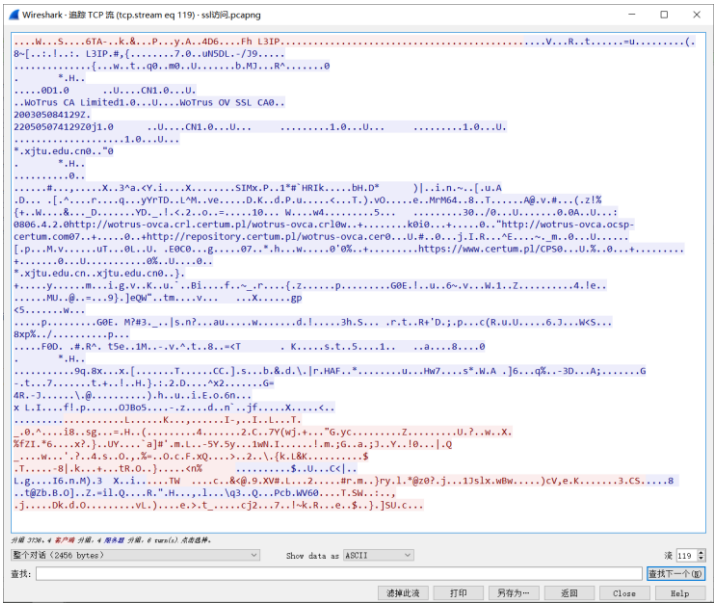
需要安装客户端。

主机主要与 222.90.111.20 进行通信，查询该 IP 发现该 IP 归属于西安市电信代理服务商。

分析报文发现通信报文主要以 TLS 协议为主，夹杂部分 TCP 报文。

2093	158.529299	192.168.43.93	222.90.111.20	TLSv1.2	197 Client Hello
2095	158.536843	222.90.111.20	192.168.43.93	TLSv1.2	1414 Server Hello
2101	158.539717	222.90.111.20	192.168.43.93	TLSv1.2	500 Certificate, Server Key Exchange, Server Hello Done
2102	158.540365	192.168.43.93	222.90.111.20	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2103	158.540495	192.168.43.93	222.90.111.20	TLSv1.2	982 Application Data
2105	158.570794	222.90.111.20	192.168.43.93	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
2106	158.572108	222.90.111.20	192.168.43.93	TLSv1.2	1414 Server Hello
2111	158.572565	222.90.111.20	192.168.43.93	TLSv1.2	485 Certificate, Server Key Exchange, Server Hello Done
2113	158.576359	222.90.111.20	192.168.43.93	TLSv1.2	1414 Application Data
2118	158.581493	192.168.43.93	222.90.111.20	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2123	158.583569	222.90.111.20	192.168.43.93	TLSv1.2	519 Application Data
2126	158.620045	222.90.111.20	192.168.43.93	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
2128	158.620852	192.168.43.93	222.90.111.20	TLSv1.2	625 Application Data
2129	158.679817	222.90.111.20	192.168.43.93	TLSv1.2	631 Application Data, Application Data
2132	158.684489	192.168.43.93	222.90.111.20	TLSv1.1	107 Application Data
2134	158.693425	192.168.43.93	222.90.111.20	TLSv1.1	143 Application Data
2158	158.857800	192.168.43.93	222.90.111.20	TLSv1.2	85 Encrypted Alert
2166	158.909298	222.90.111.20	192.168.43.93	TLSv1.2	85 Encrypted Alert

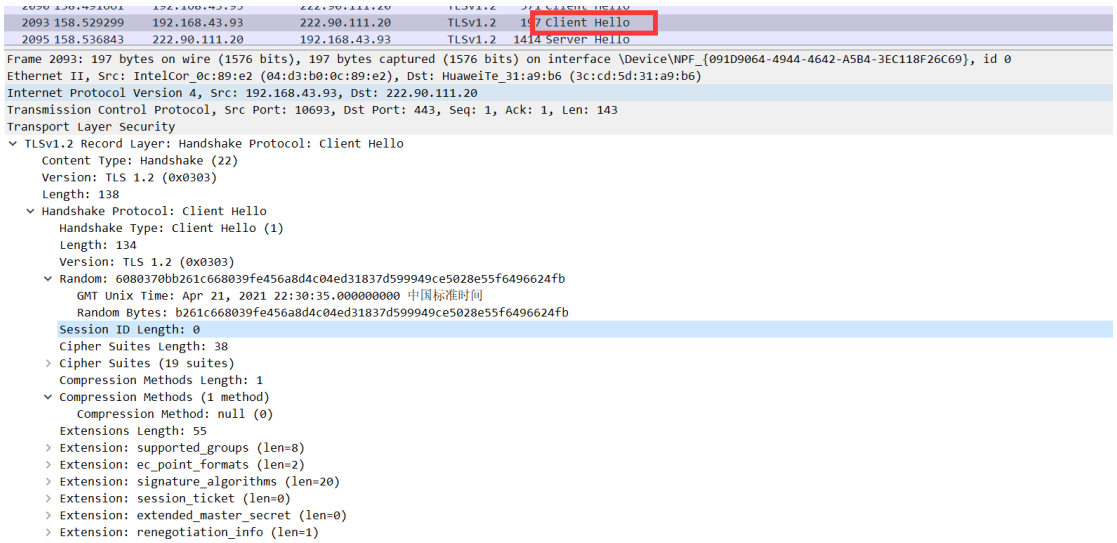
追踪字节流：



均为乱码数据。

接下来我们分析 TLS 协议的主要通信过程：

客户端发送 HELLO 报文（Client Hello）



Handshake type:握手类型，当下为 Client Hello

Random：强随机数，用于后续的密钥生成

SessionID:绘画 id,如果是第一次链接就为空

Cipher Suites:已知的密钥套件，按优先级排序，每条中包括协议、密钥加密算法、

签名、批量加密算法信息。

Compression Methods:压缩算法

Extension:各种其他参数

```
Cipher Suites (19 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

服务器接收 Hello 报文（Sever Hello），发送证书信息

```
2095 158.536843   222.90.111.20    192.168.43.93    TLSv1.2   1414 Server Hello
Frame 2095: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface \Device\NPF_{091D9064-4944-4642-A5B4-3EC118F26C69}, id 0
Ethernet II, Src: HuaweiTe_31:a9:b6 (3c:cd:5d:31:a9:b6), Dst: IntelCor_0c:89:e2 (04:d3:b0:0c:89:e2)
Internet Protocol Version 4, Src: 222.90.111.20, Dst: 192.168.43.93
Transmission Control Protocol, Src Port: 443, Dst Port: 10692, Seq: 1, Ack: 518, Len: 1360
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 104
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 100
        Version: TLS 1.2 (0x0303)
      Random: 6bc1cb8ebce27c8e583f82b10450adb4334aeab48819ca4c67bee1dce9080cbd
          GMT Unix Time: Apr 16, 2027 16:04:30.000000000 中国标准时间
          Random Bytes: bce27c8e583f82b10450adb4334aeab48819ca4c67bee1dce9080cbd
        Session ID Length: 32
        Session ID: fd76c6aec90202e102027e293ba3e882a6a28661c9d77f951114f87701fbc8dc
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 28
      Extension: renegotiation_info (len=1)
      Extension: ec_point_formats (len=4)
      Extension: application_layer_protocol_negotiation (len=11)
```

```
2101 158.539717   222.90.111.20    192.168.43.93    TLSv1.2   500 Certificate, Server Key Exchange, Server Hello Done
2102 158.540365   192.168.43.93    222.90.111.20    TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Frame 2101: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface \Device\NPF_{091D9064-4944-4642-A5B4-3EC118F26C69}, id 0
Ethernet II, Src: HuaweiTe_31:a9:b6 (3c:cd:5d:31:a9:b6), Dst: IntelCor_0c:89:e2 (04:d3:b0:0c:89:e2)
Internet Protocol Version 4, Src: 222.90.111.20, Dst: 192.168.43.93
Transmission Control Protocol, Src Port: 443, Dst Port: 10692, Seq: 4097, Ack: 518, Len: 446
[5 Reassembled TCP Segments (4086 bytes): #2095(1251), #2096(1360), #2098(1360), #2099(16), #2101(99)]
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4081
    Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4077
        Certificates Length: 4074
      Certificates (4074 bytes)
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
    Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
      EC Diffie-Hellman Server Params
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

证书的内容如下：

```
Certificates Length: 4074
Certificates (4074 bytes)
  Certificate Length: 1649
  Certificate: 3082066d30820555a003020102021062db4d4acffe8b525edd0b1497a1d3e7300d06092a… (id-at-commonName=*.xjtu.edu.cn,id-at-organizationName=西安交通大学,id-at-localityName=西…
  Certificate Length: 1208
  Certificate: 308204b43082039ca003020102021005ed88d8088d11ebddd623963cbaed42300d06092a… (id-at-commonName=WoTrus OV SSL CA,id-at-organizationName=WoTrus CA Limited,id-at-countr…
  Certificate Length: 1208
  Certificate: 308204b43082039ca003020102021100939285400165715f947f288fefc99b28300d0609… (id-at-commonName=Certum Trusted Network CA,id-at-organizationalUnitName=Certum Certific…
```

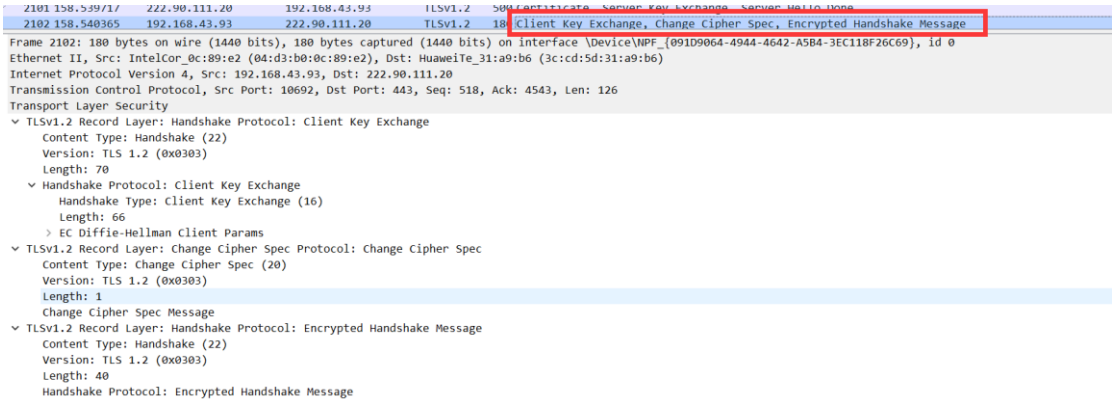
第一条为西安交大的证书，第二条为由 WoTrus CA 机构颁发的 DV 类型的 SSL

证书，第三条为：波兰证书签发机构签发的证书。

服务器密钥交换(Server Key Exchange)是可选的。仅当服务器提供的证书不足以允许客户端交换预主密钥时，才会发送此消息。

Sever_hello_done：通知客户端 Server_hello 信息结束。

客户端密钥交换、握手验证（Client Key Exchange+Change Cipher Spec+Encrypted Handshake Message）

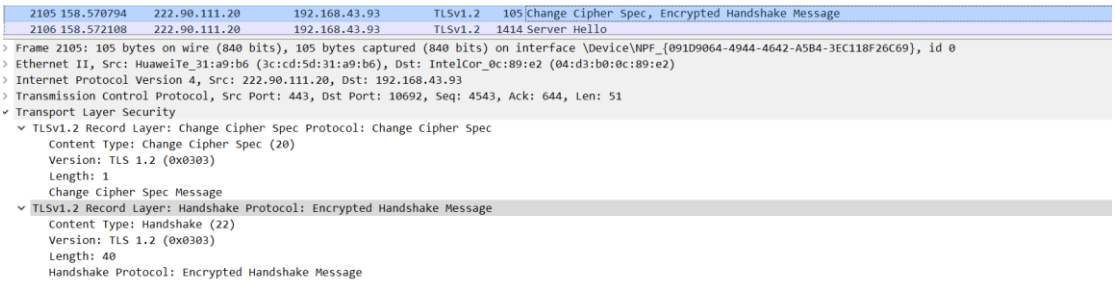


Client Key Exchange:客户端产生随机数 Pre-master 加密发回。

Change Cipher Spec：告知服务器后续的通信采用密钥加密传输。

Encrypted Handshake Message：生成一段测试数据进行测试。

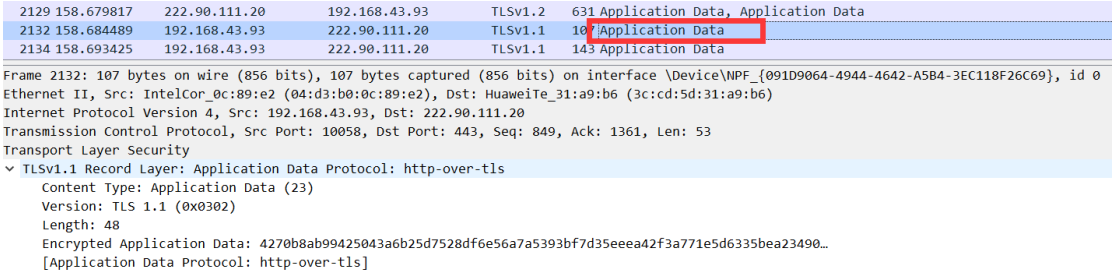
服务器生成密钥，解密测试信息，握手完成（Change Cipher Spec+Encrypted Handshake Message）



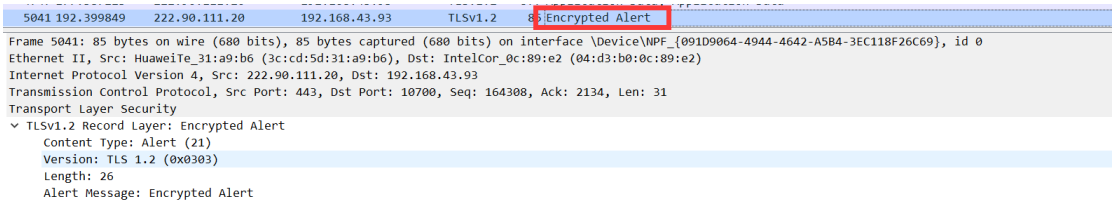
Change Cipher Spec:利用 Pre-master 和两个随机数生成密钥；并验证测试数据，通过之后告知服务器后续的通信采用密钥加密传输。

Encrypted Handshake Message：生成参数信息发回。

加密传输数据



警告信息（Encrypted Alert）

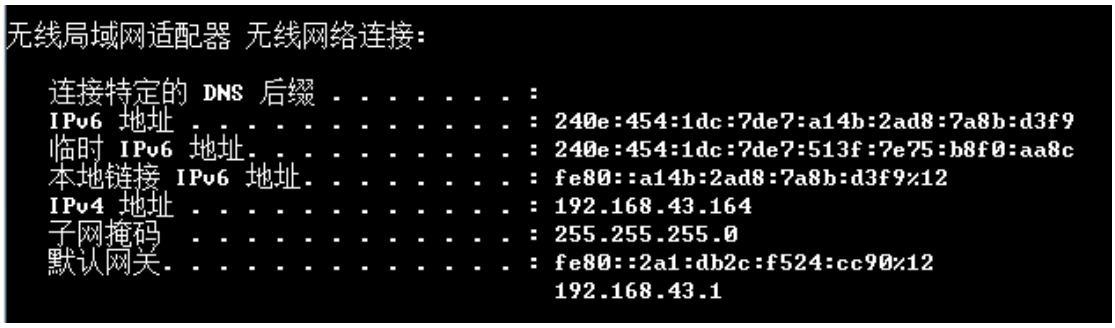


握手或通信过程中状态变化，一般由于链接关闭引起。

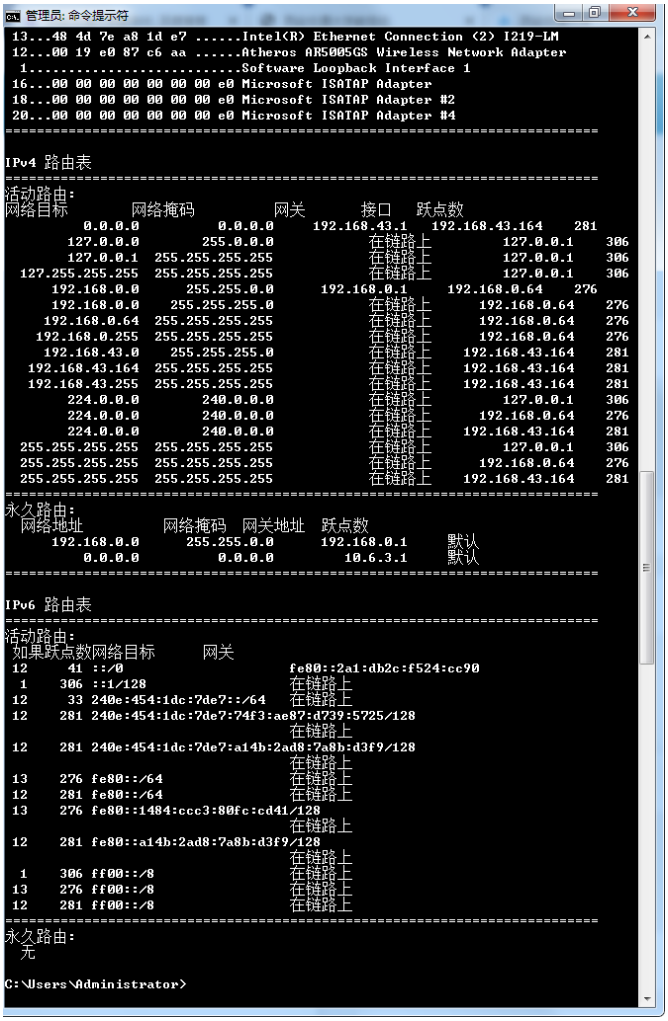
外网 webVPN 访问:

免插件安装。

数据包主要的通信地址为 117.32.153.183，查询归属地发现归属西安市电信运营商。绑定的域名为 webvpn.xjtu.edu.cn。只能在该页面内访问校园网资源。



本地路由表信息：



<table>
<tr><td rowspan="4">本组四人主要工作：</td><td colspan="3">施炎江：按实验指导进行操作，负责 PC1 的控制，连接设备，配置交换机，负责实验报告的一部分撰写和统筹。</td></tr>
<tr><td colspan="3">高浩翔：按实验指导进行操作，负责 PC4 的控制，连接设备，负责进阶自设计的准备和验收。</td></tr>
<tr><td colspan="3">薛杰锋：按实验指导进行操作，负责 PC2 的控制，连接设备，进行实时的实验报告初稿整理，负责实验报告的一部分撰写。</td></tr>
<tr><td colspan="3">贾星辰：按实验指导进行操作，负责 PC3 的控制，连接设备，配置防火墙，负责实验报告的一部分撰写。</td></tr>
<tr><td>实验中问题及解决方法，经验总结</td><td colspan="3">外网 PC 登录 VPN 客户端的过程中出现无法登录的情况，分析原因应该是多个主机使用同一用户而产生了冲突，解决方案是在防火墙端注销已登陆的 VPN 用户，然后再重新登陆即可解决问题。</td></tr>
<tr><td>师生互动交流</td><td colspan="3">在验收过程中，老师主要提出的一个问题是通过 web 方式连接和客户端方式连接的区别在哪，当时我们不是很理解，老师带着我们从原理图来分析，二者最本质的区别在于客户端方式连接会生成一个虚拟网卡而 web 方式连接不生成虚拟网卡。因此，抓包结果显示，web 方式连接是主机和防火墙直接的报文的发送和接收，而客户端方式连接是两台主机间报文的发送和接受。</td></tr>
<tr><td>验收教师</td><td>张利平</td><td>本实验成绩</td><td></td></tr>
</table>