计算机网络实验报告

警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4.实验报告文件以 PDF 格式提交。

专业	软件工程	班 级	19 级软件工程	组长	冼子婷
学号	18338072	18346019	18322043		
学生	冼子婷	胡文浩	廖雨轩		
实验分工					
冼子婷	进行实验，截图，编写和分析实验报告	廖雨轩	进行实验，截图，编写和分析实验报告		
胡文浩	进行实验，截图，编写和分析实验报告				

【实验题目】配置 TCP 负载分配

【实验目的】

1. 配置网络地址变换，使用一个单地址实现两台 WEB 服务器负载平衡。

【实验内容】

1. 完成实验实 9-4（P314），注意步骤 0 和步骤 6。
2. 在进行验证时如果不用 Web，而改用 Telnet 或远程桌面连接，同样能验证吗？
3. **请回答 P317 的实验思考。**

【实验要求】

重要信息需给出截图，注意实验步骤的前后对比。

【实验记录】(如有实验拓扑请自行画出)

【技术原理】

NAT TCP 负载均衡只适用于 TCP 连接，对于非 TCP 连接请求，NAT 进程将不会对其进行转换。在图 9-11 中，172.2.2.2 是虚拟服务器，172.2.2.2 是虚拟的 IP。NAT 路由器收到数据报时，查询 NAT 表，确定 172.2.2.2 已经被设定为映射到 Web-A、Web-B、Web-C 服务器的虚拟 IP。路由器收到主机 D 访问的数据包时，以**循环**方式把目的地址转换到对应的真实主机上（10.1.1.1、10.1.1.2 和 10.1.1.3），这样就可以完成内部真实主机（服务器）的 TCP 负载均衡。

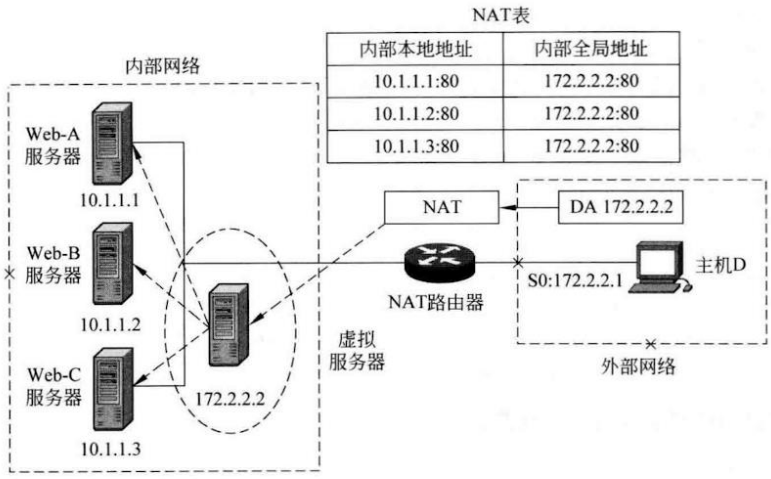


图 9-11　TCP 负载均衡

【实验拓扑】

本实验的拓扑结构如图 9-12 所示。选择 192.168.1.0/24 作为**私有地址**，采用 NAT 技术处理和外部网络的连接。内部有 2 台 Web 服务器，IP 地址分别为 192.168.1.5 和 192.168.1.6，虚拟服务器地址为 50.1.1.10。

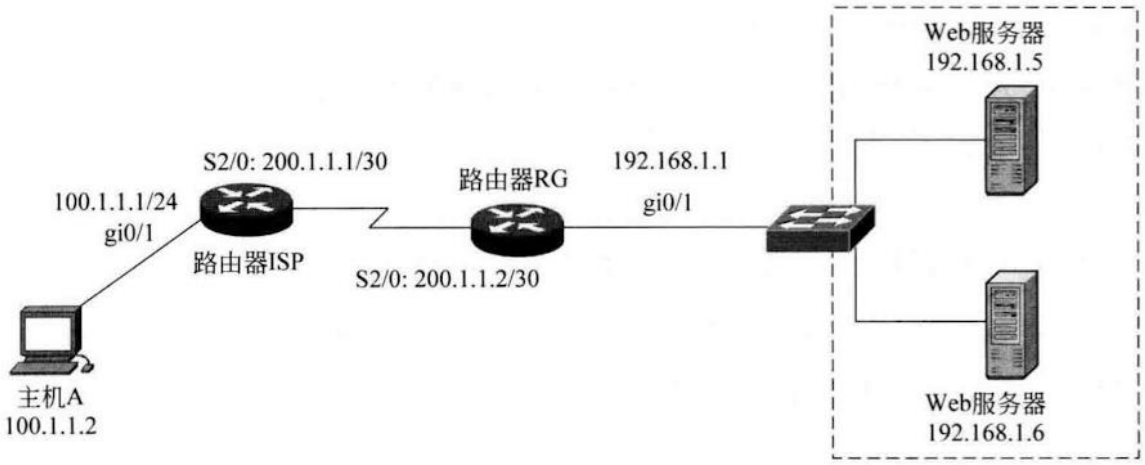


图 9-12　TCP 负载均衡实验拓扑

【实验设备】

路由器 2 台，交换机 1 台，计算机 1 台，Web 服务器 2 台。

【实验步骤】

分析：根据要求，可在路由器上定义内网与外网端口，利用 TCP 负载均衡实现 2 台服务器负载均衡。为此，必须搭建好服务器端的 Web 应用服务，可以是 Windows Server 自带的 IIS 服务或 Apache 服务，也可以是其他 Web 服务器软件。否则验证时 show ip nat translations、debug ip nat 均无法显示预期的结果。

步骤 0：

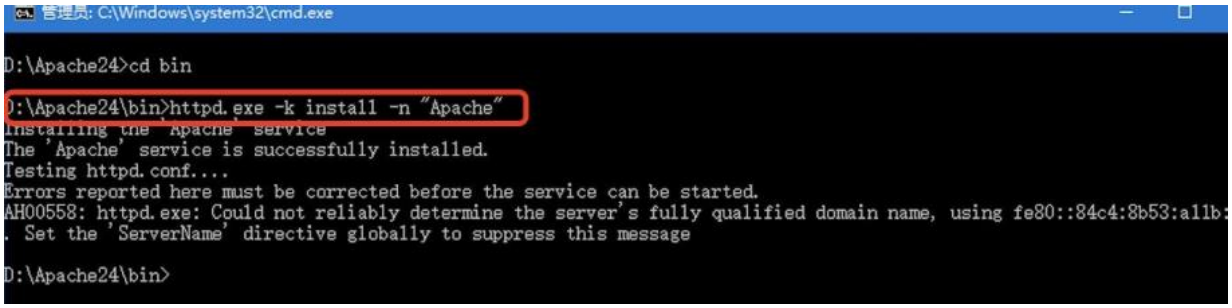
根据实验拓扑图连接主机、路由器和交换机，并进行主机和服务器 IP 地址的设置：

图 1：主机 A、Web 服务器 IP 设置图

步骤 1：

（1）搭建 Web 服务器

与实验 8 访问控制列表实验中搭建 Apache WEB 服务器一致，安装 Apache 并且更改本地 Apache 目录后将 WEB 服务器映射到本机 80 端口：



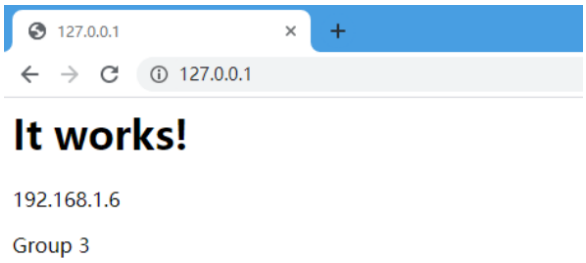
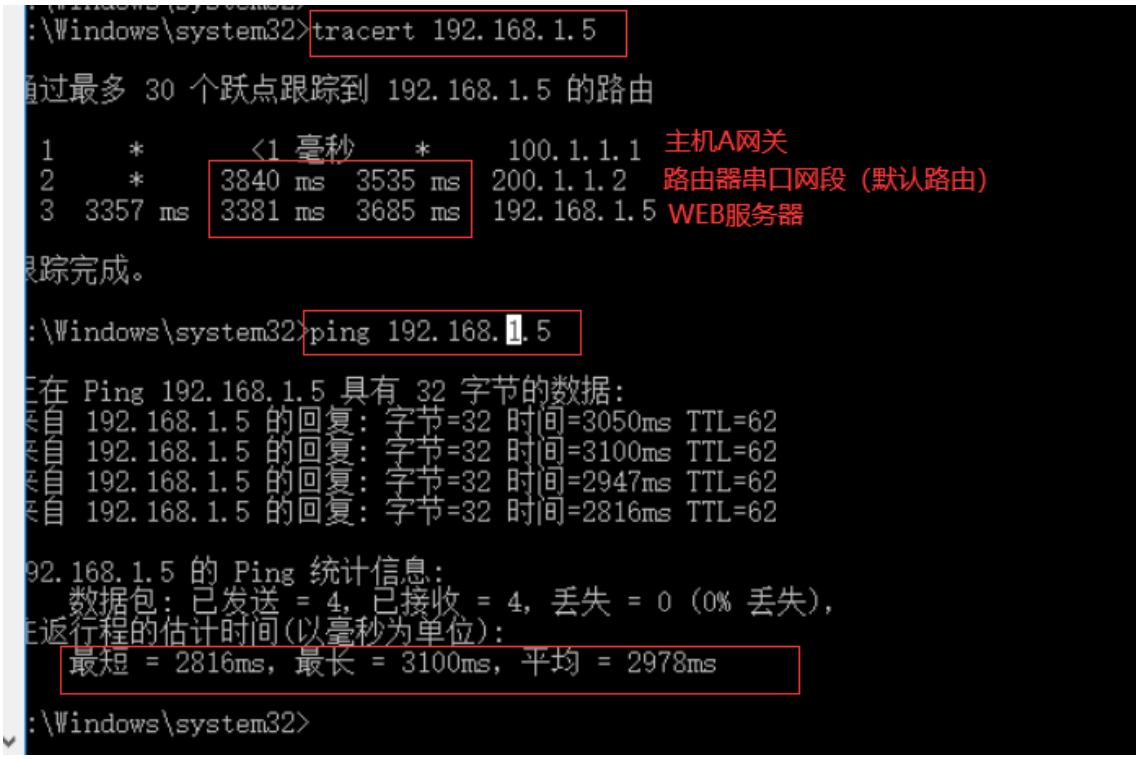


图 2：搭建 Web 服务器图

（2）在完成步骤 2 后，验证整个网络的连通性（必须确保连通）：

此时主机与 WEB 服务器之间经过两个路由与交换机，是连通的，但由于其路由器之间使用了默认路由，不论是用 ping 或是 tracert 验证连通性**其延迟都比较高**，甚至**偶尔会发生无法 ping 通**的情况。同时可以验证主机通过 http://192.168.1.5 和 http://192.168.1.6 打开这两个 WEB 服务器：



```
C:\Users\Administrator>tracert 192.168.1.6

通过最多 30 个跃点跟踪
到 DESKTOP-BVAQLT3 [192.168.1.6] 的路由:

  1    <1 毫秒    *        *     100.1.1.1  主机A网关
  2     *     2009 ms     *     200.1.1.2  路由器串口网段（默认路由）
  3  1652 ms  1646 ms  1609 ms  DESKTOP-BVAQLT3 [192.168.1.6] WEB服务器2

跟踪完成。

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.1.6

正在 Ping 192.168.1.6 具有 32 字节的数据:
来自 192.168.1.6 的回复: 字节=32 时间=1483ms TTL=62
来自 192.168.1.6 的回复: 字节=32 时间=1685ms TTL=62
来自 192.168.1.6 的回复: 字节=32 时间=1631ms TTL=62
来自 192.168.1.6 的回复: 字节=32 时间=1615ms TTL=62

192.168.1.6 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 = 1483ms, 最长 = 1685ms, 平均 = 1603ms
```

图 3：主机 A 分别 ping 两个路由器 1 和路由器 2

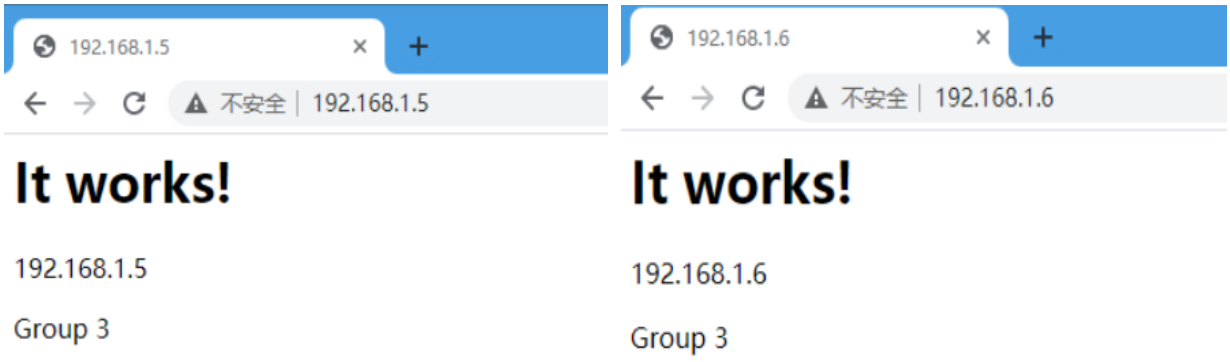


图 4：主机 A 能够分别登陆 2 个 Web 服务器

（3）查看 NAT 表：# show ip nat translations

此时由于还未设置路由器 RG 和路由器 ISP 的端口 IP 以及 NAT，所以 NAT 转换表此时为空。

```
RG#show ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
RG#
```

图 5：查看 NAT 表

步骤 2：在路由器上配置 IP 地址和路由。

路由器 RG 的设置：

```
RG(config)#interface serial 2/0
RG(config-if-Serial 2/0)#ip address 200.1.1.2 255.255.255.252
RG(config-if-Serial 2/0)#no shutdown
RG(config-if-Serial 2/0)#exit
RG(config)#
RG(config)#interface gigabitethernet 0/1
RG(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0
RG(config-if-GigabitEthernet 0/1)#no shutdown
RG(config-if-GigabitEthernet 0/1)#exit
RG(config)#
RG(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0
```

图 6：路由器 RG 设置

路由器 ISP 的设置：

按照网络拓扑图：

1）设置路由器串口 serial 2/0 的 IP 地址以及子网掩码:

```
interface serial 2/0
ip address 200.1.1.1 255.255.255.252
no shutdown
exit
```

2）设置 gigabitEthernet 0/1 的 IP 地址与子网掩码，即主机 A 的网关

```
Interface gigabitethernet 0.1
ip address  100.1.1.1 255.255.255.0
no shutdown
exit
```

3）在路由器 ISP 到路由器 RG 间添加默认路由

```
ip route 0.0.0.0 0.0.0.0 serial 2/0
```

```
11-RSR20-1#config
Enter configuration commands, one per line.  End with CNTL/Z.
11-RSR20-1(config)#hostname ISP
ISP(config)#
ISP(config)#interface serial 2/0
ISP(config-if-Serial 2/0)#ip address 200.1.1.1 255.255.255.252
ISP(config-if-Serial 2/0)#no shutdown
ISP(config-if-Serial 2/0)#exit
ISP(config)#
ISP(config)#interface gigabitethernet 0/1
ISP(config-if-GigabitEthernet 0/1)#ip address 100.1.1.1 255.255.255.0
ISP(config-if-GigabitEthernet 0/1)#no shutdown
ISP(config-if-GigabitEthernet 0/1)#exit
ISP(config)#
ISP(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0
ISP(config)#
```

图 7：路由器 ISP 的设置

步骤 3：通过一个虚拟主机许可声明定义一个拓展的 IP 访问列表。

在路由器 RG 上定义一个 access-list 扩展访问控制列表，**允许来自任何网段的地址访问 50.1.1.10 的 IP**。

```
Enter configuration commands, one per line.  End with CNTL/Z.
RG(config)#access-list 150 permit ip any host 50.1.1.10
RG(config)#$2.168.1.5 192.168.1.6 prefix-length 24 type rotary
RG(config)#
RG(config)#ip nat inside destination list 150 pool webserver
RG(config)#interface serial 2/0
RG(config-if-Serial 2/0)#ip nat outside
RG(config-if-Serial 2/0)#exit
RG(config)#interface gigabitethernet 0/1
RG(config-if-GigabitEthernet 0/1)#ip nat inside
RG(config-if-GigabitEthernet 0/1)#exit
```

图 8：通过一个虚拟主机许可声明定义一个拓展的 IP 访问列表

步骤 4：为真实主机定义一个 IP NAT 池，确保其为旋转式池。

在路由器终端由于该命令较长，前面部分被缩写，其源命令为：ip nat pool webserver 192.168.1.5 192.168.1.6 prefix-length 24 type rotary，定义一个全局地址池，该池名为 webserver，起始地址从 192.168.1.5 到终止地址 192.168.1.6，前缀长度为 24（即子网掩码长度），type rotary 表示定义为**轮转型**地址池，**每个地址分配的概率相等。**

```
Enter configuration commands, one per line.  End with CNTL/Z.
RG(config)#access-list 150 permit ip any host 50.1.1.10
RG(config)#$2.168.1.5 192.168.1.6 prefix-length 24 type rotary
RG(config)#
RG(config)#ip nat inside destination list 150 pool webserver
RG(config)#interface serial 2/0
RG(config-if-Serial 2/0)#ip nat outside
RG(config-if-Serial 2/0)#exit
RG(config)#interface gigabitethernet 0/1
RG(config-if-GigabitEthernet 0/1)#ip nat inside
RG(config-if-GigabitEthernet 0/1)#exit
RG(config)#debug ip nat
```

图 9：为真实主机定义一个 IP NAT 池，确保其为旋转式池。

步骤 5：定义访问列表与真实主机池之间的映射

使用 ip nat inside destination list 150 pool webserver，利用事先建立的 ACL 列表建立动态的**目的地址** destination 转换，将从 inside 内部端口进入，从 outside 外部端口出去的数据包，按照 list 150 **访问控制表**转换为**全局转换池** webserver 中的地址。按照下面的命令，可以理解为将主机 A 的数据包经过路由器 ISP 的目的地址进行**目的地址**转换，按照转换池中的地址循环遍历。

```
Enter configuration commands, one per line.  End with CNTL/Z.
RG(config)#access-list 150 permit ip any host 50.1.1.10
RG(config)#$2.168.1.5 192.168.1.6 prefix-length 24 type rotary
RG(config)#
RG(config)#ip nat inside destination list 150 pool webserver
RG(config)#interface serial 2/0
RG(config-if-Serial 2/0)#ip nat outside
RG(config-if-Serial 2/0)#exit
RG(config)#interface gigabitethernet 0/1
RG(config-if-GigabitEthernet 0/1)#ip nat inside
RG(config-if-GigabitEthernet 0/1)#exit
```

图 10：定义访问列表与真实主机池之间的映射

步骤 6：指定一个内部端口和一个外部端口

按照上述分析，将路由器串口网段定义为 outside 外部端口，主机 A 的网关第一跳端口设置为 inside 内部端口，即将主机 A 访问路由器 ISP 到路由器 RG 串口网段的数据包的**目的地址**虚拟地址 50.1.1.10 按照旋转池遍历修改，以达到 NAT **动态平衡**。

```
RG#config
Enter configuration commands, one per line.  End with CNTL/Z.
RG(config)#access-list 150 permit ip any host 50.1.1.10
RG(config)#$2.168.1.5 192.168.1.6 prefix-length 24 type rotary
RG(config)#
RG(config)#ip nat inside destination list 150 pool webserver
RG(config)#interface serial 2/0
RG(config-if-Serial 2/0)#ip nat outside
RG(config-if-Serial 2/0)#exit
RG(config)#interface gigabitethernet 0/1
RG(config-if-GigabitEthernet 0/1)#ip nat inside
RG(config-if-GigabitEthernet 0/1)#exit
```

图 11：指定一个内部端口和一个外部端口

步骤 7：验证测试。

（1）在主机 A 上用浏览器打开 http://50.1.1.10

此时使用主机 A 浏览器访问 http://50.1.1.10 发现其目的地址最终转换到了 192.168.1.5，也即 NAT 地址转换成功。

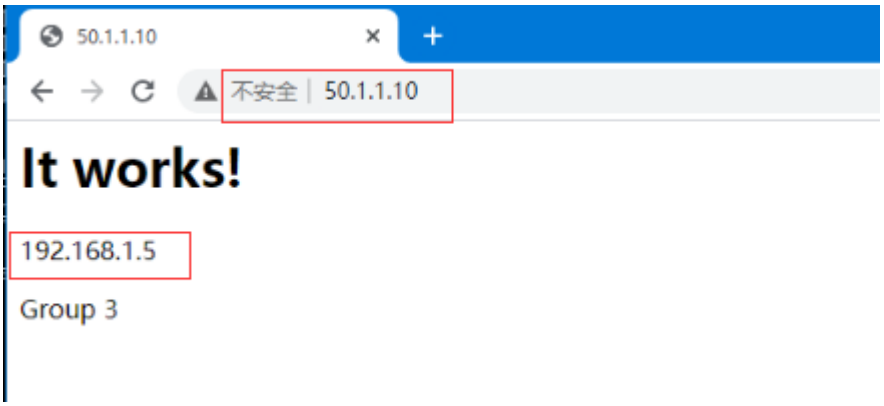
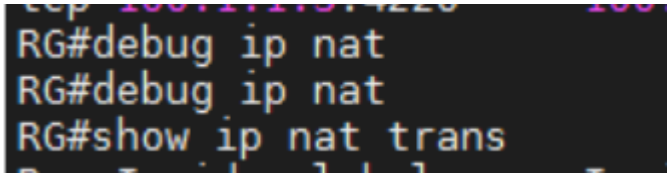


图 12：在主机 A 上用浏览器打开 http://50.1.1.10

（2）查看地址翻译的过程：#debug ip nat

当在 Cisco Packet Tracer 软件中路由器终端输入 debug ip nat 命令时，会提示 IP NAT debugging is on:




```
Router#debug ip nat
IP NAT debugging is on
Router#
```

图 13：debug ip nat 命令（上为锐捷路由器，下为思科模拟路由器）

表示正在调试 NAT，但在计网实验室 D502 机房中的路由器终端中输入 debug ip nat 没有反应，并且在后续 NAT 转换发生时，也没有显示 NAT 地址翻译的过程。我们怀疑是路由器的型号带来的差异或配

置上出了问题，但由于在 Cisco Packet Tracer 中思科的路由器并不支持使用 NAT 转换目的地址（实验室为锐捷路由器），只支持转换源地址，所以无法使用 Packet Tracer 补充该步骤：

```
Router(config)#ip nat inside ?
  source  Source address translation
Router(config)#ip nat inside
```

图 14：无法补充的步骤

（3）查看 NAT 表：#show ip nat translations；说明表中端口号有什么作用？

当主机 A 通过 50.1.1.10 访问 WEB 服务器时，使用 TCP 协议。内部端口中 Inside global 表示主机 A 的用于外部通信的**公网地址**，也即 ISP 提供的网址是 100.1.1.2，使用端口 3570-3572（我们打开了多个网页以测试负载均衡），而 Inside local 表示主机 A 在其内网中使用的 IP 地址和端口，由于主机 A 并没有使用 NAT，则其公网地址和内网地址一致。

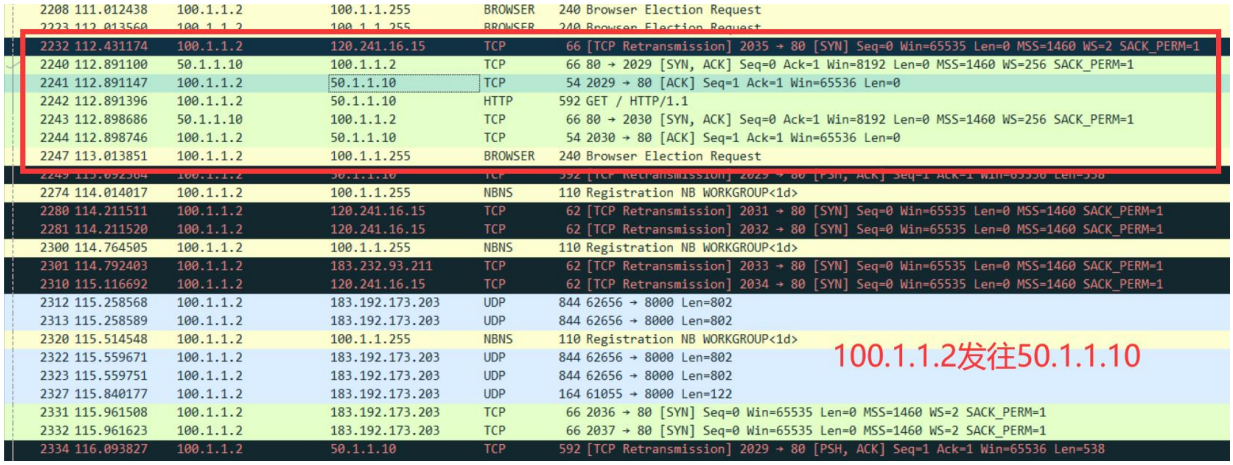
对于外部端口中，我们认为这两列应该是反了，其中 Outside local 才应该表示外部网络的**公网地址**，也即虚拟服务器地址 50.1.1.10。Outside global 为外部网络的**内网地址**，也即 192.168.1.5，其都使用 80 端口，以提供 WEB 服务。

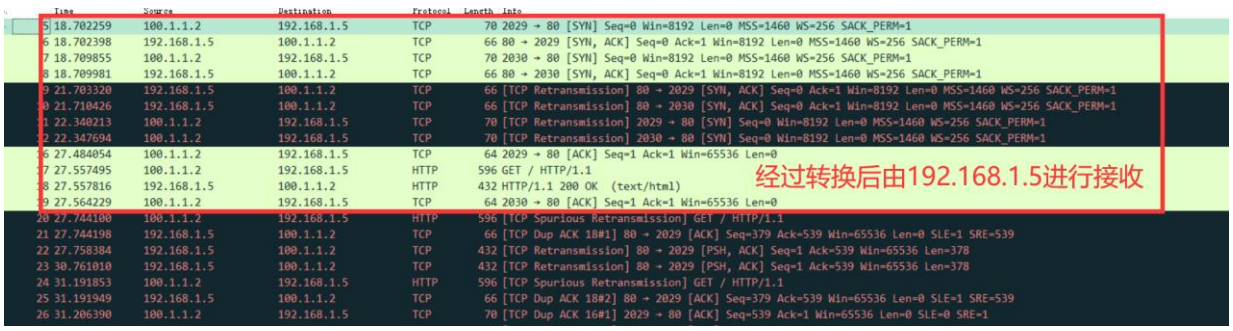
```
RG#show ip nat statis rule
ip nat inside destination list 150 pool webserver
        used 3 times
RG#show ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:3572     100.1.1.2:3572     50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:3570     100.1.1.2:3570     50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:3571     100.1.1.2:3571     50.1.1.10:80       192.168.1.5:80
```

图 15：查看 NAT 表

（4）在 Web 服务器上捕获数据包，查看发送过程中报文的 IP 地址转换情况，并作出合理解释。

使用 100.1.1.2 访问 http:// 50.1.1.10





使用 100.1.1.3 访问 http:// 50.1.1.10

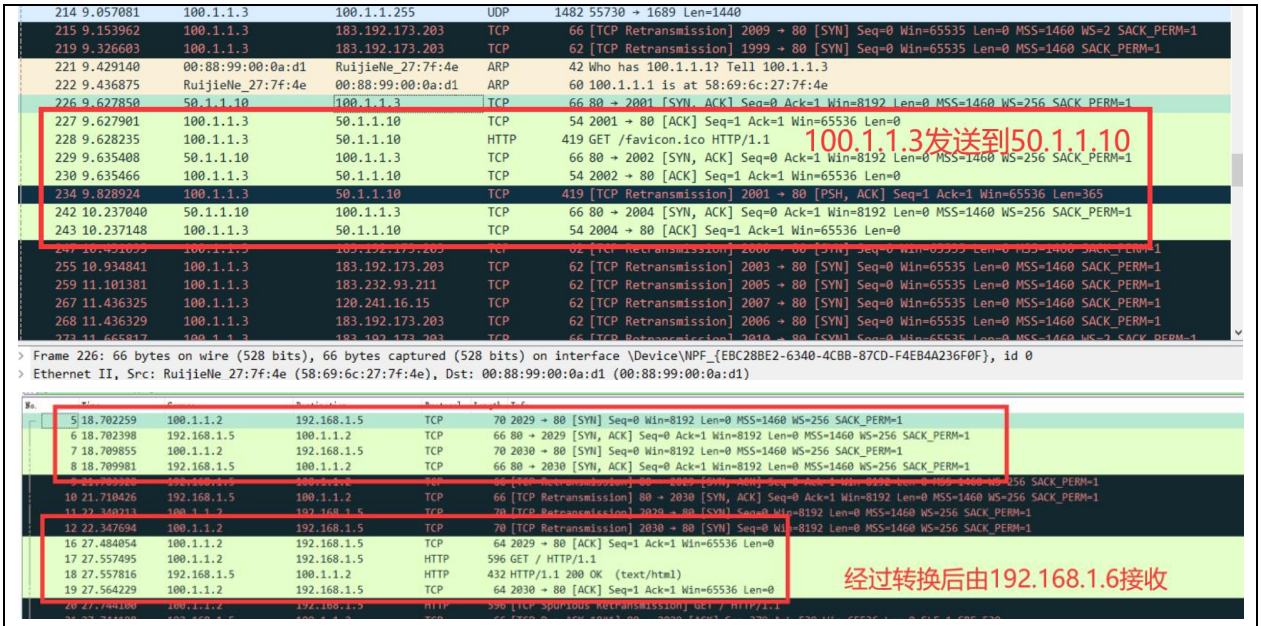


图 16：Wireshark 数据包截图

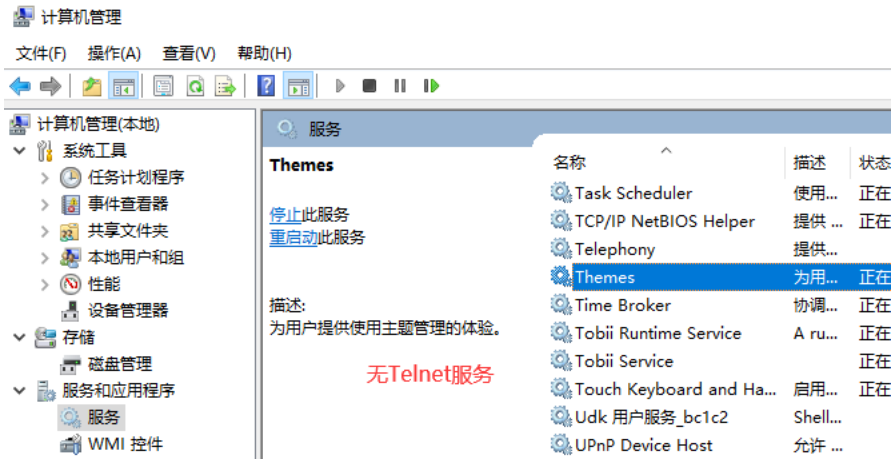
从 100.1.1.2 发送到 50.1.1.10 的数据包中可以知道主机 A 与该虚拟服务器开始进行三次握手的 TCP 连接过程，而且在 192.168.1.5 Web 服务器中也能够捕获到三次握手的 TCP 数据包。对比 SYN 与 ACK 的序号我们可以确认此时主机 A 与 192.168.1.5 的 Web 服务器建立了连接。

主机 A 发送出来的数据包通过指向 50.1.1.10 到达了 RG 路由器的 outside 端口，由于 RG 路由器启用了 NAT 转换技术，到达的数据包所指向的目的地被 RG 路由器改写为 192.168.1.5，然后从 RG 路由器的 inside 端口转发到 192.168.1.5 的 Web 服务器主机，从而实现了服务器资源的访问。

（5）在 192.168.1.5 和 192.168.1.6 主机上建立用户名和口令。建立方法是右击“计算机”图标，在弹出的快捷菜单中选择“管理”选项，在“计算机管理”窗口中选择“本地用户和组”->“用户”选项，右击后在弹出的快捷菜单中选择“新建用户”选项。分别采用 Telnet 和远程桌面连接（设置方法是右击“计算机图标”，在弹出的快捷菜单中选择“属性”选项，在“系统属性”对话框中选择“远程”，选择“允许用户远程到此计算机”复选框）的方法代替（1），重做（2）～（4）的内容。

建立的用户必须有属于管理员的权限（或直接用 administrator 用户登录）

Telnet 方法：由于 Windows10 中弃用了 Telnet 服务端服务，仅提供 Telnet 客户端服务，可以使用 MobaXterm 软件开启 telnet server 服务器。



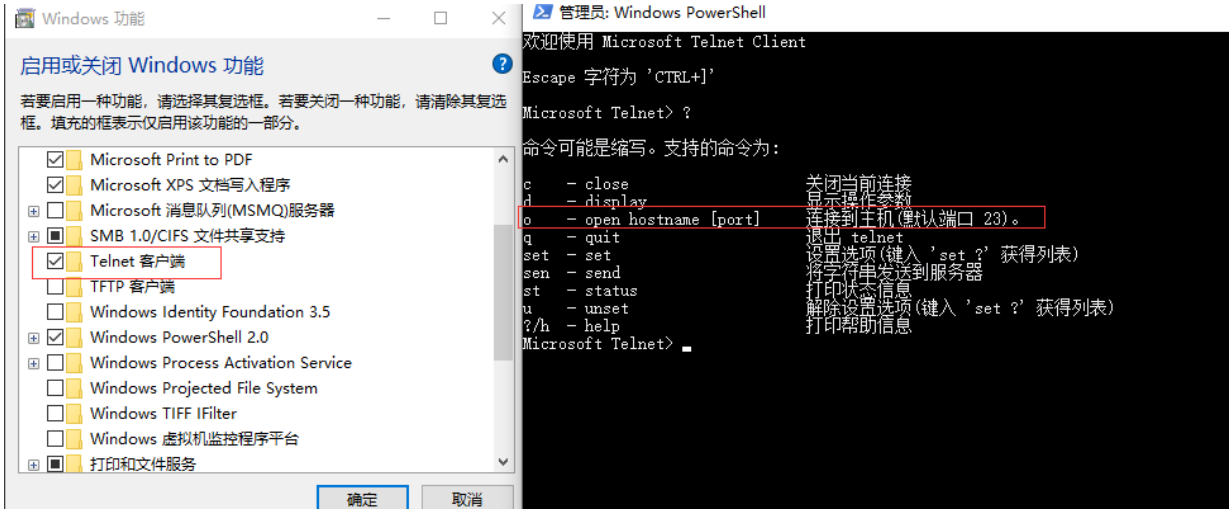


图 17：Windows10 不提供 Telnet 服务端服务，仅提供 Telnet 客户端服务。

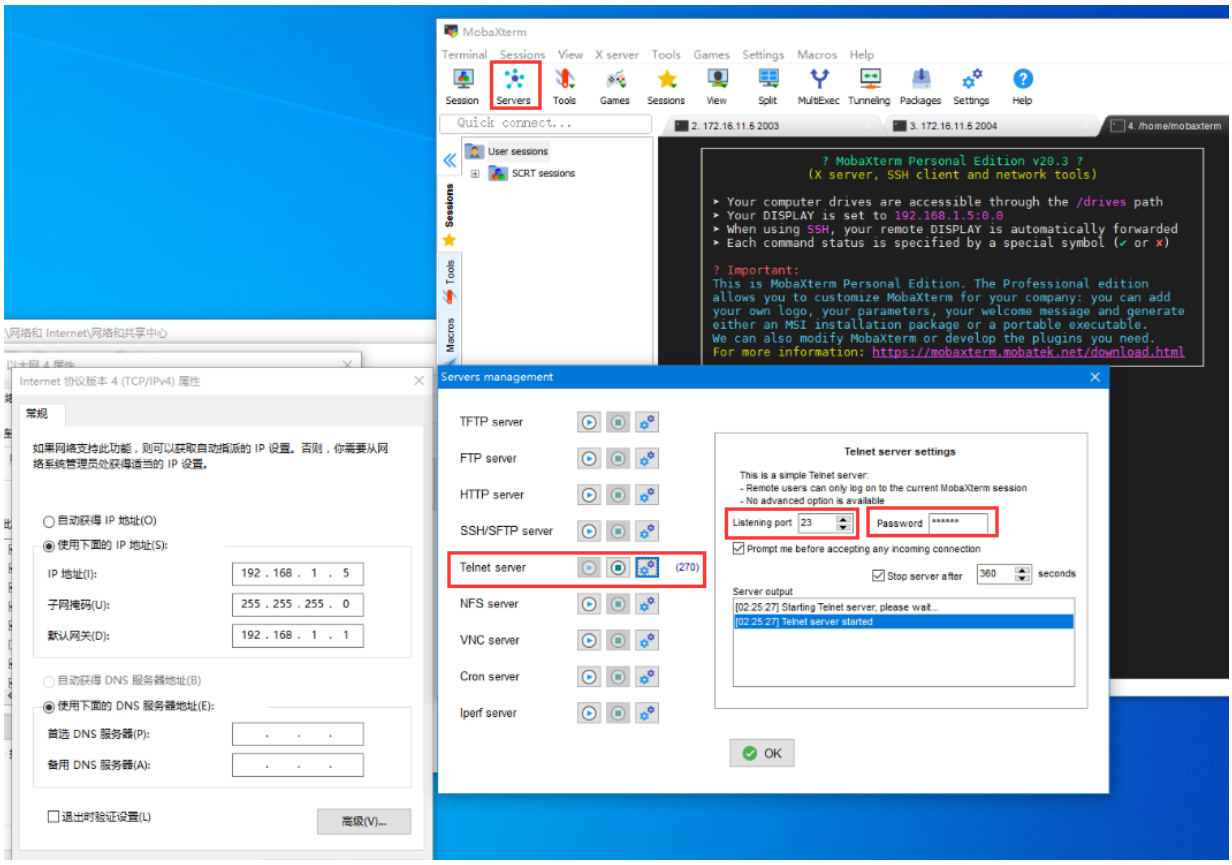


图 18：使用 MobaXterm 开启 Telnet Server

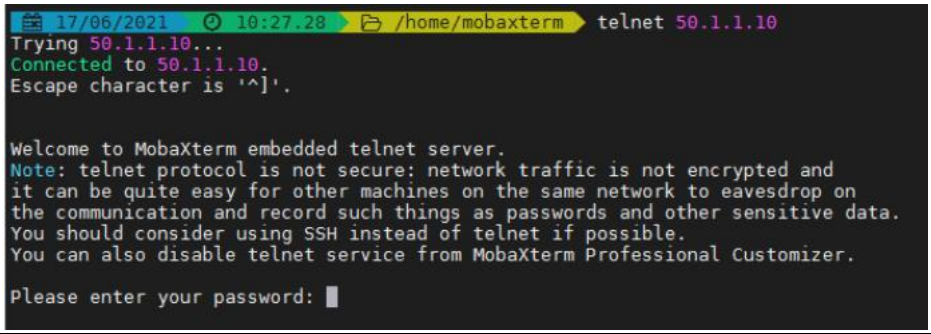
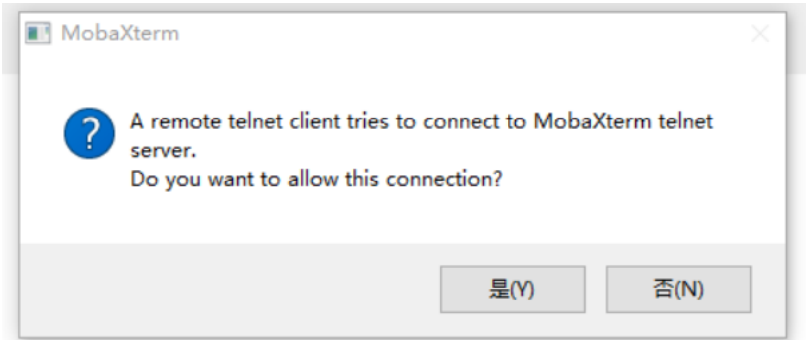


图 19：主机使用 telnet 50.1.1.10 连接 telnet 服务器




```
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:1839     100.1.1.2:1839     50.1.1.10:23       192.168.1.5:23
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:1839     100.1.1.2:1839     50.1.1.10:23       192.168.1.5:23
```

```
17/06/2021  10:27.28  /home/mobaxterm  telnet 50.1.1.10
Trying 50.1.1.10...
Connected to 50.1.1.10.
Escape character is '^]'.


Welcome to MobaXterm embedded telnet server.
Note: telnet protocol is not secure: network traffic is not encrypted and
it can be quite easy for other machines on the same network to eavesdrop on
the communication and record such things as passwords and other sensitive data.
You should consider using SSH instead of telnet if possible.
You can also disable telnet service from MobaXterm Professional Customizer.

Please enter your password:

  Login successful
```

图 20：输入密码后连接到 192.168.1.5 telnet 服务器

1）查看地址翻译的过程：#debug ip nat。
同步骤 7（3）中，由于路由器 debug 后无反应，无法显示结果。

2）查看 NAT 表：#show ip nat translations；说明表中端口号有什么作用？

```
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:1839     100.1.1.2:1839     50.1.1.10:23       192.168.1.5:23
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:1839     100.1.1.2:1839     50.1.1.10:23       192.168.1.5:23
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.3:1919     100.1.1.3:1919     50.1.1.10:23       192.168.1.6:23
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.3:1919     100.1.1.3:1919     50.1.1.10:23       192.168.1.6:23
RG#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.3:1919     100.1.1.3:1919     50.1.1.10:23       192.168.1.6:23
RG#
```

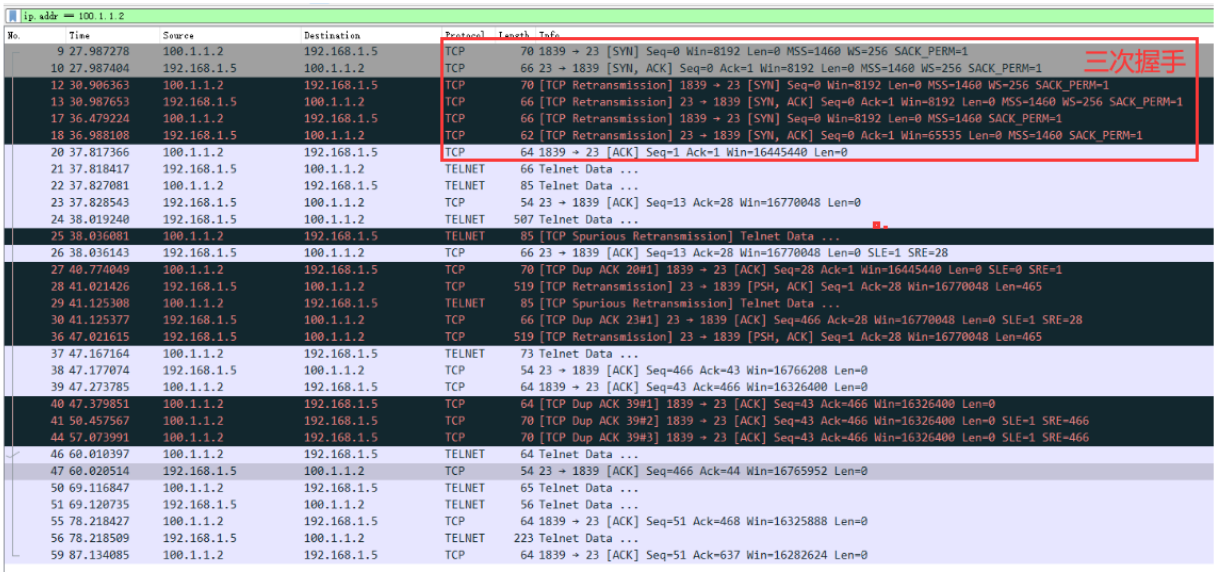
图 21：查看 NAT 表

当主机 A 通过使用 telnet 50.1.1.10 访问 telnet 服务器时，使用 TCP 协议。内部端口中 Inside global

表示主机 A 的用于外部通信的**公网地址**，也即 ISP 提供的网址是 100.1.1.2，使用端口 3570-3572（我们打开了多个网页以测试负载均衡），而 Inside local 表示主机 A 在其内网中使用的 IP 地址和端口，由于主机 A 并没有使用 NAT，则其公网地址和内网地址一致。

对于外部端口中，我们认为这两列应该是反了，其中 Outside local 才应该表示外部网络的**公网地址**，也即虚拟服务器地址 50.1.1.10。Outside global 为外部网络的**内网地址**，也即 192.168.1.5，其都使用 23 端口，以提供 telnet 服务。

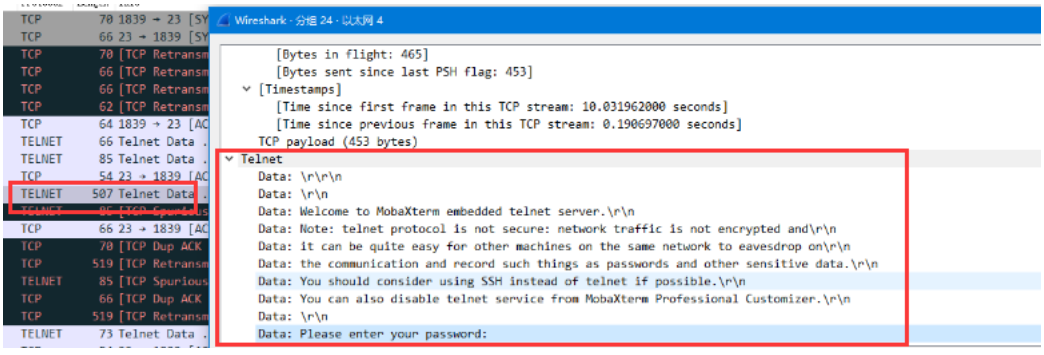
3）在 Telnet 服务器上捕获数据包，查看发送过程中报文的 IP 地址转换情况，并作出合理解释：

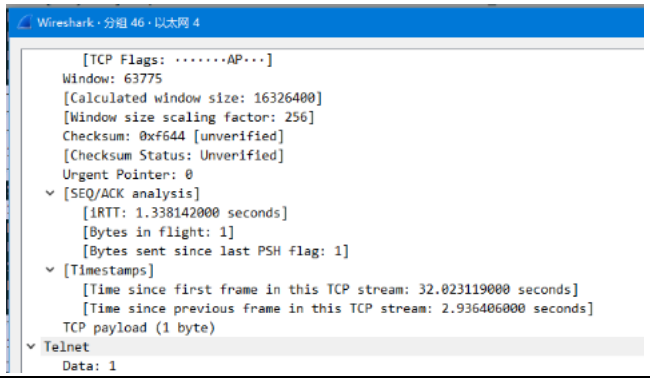


No.	Time	Source	Destination	Protocol	Length	Info
9	27.987278	100.1.1.2	192.168.1.5	TCP	70	1839 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	27.987404	192.168.1.5	100.1.1.2	TCP	66	23 → 1839 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	30.906363	100.1.1.2	192.168.1.5	TCP	70	[TCP Retransmission] 1839 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	30.987653	192.168.1.5	100.1.1.2	TCP	66	[TCP Retransmission] 23 → 1839 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	36.479224	100.1.1.2	192.168.1.5	TCP	66	[TCP Retransmission] 1839 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
18	36.988108	192.168.1.5	100.1.1.2	TCP	62	[TCP Retransmission] 23 → 1839 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
20	37.817366	100.1.1.2	192.168.1.5	TCP	64	1839 → 23 [ACK] Seq=1 Ack=1 Win=16445440 Len=0
21	37.818417	192.168.1.5	100.1.1.2	TELNET	66	Telnet Data ...
22	37.827081	100.1.1.2	192.168.1.5	TELNET	85	Telnet Data ...
23	37.828543	192.168.1.5	100.1.1.2	TCP	54	23 → 1839 [ACK] Seq=13 Ack=28 Win=16770048 Len=0
24	38.019240	192.168.1.5	100.1.1.2	TELNET	507	Telnet Data ...
25	38.036081	100.1.1.2	192.168.1.5	TELNET	85	[TCP Spurious Retransmission] Telnet Data ...
26	38.036143	192.168.1.5	100.1.1.2	TCP	66	23 → 1839 [ACK] Seq=13 Ack=28 Win=16770048 Len=0 SLE=1 SRE=28
27	40.774049	100.1.1.2	192.168.1.5	TCP	70	[TCP Dup ACK 20#1] 1839 → 23 [ACK] Seq=28 Ack=1 Win=16445440 Len=0 SLE=0 SRE=1
28	41.021426	192.168.1.5	100.1.1.2	TCP	519	[TCP Retransmission] 23 → 1839 [PSH, ACK] Seq=1 Ack=28 Win=16770048 Len=465
29	41.125308	100.1.1.2	192.168.1.5	TELNET	85	[TCP Spurious Retransmission] Telnet Data ...
30	41.125377	192.168.1.5	100.1.1.2	TCP	66	[TCP Dup ACK 23#1] 23 → 1839 [ACK] Seq=466 Ack=28 Win=16770048 Len=0 SLE=1 SRE=28
36	47.021615	192.168.1.5	100.1.1.2	TCP	519	[TCP Retransmission] 23 → 1839 [PSH, ACK] Seq=1 Ack=28 Win=16770048 Len=465
37	47.167164	100.1.1.2	192.168.1.5	TELNET	73	Telnet Data ...
38	47.177074	192.168.1.5	100.1.1.2	TCP	54	23 → 1839 [ACK] Seq=466 Ack=43 Win=16766208 Len=0
39	47.273785	100.1.1.2	192.168.1.5	TCP	64	1839 → 23 [ACK] Seq=43 Ack=466 Win=16326400 Len=0
40	47.379851	100.1.1.2	192.168.1.5	TCP	64	[TCP Dup ACK 39#1] 1839 → 23 [ACK] Seq=43 Ack=466 Win=16326400 Len=0
41	50.457567	100.1.1.2	192.168.1.5	TCP	70	[TCP Dup ACK 39#2] 1839 → 23 [ACK] Seq=43 Ack=466 Win=16326400 Len=0 SLE=1 SRE=466
44	57.073991	100.1.1.2	192.168.1.5	TCP	70	[TCP Dup ACK 39#3] 1839 → 23 [ACK] Seq=43 Ack=466 Win=16326400 Len=0 SLE=1 SRE=466
46	60.010397	100.1.1.2	192.168.1.5	TELNET	64	Telnet Data ...
47	60.020514	192.168.1.5	100.1.1.2	TCP	54	23 → 1839 [ACK] Seq=466 Ack=44 Win=16765952 Len=0
50	69.116847	100.1.1.2	192.168.1.5	TELNET	65	Telnet Data ...
51	69.120735	192.168.1.5	100.1.1.2	TELNET	56	Telnet Data ...
55	78.218427	100.1.1.2	192.168.1.5	TCP	64	1839 → 23 [ACK] Seq=51 Ack=468 Win=16325888 Len=0
56	78.218509	192.168.1.5	100.1.1.2	TELNET	223	Telnet Data ...
59	87.134085	100.1.1.2	192.168.1.5	TCP	64	1839 → 23 [ACK] Seq=51 Ack=637 Win=16282624 Len=0

图 22：Wireshark-TCP 三次握手

在 telnet 服务器上使用 Wireshark 捕获数据包，可以发现源主机地址 100.1.1.2 通过 telnet 50.1.1.10，虚拟地址经过 NAT 目的地址转换，最终转换到 192.168.1.5 服务器上，并且与该服务器建立 TCP 连接，经过三次握手后，开始发送 Telnet 数据包：





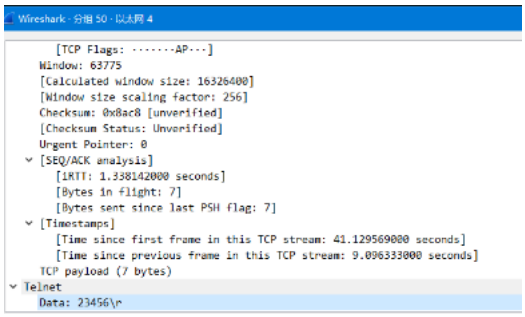


图 23：Wireshark-Telnet 数据包

并且可以发现，Telnet 使用明文传输密码，其中分组 46-50 中除了 TCP 包以外，Telnet 数据包中的载荷都为明文密码，这是极其不安全的，所以 Windows10 考虑到 Telnet 不支持加密，数据以纯文本通过网络，在后来的版本中也取消了这项古早的技术。

远程桌面连接方法：为了不更改计网实验室机器的配置，我们使用自己的电脑（两台 Windows10 专业版笔记本，开启远程桌面）
开启服务器中的远程桌面服务，使用主机 A 连接远程桌面：

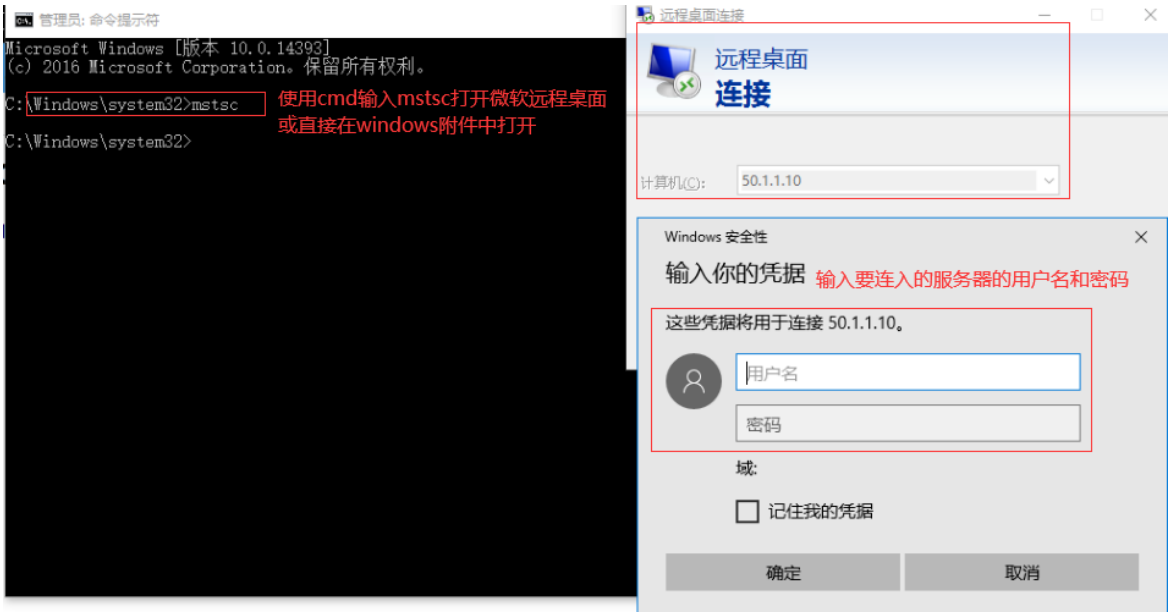
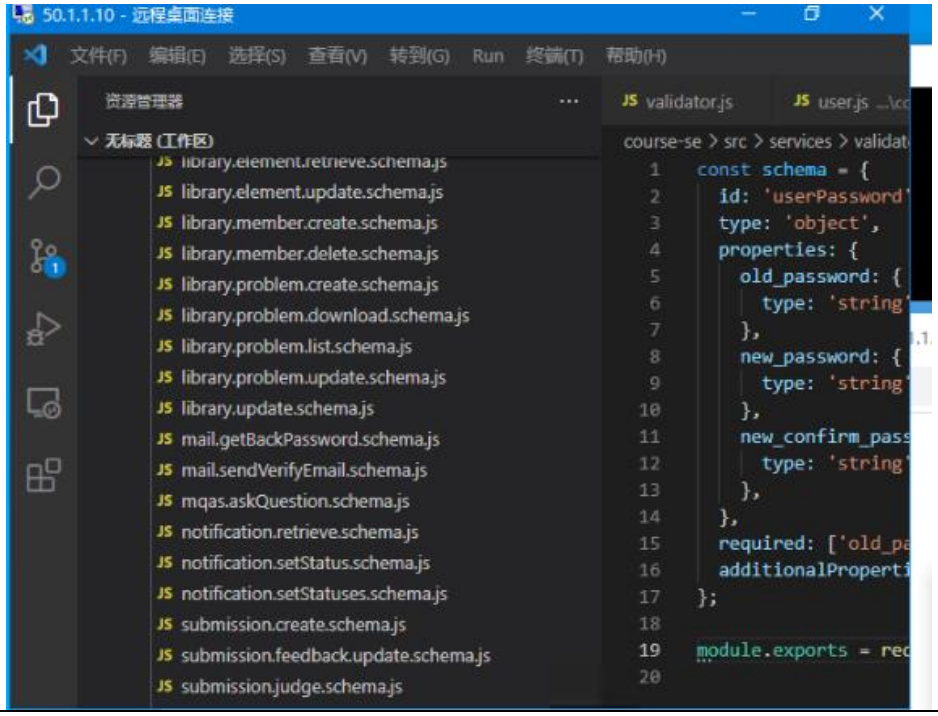


图 24：开启远程桌面

由于使用默认路由以及远程桌面**需要使用较大的带宽**，所以**连接过程较慢**，可以在连接时进行设置：



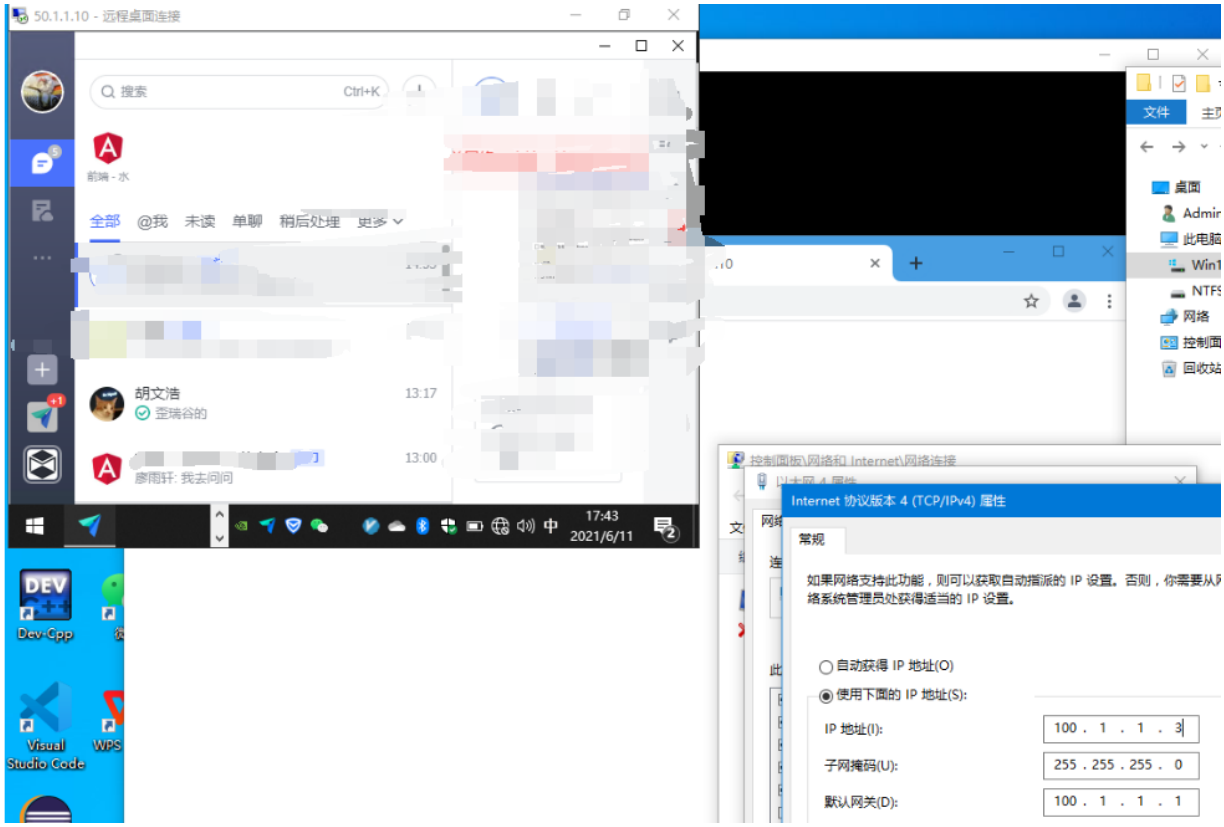


图 25：连接远程桌面

1）查看地址翻译的过程：#debug ip nat。
同步骤 7（3）中，由于路由器 debug 后无反应，无法显示结果。

3）查看 NAT 表：#show ip nat translations；说明表中端口号有什么作用？
当主机 A 通过 50.1.1.10 使用远程桌面服务时，使用 TCP 协议。内部端口中 Inside global 表示主机 A 的用于外部通信的**公网地址**，也即 ISP 提供的网址是 100.1.1.2，使用端口 3645 进行 TCP 连接，而 Inside local 表示主机 A 在其内网中使用的 IP 地址和端口，由于主机 A 并没有使用 NAT，则其公网地址和内网地址一致。
对于外部端口中，我们认为这两列应该是反了，其中 Outside local 才应该表示外部网络的公网地址，也即虚拟服务器地址 50.1.1.10。Outside global 为外部网络的内网地址，也即 192.168.1.5，其使用 3389 端口，以提供 Windows 远程桌面服务。

```
RG#show ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:3645     100.1.1.2:3645     50.1.1.10:3389     192.168.1.5:3389
RG#show ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.1.1.2:3645     100.1.1.2:3645     50.1.1.10:3389     192.168.1.5:3389
RG#
```

图 26：查看 NAT 表

4）在远程桌面上捕获数据包，查看发送过程中报文的 IP 地址转换情况，并作出合理解释：
整个连接使用的是 TCP，因此会首先进行 TCP 三次握手。在实验中还能够观察到 TLS 与 SSL 数据包，说明远程连接使用了 TLS 和 SSL 协议作为其传输层安全性协议，用于保证通信数据的保密性以及完整性。

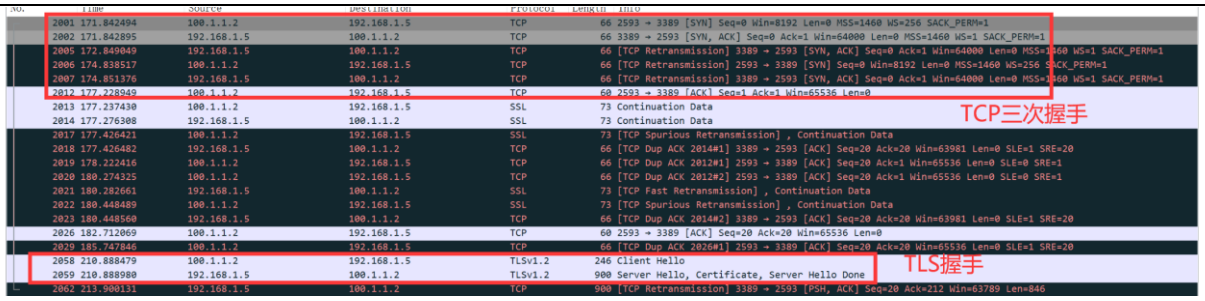


图 27：Wireshark-TCP 三次握手，TLS 握手

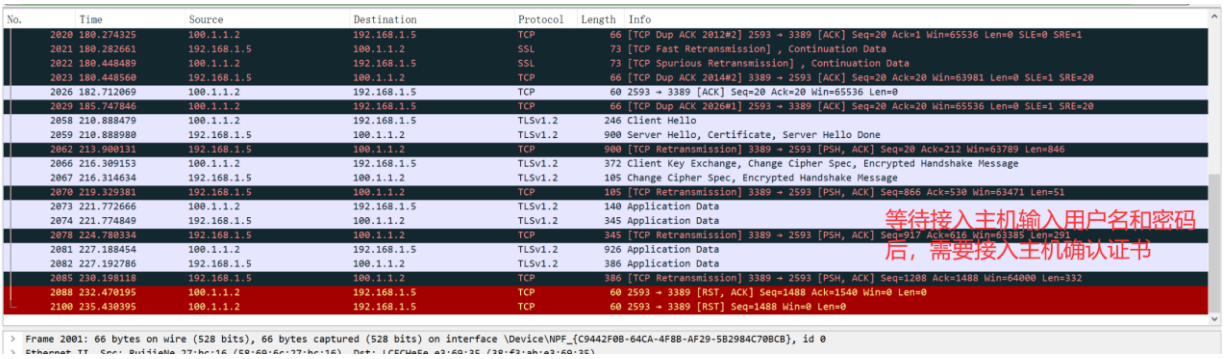


图 28：Wireshark-等待接入主机输入用户名和密码，需要接入主机确认证书

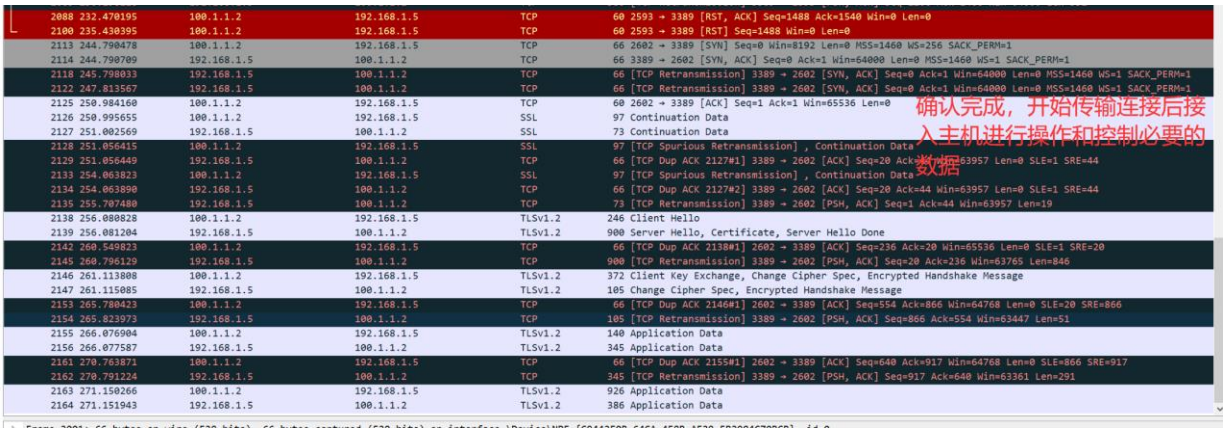


图 29：Wireshark-确认完成，开始传输连接后接入主机进行操作和控制的必要数据

由于路由器使用了 NAT 技术以及默认路由，因此在进行远程连接的时候需要等待非常长的时间才能够进行远程主机的控制和操作。并且当尝试关闭连接时，由于网络质量差，导致关闭的操作并不能够正常地退出远程连接，因此最后观察到了带有 RST 的 TCP 包，表示这个连接异常关闭。

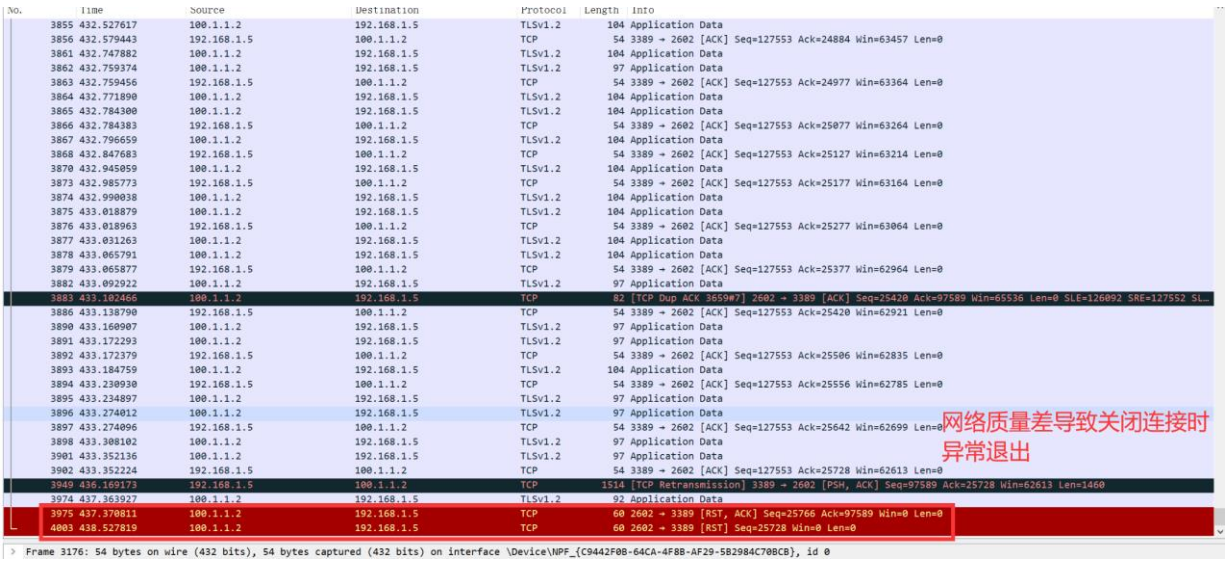


图 30：Wireshark-网络质量差导致关闭连接时异常退出。

【实验思考】

（1）实验时不能简单地采用从主机 A ping 50.1.1.10 的方式进行验证，这是什么原因？

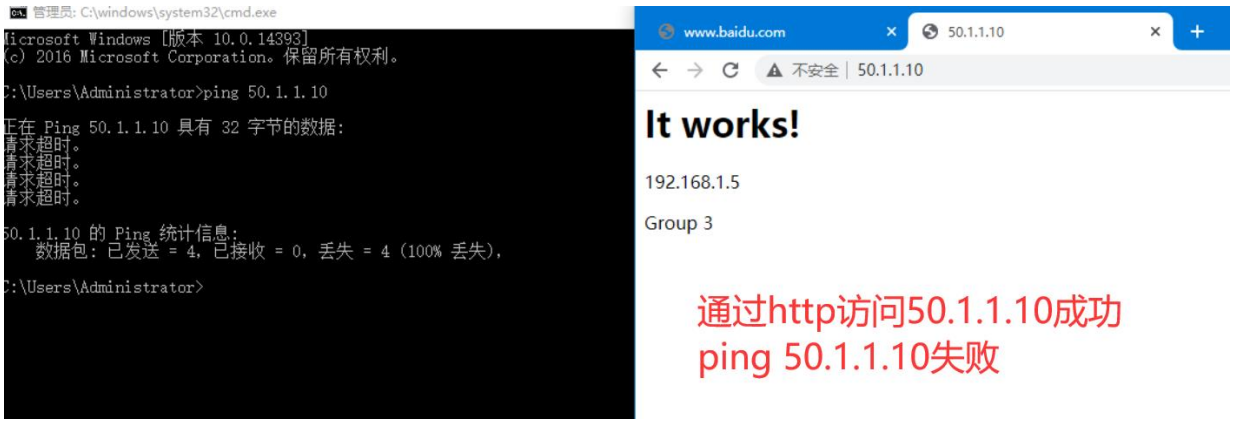


图 31：Wireshark-Ping 失败，http 访问失败

使用网络地址转换 NAT 技术后，由于地址的内/外部特性，即服务器的真实地址已经藏在了虚拟地址后面，不能简单地通过 ping 或 tracert 的方法验证连通性。并且由于 NAT TCP 负载均衡仅适用于 TCP 链接，对于使用 ICMP 包的 ping 方法，NAT 进程不会对其进行转换，并且 ping 和 tracert 不能再进行端对端 IP 的追踪，所以需要使用 telnet 或远程桌面或 WEB 服务的方式验证连通性以及负载均衡。

（2）TCP 负载均衡与访问量有关吗？请设计有效方法，该方法可以考查到负载均衡的效果，并总结其规律性。

我们认为 TCP 负载均衡**与访问量无关**而是**与当前服务器的最小连接数有关**，当使用同一台主机 A，固定其 IP 为 100.1.1.2 时，不论开启多少 TCP 链接到虚拟地址 50.1.1.10，其最终还是转换到了 192.168.1.5，不会走到 192.168.1.6（我们猜测是由于默认 NAT 中 TCP 连接过期时间较长，可能为 24 小时，但在锐捷路由器中没有办法修改其过期时间以验证当该机器 TCP 连接过期后，是否会连接到旋转池中下一个 IP 地址）。

而当修改主机 A 的 IP 地址为 100.1.1.3 时，开启新的 TCP 链接到 50.1.1.10，此时为了**负载均衡**，NAT 会选择最小连接数的服务器与其链接，也即 100.1.1.3 连接到了 192.168.1.6 服务器，并且此时 show ip nat translations，上一个 IP 与服务器的 TCP 连接还未过期，并且由于 TCP 连接的寿

命较长，就算切换回 100.1.1.2 IP 重新连接 WEB 服务器，也仍然会走老的连接，即 192.168.1.5。

```
RG#show ip nat translations
Pro Inside global       Inside local        Outside local      Outside global
tcp 100.1.1.2:1246      100.1.1.2:2780      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2808      100.1.1.2:2808      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2810      100.1.1.2:2810      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2748      100.1.1.2:2748      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2681      100.1.1.2:2681      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2815      100.1.1.2:2815      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2804      100.1.1.2:2804      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2806      100.1.1.2:2806      50.1.1.10:80       192.168.1.5:80
RG#show ip nat translations
Pro Inside global       Inside local        Outside local      Outside global
tcp 100.1.1.2:1246      100.1.1.2:2780      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2808      100.1.1.2:2808      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2810      100.1.1.2:2810      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2681      100.1.1.2:2681      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2815      100.1.1.2:2815      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2804      100.1.1.2:2804      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2806      100.1.1.2:2806      50.1.1.10:80       192.168.1.5:80
RG#show ip nat translations
Pro Inside global       Inside local        Outside local      Outside global
tcp 100.1.1.3:2921      100.1.1.3:2921      50.1.1.10:80       192.168.1.6:80
tcp 100.1.1.2:1246      100.1.1.2:2780      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2808      100.1.1.2:2808      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.3:2923      100.1.1.3:2923      50.1.1.10:80       192.168.1.6:80
tcp 100.1.1.2:2681      100.1.1.2:2681      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2815      100.1.1.2:2815      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2804      100.1.1.2:2804      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.2:2806      100.1.1.2:2806      50.1.1.10:80       192.168.1.5:80
tcp 100.1.1.3:2924      100.1.1.3:2924      50.1.1.10:80       192.168.1.6:80
RG#show ip nat translations
```

全部来自100.1.1.2主机A，不论开启多少TCP链接，仍会连上192.168.1.5的WEB服务器

当更改主机A的IP地址为100.1.1.3，此时再访问50.1.1.10，此时链接到了192.168.1.6WE

图 32：验证负载均衡的效果-1

使用远程桌面服务，同样地，只有当修改主机 A 的 IP 后，才能实现负载均衡，也即**按照最小连接数循环分配连接池中的 IP**：

```
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
tcp 100.1.1.3:4198      100.1.1.3:4198      50.1.1.10:3389      192.168.1.6:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
tcp 100.1.1.3:4198      100.1.1.3:4198      50.1.1.10:3389      192.168.1.6:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
tcp 100.1.1.3:4198      100.1.1.3:4198      50.1.1.10:3389      192.168.1.6:3389
RG#show ip nat trans
Pro Inside global       Inside local        Outside local       Outside global
tcp 100.1.1.2:3681      100.1.1.2:3681      50.1.1.10:3389      192.168.1.5:3389
tcp 100.1.1.3:4198      100.1.1.3:4198      50.1.1.10:3389      192.168.1.6:3389
```

图 33：验证负载均衡的效果-2

（3）本实验采用的技术有什么现实意义？

计算机网络实验报告

1）NAT 网络地址转换可以允许内部网络使用私有地址，并且通过设置合法地址池让内部网络可以与外部网络进行通信，以达到节约地址的目的。通过使用少量的全球 IP 地址（公网 IP 地址）代表较多的私有 IP 地址的方式，将有助于减缓可用的 IP 地址空间的枯竭。
2）同时 NAT 网络地址转换技术可以减少规划地址集时地址重叠的情况发生，其增强了内部网络与外部网络连接的灵活性，通过地址集、备份地址、负载分担以及均衡地址集确保了其可靠性，可以隐藏内部地址，以提高本地系统的可靠性。
3）在现实生活中，由于 IPv4 地址数量稀少，并且已经分配完毕而 IPv6 技术还未完全部署，面对日益增长的网络设备和缺乏的 IPv4 地址，此时就需要用到网络地址转换技术节约地址，让用户的每个网络设备都能正常访问 Internet。

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）

学号	学生	自评分
18338072	冼子婷	98
18322043	廖雨轩	98
18346019	胡文浩	98

【交实验报告】

上传实验报告：ftp://172.18.178.1/　　截止日期（不迟于）：1 周之内

上传包括两个文件：

（1）小组实验报告。上传文件名格式：小组号_ Ftp 协议分析实验.pdf （由组长负责上传）

例如: 文件名“10_ Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告

（2）小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。

文件名格式：小组号_学号_姓名_ Ftp 协议分析实验.pdf （由组员自行上传）

例如: 文件名“10_05373092_张三_ Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告。

注意：不要打包上传！