



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。

【实验题目】NAT 实验。

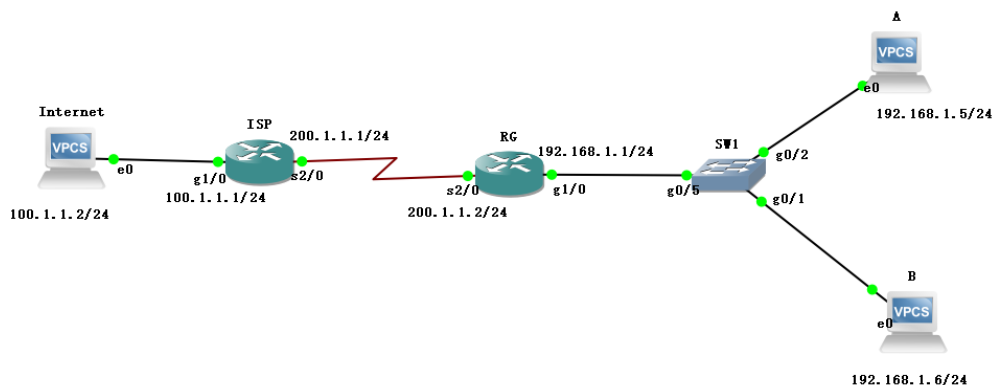
院系	电子与信息工程学院	班 级	通信工程 1 班	组长	刘渤
学号	16308073	16308161	16308091	16308015	
学生	刘渤	邹紫婧	彭肖文	陈瑞佳	
实验分工					
刘渤	NAT 模块 贡献: 25%		邹紫婧	NAT 模块 贡献: 25%	
彭肖文	NAT 模块 贡献: 25%		陈瑞佳	NAT 模块 贡献: 25%	

【实验目的】

配置网络地址变换，提供共享服务器的可靠外部访问。

【实验内容】

实验拓扑：



第二版

1. 完成实验 9.1 静态 NAT (P306)、9.2 动态 NAT (P308)、9.3 端口 NAT (P311)

第一版：

1. 完成实验 6.1 静态 NAT (P199)、6.2 动态 NAT (201)、6.3 端口 NAT (204)

2. 注意：实验中的 ISP 路由器不用配置默认路由（课本上是错的，因为配置了默认路由，就直接可以互相 ping 通，不需要 NAT 了）。

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)

一、NAT 实验

【实验步骤】

步骤 1:

配置 telnet 用户名和口令；

查看 NAT 表：



```
-----
21-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
21-RSR20-2#
```

可以看出，未配置之前没有 NAT 信息。

步骤 2:

配置 ip 路由和地址，按照实验书教程配置，例如 ISP 路由的配置：

```
Password:
21-RSR20-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
21-RSR20-1(config)#interface serial 2/0
21-RSR20-1(config-if-Serial 2/0)#ip address 200.1.1.1 255.255.255.0
21-RSR20-1(config-if-Serial 2/0)#interface gigabitethernet 0/1
21-RSR20-1(config-if-GigabitEthernet 0/1)#ip address 100.1.1.1 255.255.255.0
21-RSR20-1(config-if-GigabitEthernet 0/1)#exit
21-RSR20-1(config)#ip route 0.0.0.0 0.0.0.0 serial 2/0
21-RSR20-1(config)#
```

步骤 3:

静态转换配置：

步骤 4:

指定一个内部端口和外部端口；

我们全部配置完毕之后，可以查看路由表（R1 为 ISP 路由器，R2 为 RG 路由器）

输入 show ip interface brief 查看 RG 路由器的路由表

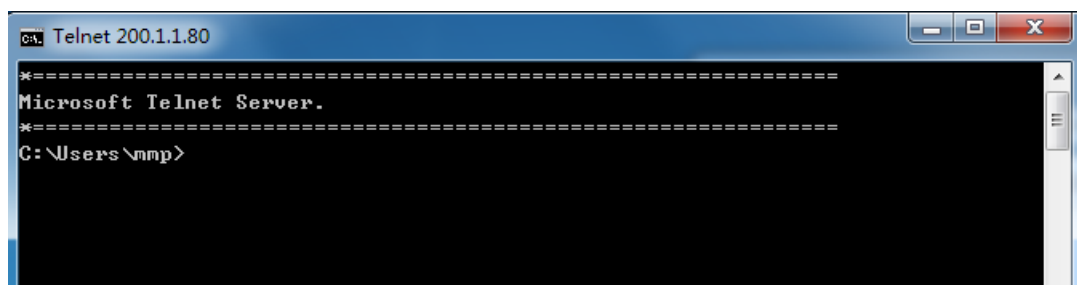
```
21-RSR20-2(config)#
21-RSR20-2(config)#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)      Statu
s
Serial 2/0                Protocol              200.1.1.1/24          no address            up
                          up
Serial 3/0                down                  no address            no address            down
                          down
GigabitEthernet 0/0       down                  no address            no address            down
                          down
GigabitEthernet 0/1       up                    192.168.1.1/24        no address            up
VLAN 1                    down                  no address            no address            up
                          down
21-RSR20-2(config)#
```

可以发现端口是正确的，和我们配置的相同。

按照步骤配置好交换机和路由器之后：

（1）在路由器 ISP 端用 Telnet（或远程桌面）登录远程主机 200.1.1.80，测试 NAT 的转换。

我们在命令行输入 telnet 200.1.1.80，可以出现如下界面，登录成功





然后可以对这台主机做出操作，比如在登录的用户上查看目录和新建文件。

```
C:\ Telnet 200.1.1.81
Microsoft Telnet Server.
*=====
C:\Users\chen>cd
C:\Users\chen

C:\Users\chen>dir
驱动器 c 中的卷是 系统分区
卷的序列号是 0000-4823

C:\Users\chen 的目录
2018/12/20 17:48 <DIR>      .
2018/12/20 17:48 <DIR>      ..
2009/07/14 10:34 <DIR>      Desktop
2018/12/20 17:48 <DIR>      Documents
2009/07/14 10:34 <DIR>      Downloads
2009/07/14 10:34 <DIR>      Favorites
2009/07/14 10:34 <DIR>      Links
2009/07/14 10:34 <DIR>      Music
2009/07/14 10:34 <DIR>      Pictures
2009/07/14 10:34 <DIR>      Saved Games
2009/07/14 10:34 <DIR>      Videos
          0 个文件          0 字节
          11 个目录 174,374,375,424 可用字节

C:\Users\chen>
```

(2) 查看地址翻译的过程：#debug ip nat 分析结果

由于锐捷交换机不支持 debug ip nat，我们输入之后没有现象产生，无论是在 terminal 环境的里面还是外面都没有现象。

(3) 查看 NAT 表：#show ip nat translations，分析结果

我们使用的锐捷交换机版本型号可能有差异，所以使用了#show ip nat translations 还是一片空白：

```
21-RSR20-2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
21-RSR20-2#
```

查询资料，我们可以通过#show ip nat static 看到地址转换的情况：

```
21-RSR20-2(config)#show ip nat static
192.168.1.5 200.1.1.80 permit-inside
192.168.1.6 200.1.1.81 permit-inside
21-RSR20-2(config)#
```

从上表可以看出内网地址：

192.168.1.5 转换为 200.1.1.80；

192.168.1.6 转换为 200.1.1.81。

(4) 捕获数据包，结合 (2) 和 (3) 分析 Telnet 登录时的地址转换情况

在地址为 192.168.1.6 的主机上抓取到的数据包是：

No.	Time	Source	Destination	Protocol	Length	Info
16	1.623881	100.1.1.2	200.1.1.81	TCP	66	1296 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0
17	1.658529	200.1.1.81	100.1.1.2	TCP	66	23 → 1296 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
18	1.658608	100.1.1.2	200.1.1.81	TCP	54	1296 → 23 [ACK] Seq=1 Ack=1 Win=65536 Len=0
54	6.207741	200.1.1.81	100.1.1.2	TELNET	75	Telnet Data ...
55	6.208502	100.1.1.2	200.1.1.81	TELNET	60	Telnet Data ...
56	6.241964	200.1.1.81	100.1.1.2	TELNET	62	Telnet Data ...
57	6.242047	100.1.1.2	200.1.1.81	TELNET	78	Telnet Data ...
58	6.281511	200.1.1.81	100.1.1.2	TELNET	89	Telnet Data ...
60	6.477600	100.1.1.2	200.1.1.81	TCP	54	1296 → 23 [ACK] Seq=31 Ack=65 Win=65536 Len=0
70	21.274299	100.1.1.2	200.1.1.81	TELNET	117	Telnet Data ...
71	21.335863	200.1.1.81	100.1.1.2	TELNET	209	Telnet Data ...
72	21.335960	100.1.1.2	200.1.1.81	TELNET	93	Telnet Data ...
73	21.576447	200.1.1.81	100.1.1.2	TCP	60	23 → 1296 [ACK] Seq=220 Ack=133 Win=65536 Len=0
74	21.576510	100.1.1.2	200.1.1.81	TELNET	489	Telnet Data ...

1) Telnet 登录，首先是与服务器端建立 TCP 连接，从抓取的数据包来看，建立连接的方式是典型的 TCP



三次握手协议:

No.	Time	Source	Destination	Protocol	Length	Info
16	1.623881	100.1.1.2	200.1.1.81	TCP	66	1296 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0
17	1.658529	200.1.1.81	100.1.1.2	TCP	66	23 → 1296 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=0
18	1.658608	100.1.1.2	200.1.1.81	TCP	54	1296 → 23 [ACK] Seq=1 Ack=1 Win=65536 Len=0

而且这里就出现了地址转换，我们配置的静态路由是这样的

```
#ip nat inside source static 192.168.1.5 200.1.1.80
#ip nat inside source static 192.168.1.6 200.1.1.81
```

服务器的地址原本是 192.168.1.6，但是经过 NAT 地址转换之后，地址变成了 200.1.1.81，可见通过 NAT 可以实现外网对内网的访问。

2) 然后是身份确认，TCP 连接建立之后，主机和服务器交换信息，通过 TELNET 协议，包括服务器端的配置信息，主机的应答，是否需要登录，等等

观察其中一个数据包:

75	21.688329	200.1.1.81	100.1.1.2	TELNET	245	Telnet Data ...
76	21.887917	100.1.1.2	200.1.1.81	TCP	54	1296 → 23 [ACK] Seq=
Type: IPv4 (0x0800)						
▶ Internet Protocol Version 4, Src: 200.1.1.81, Dst: 100.1.1.2						
▶ Transmission Control Protocol, Src Port: 23, Dst Port: 1296, Seq: 220, Ack: 568, Len: 191						
▼ Telnet						
0000	44 33 4c 0e b6 ad 58 69	6c 27 bf a6 08 00 45 00	D3L...Xi l'...E.			
0010	00 e7 02 f4 40 00 7e 06	ca c7 c8 01 01 51 64 01	...@~...Qd.			
0020	01 02 00 17 05 10 de 9a	87 24 cc fe c4 5d 50 18	...\$...P.			
0030	00 fe da a3 00 00 ff fa	25 02 0f 00 04 ff f0 0d	...%...server			
0040	0a 54 65 6c 6e 65 74 20	73 65 72 76 65 72 20 63	.Telnet server c			
0050	6f 75 6c 64 20 6e 6f 74	20 6c 6f 67 20 79 6f 75	ould not log you			
0060	20 69 6e 20 75 73 69 6e	67 20 4e 54 4c 4d 20 61	in usin g NTLM a			
0070	75 74 68 65 6e 74 69 63	61 74 69 6f 6e 2e 0d 0a	uthentic ation...			
0080	59 6f 75 72 20 70 61 73	73 77 6f 72 64 20 6d 61	Your pas sword ma			
0090	79 20 68 61 76 65 20 65	78 70 69 72 65 64 2e 0d	y have e xpired..			
00a0	0a 4c 6f 67 69 6e 20 75	73 69 6e 67 20 75 73 65	.Login u sing use			
00b0	72 6e 61 6d 65 20 61 6e	64 20 70 61 73 73 77 6f	rname an d passwo			
00c0	72 64 0d 0a 0d 0a 57 65	6c 63 6f 6d 65 20 74 6f	rd...We lcome to			
00d0	20 4d 69 63 72 6f 73 6f	66 74 20 54 65 6c 6e 65	Microso ft Telne			
00e0	74 20 53 65 72 76 69 63	65 20 0d 0a 0a 0d 6c 6f	t Servic elo			
00f0	67 69 6e 3a 20		gin:			

可以看到，报文里面出现了登录提示，并要求输入用户名和密码。

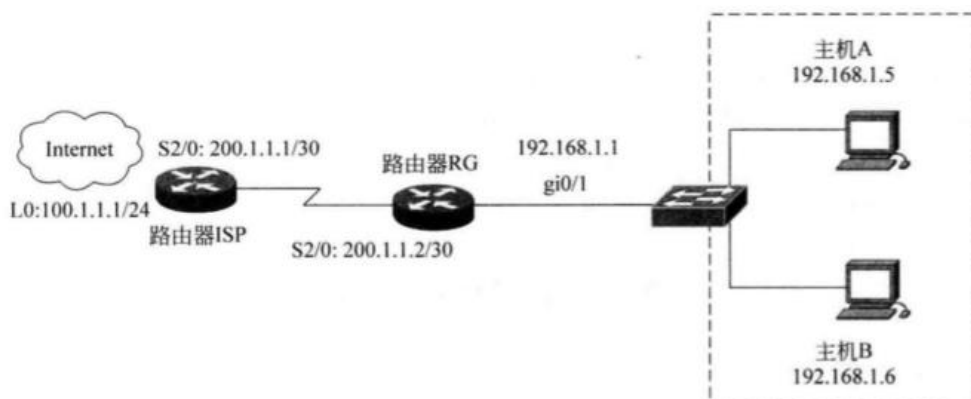
【实验思考】

采用地址转换后，不能再进行端对端 IP 的追踪。也就是说，不能再经过网路地址转换使用 ping 和 tracert 命令，另外一些 IP 对 IP 的程序也可能无法正常运行。请思考原因。

答：因为进行 NAT 转换之后，外网到达内网的地址会发生变化，ping 和 tracert 追踪是根据 ip 地址来进行的，当 ip 变化之后，就无法准确追踪了。

二、动态 NAT 实验

拓扑图:





【实验步骤】

在做实验之前，按照老师提示，我们没有使用 Internet，而是把 100.1.1.2 当做主机，而 100.1.1.1 是路由器 ISP 的端口地址。

步骤 1:

在主机 100.1.1.2 上建立用户名和口令

验证整个网络的连通性，查看 NAT 表

```
22-RSR20-2(config)#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
22-RSR20-2(config)#
```

因为上次配置完毕之后，我们把它清空了，所以现在仍然是空的

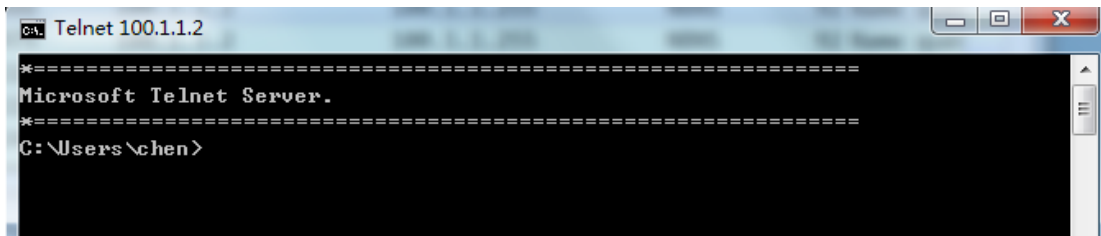
然后我们按照步骤配置好交换机和路由器之后

(1) 用 2 台主机 Telnet 登录远程主机 100.1.1.2，测试 NAT 的转换。用步骤一建立的用户名和密码登录，是否可以登录？

C:\telnet 100.1.1.2

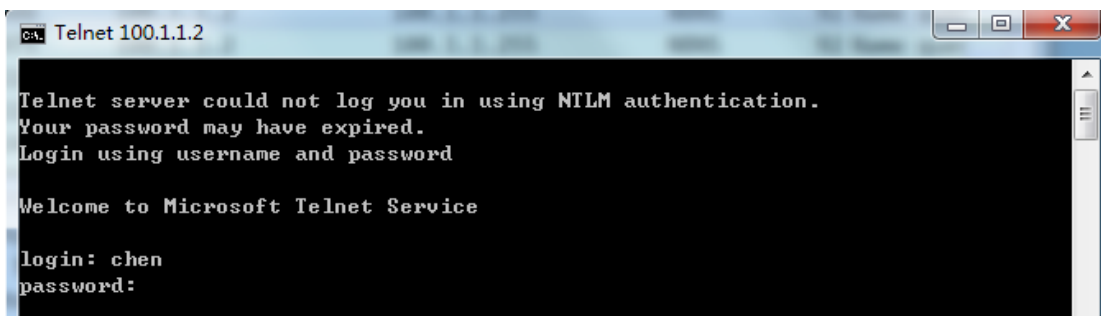
我们设置主机的用户名为 chen，密码 123456，发现可以两台都可以登录并查看远程主机的目录

主机 A 登录远程主机：



```
CA: Telnet 100.1.1.2

*****
Microsoft Telnet Server.
*****
C:\Users\chen>
```

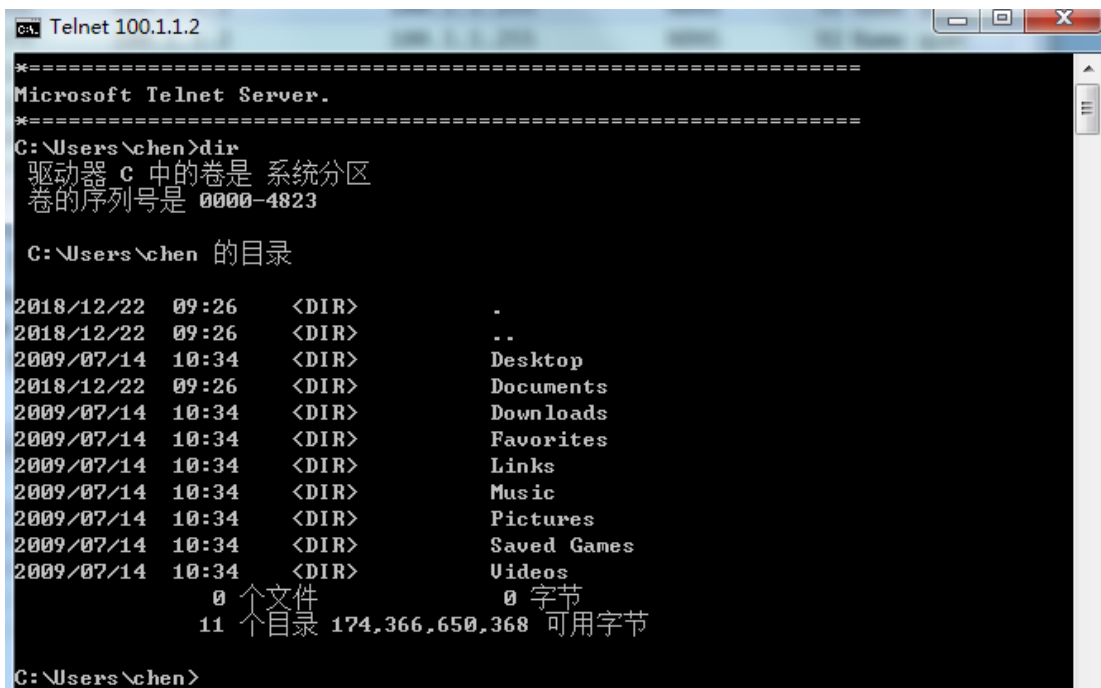


```
CA: Telnet 100.1.1.2

Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

Welcome to Microsoft Telnet Service

login: chen
password:
```



```
CA: Telnet 100.1.1.2

*****
Microsoft Telnet Server.
*****
C:\Users\chen>dir
驱动器 c 中的卷是 系统分区
卷的序列号是 0000-4823

C:\Users\chen 的目录

2018/12/22 09:26 <DIR> .
2018/12/22 09:26 <DIR> ..
2009/07/14 10:34 <DIR> Desktop
2018/12/22 09:26 <DIR> Documents
2009/07/14 10:34 <DIR> Downloads
2009/07/14 10:34 <DIR> Favorites
2009/07/14 10:34 <DIR> Links
2009/07/14 10:34 <DIR> Music
2009/07/14 10:34 <DIR> Pictures
2009/07/14 10:34 <DIR> Saved Games
2009/07/14 10:34 <DIR> Videos
0 个文件 0 字节
11 个目录 174,366,650,368 可用字节

C:\Users\chen>
```

主机 B 登录远程主机：



```
Microsoft Telnet Server.  
C:\Users\chen>
```

```
Telnet 100.1.1.2  
  
Telnet server could not log you in using NTLM authentication.  
Your password may have expired.  
Login using username and password  
  
Welcome to Microsoft Telnet Service  
  
login: chen  
password:
```

```
Telnet 100.1.1.2  
  
Microsoft Telnet Server.  
C:\Users\chen>dir  
驱动器 c 中的卷是 系统分区  
卷的序列号是 0000-4823  
  
C:\Users\chen 的目录  
  
2018/12/22 09:26 <DIR> .  
2018/12/22 09:26 <DIR> ..  
2009/07/14 10:34 <DIR> Desktop  
2018/12/22 09:26 <DIR> Documents  
2009/07/14 10:34 <DIR> Downloads  
2009/07/14 10:34 <DIR> Favorites  
2009/07/14 10:34 <DIR> Links  
2009/07/14 10:34 <DIR> Music  
2009/07/14 10:34 <DIR> Pictures  
2009/07/14 10:34 <DIR> Saved Games  
2009/07/14 10:34 <DIR> Videos  
0 个文件 0 字节  
11 个目录 174,366,650,368 可用字节  
  
C:\Users\chen>
```

(2) 查看地址翻译的过程: #debug ip nat 分析结果

同上, 无法 debug ip nat

(3) 查看 NAT 表: #show ip nat translations, 分析结果

```
22-RSR20-2(config)#show ip nat translations  
Pro Inside global      Inside local      Outside local      Outside global  
tcp 200.1.1.205:1084    192.168.1.5:1084  100.1.1.2:23      100.1.1.2:23  
22-RSR20-2(config)#
```

我们在路由器 2 上面输入 show ip nat translations 命令得出上面的结果, 可以发现: 内部地址为



192.168.1.5, 而且内部地址也被映射成 200.1.1.205;

外部地址为 100.1.1.2。

(4) 捕获数据包, 分析 Telnet 时的地址转换情况

在 ip 地址为 192.168.1.6 的主机上抓取数据包

8	12.134878	192.168.1.6	100.1.1.2	TCP	66	1079 → 23 [SYN] Seq=
9	12.174947	100.1.1.2	192.168.1.6	TCP	66	23 → 1079 [SYN, ACK]
10	12.175007	192.168.1.6	100.1.1.2	TCP	54	1079 → 23 [ACK] Seq=
14	16.735142	100.1.1.2	192.168.1.6	TELNET	75	Telnet Data ...
15	16.735977	192.168.1.6	100.1.1.2	TELNET	84	Telnet Data ...
16	16.778900	100.1.1.2	192.168.1.6	TELNET	97	Telnet Data ...
17	16.974750	192.168.1.6	100.1.1.2	TCP	54	1079 → 23 [ACK] Seq=
19	18.393317	192.168.1.6	100.1.1.2	TELNET	117	Telnet Data ...
20	18.452700	100.1.1.2	192.168.1.6	TELNET	209	Telnet Data ...
21	18.452809	192.168.1.6	100.1.1.2	TELNET	93	Telnet Data ...
23	18.694252	100.1.1.2	192.168.1.6	TCP	60	23 → 1079 [ACK] Seq=
24	18.694300	192.168.1.6	100.1.1.2	TELNET	485	Telnet Data ...
25	18.809373	100.1.1.2	192.168.1.6	TELNET	245	Telnet Data ...

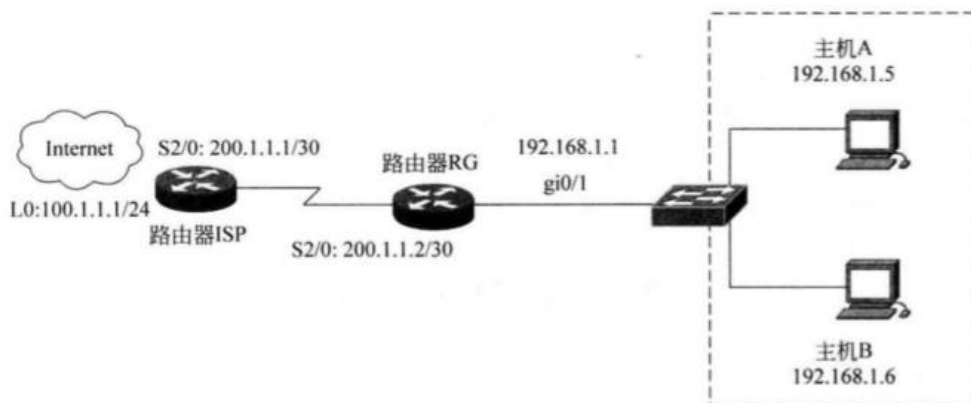
图中我们可以看出, 地址转换没有体现出来, 一直是 192.168.1.6 的主机和 100.1.1.2 的远程主机进行信息交流。

但是 100.1.1.2 主机的数据包能够经过 NAT 之后传入客户端, 说明还是进行了地址转换的, 但是没有在主机上体现出来。

三、端口 NAT 实验

【实验步骤】

拓扑图同 2



除了配置静态转换之外, 其他的配置都和实验 2 相同, 仍然是把 100.1.1.2 当做远程主机
我们按照步骤配置好交换机和路由器之后

(1) 用 2 台主机 Telnet 登录远程主机 100.1.1.2, 测试 NAT 的转换。

C:\telnet 100.1.1.2

用步骤一建立的用户名和密码登录, 是否可以登录?

我们尝试 telnet 远程主机, 可以登录。



```
Ca. Telnet 100.1.1.2

=====
Microsoft Telnet Server.
=====

C:\Users\chen>dir
驱动器 C 中的卷是 系统分区
卷的序列号是 0000-4823

C:\Users\chen 的目录

2018/12/22 09:26 <DIR> .
2018/12/22 09:26 <DIR> ..
2009/07/14 10:34 <DIR> Desktop
2018/12/22 09:26 <DIR> Documents
2009/07/14 10:34 <DIR> Downloads
2009/07/14 10:34 <DIR> Favorites
2009/07/14 10:34 <DIR> Links
2009/07/14 10:34 <DIR> Music
2009/07/14 10:34 <DIR> Pictures
2009/07/14 10:34 <DIR> Saved Games
2009/07/14 10:34 <DIR> Videos
0 个文件 0 字节
11 个目录 174,364,114,944 可用字节

C:\Users\chen>
```

(2) 查看地址翻译的过程: #debug ip nat 分析结果

依然无法 debug ip nat

(3) 查看 NAT 表: #show ip nat translations, 分析结果

```
22-RSR20-2(config)#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 200.1.1.2:1099     192.168.1.6:1099  100.1.1.2:23      100.1.1.2:23
22-RSR20-2(config)#
```

NAT 表和实验 9-2 的不同, 主机地址为 192.168.1.6 经过地址 PAT 复用转化为 200.1.1.2, 然后再和远程的 100.1.1.2 做数据交换。

(4) 捕获数据包, 分析 Telnet 时的地址转换情况

23	11.204967	192.168.1.6	100.1.1.2	TCP	66	1097 → 23 [SYN] Seq=
24	11.240551	100.1.1.2	192.168.1.6	TCP	66	23 → 1097 [SYN, ACK]
25	11.240630	192.168.1.6	100.1.1.2	TCP	54	1097 → 23 [ACK] Seq=
31	15.792479	100.1.1.2	192.168.1.6	TELNET	75	Telnet Data ...
32	15.793321	192.168.1.6	100.1.1.2	TELNET	57	Telnet Data ...
33	15.826772	100.1.1.2	192.168.1.6	TELNET	62	Telnet Data ...
34	15.826857	192.168.1.6	100.1.1.2	TELNET	81	Telnet Data ...
35	15.870306	100.1.1.2	192.168.1.6	TELNET	89	Telnet Data ...
36	16.072416	192.168.1.6	100.1.1.2	TCP	54	1097 → 23 [ACK] Seq=
41	17.742225	192.168.1.6	100.1.1.2	TELNET	156	Telnet Data ...
42	17.808958	100.1.1.2	192.168.1.6	TELNET	209	Telnet Data ...
43	17.809962	192.168.1.6	100.1.1.2	TELNET	485	Telnet Data ...
44	17.921593	100.1.1.2	192.168.1.6	TELNET	245	Telnet Data ...

抓取到的包和实验 2 类似, 并没有捕捉到 192.168.1.6 转化为 200.1.1.2 地址, 但可以分析的是数据包一定通过了 PAT 运行复用同一外网 IP 然后传输, 所以一定是经过了地址转换的。

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
16308073	刘渤	100
16308161	邹紫婧	100
16308091	彭肖文	100
16308015	陈瑞佳	100

【交实验报告】

上传实验报告：<ftp://222.200.181.161/>

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！