



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。

| | | | | | |
|------|-----------------|----------|--------|-----------------|----|
| 院系 | 计算机学院 | 班 级 | 1 班+保密 | 组长 | 马岱 |
| 学号 | <u>22336180</u> | | | <u>22336090</u> | |
| 姓名 | <u>马岱</u> | | | <u>黄集瑞</u> | |
| 实验分工 | | | | | |
| 姓名 | | 分工 | | 在本次中的占比 | |
| 马岱 | | 合作完成本次实验 | | <u>50%</u> | |
| 黄集瑞 | | 合作完成本次实验 | | <u>50%</u> | |

【实验题目】网络地址转换实验。

【实验目的】

1. 了解静态地址转换、动态地址转换和端口地址转换的区别。
2. 掌握静态地址转换、动态地址转换和端口地址转换。

【实验内容】

完成教材 P319 【习题 7】

(1) 按照如图 9-17 所示拓扑结构利用动态网络地址转换实现局域网访问 Internet。

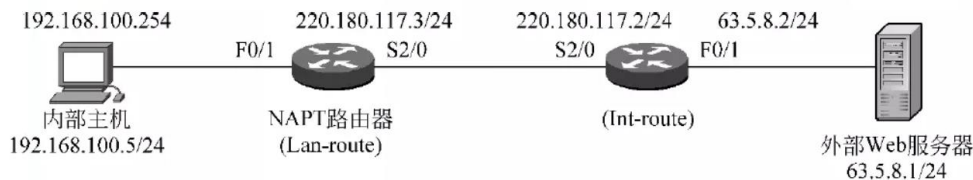


图 9-17 第 7 题(1)拓扑结构

(2) 按照如图 9-18 所示拓扑结构利用网络地址转换实现外网主机访问内网服务器。

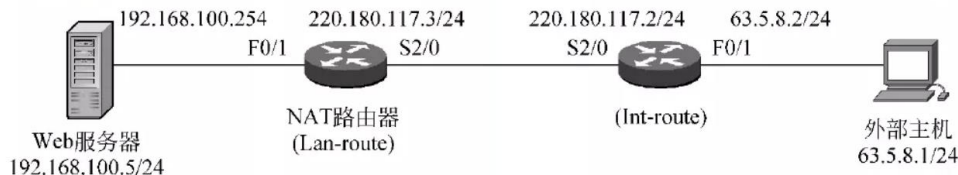


图 9-18 第 7 题(2)拓扑结构

【实验记录】

重要信息需给出截图，注意实验步骤的前后对比。

1. 局域网访问 Internet 可以用动态地址转换或端口地址转换完成
2. 用主机模拟 Web 服务器、FTP 服务器
3. 记录 NAT 转换表
#show ip nat translations
4. 用 Wireshark 进行数据包捕获，分析地址转换情况

【实验步骤】

在本次实验中，我们利用动态地址池分配完成任务一，然后使用静态地址转换完成任务二，以下是详细的配置过程：



● 任务一：

(1) 按照拓扑图上的标示，配置 PC1 和 PC2 的 IP 地址、子网掩码、网关，具体配置如下：



我们根据上面的拓扑图，分别将主机和服务器的 IP 地址配置成 192.168.100.254 以及 63.5.8.1；同时将网关分别设置成第一跳路由器的 IP 地址为 192.168.100.5 以及 63.5.8.2

(2) 按照以上拓扑图，分别在 Lan 路由以及 Int 路由处配置端口的 IP 地址具体配置过程如下：

🌈 Lan-route:

```
14-RSR20-1(config)#220.180.117.5 220.180.117.100 netmask 255.255.255.0
14-RSR20-1(config)#ip nat inside source list 1 pool nat-208
14-RSR20-1(config)#interface gigabitethernet 0/1
14-RSR20-1(config-if-GigabitEthernet 0/1)#2.168.100.5 255.255.255.0
14-RSR20-1(config-if-GigabitEthernet 0/1)#ip nat inside
14-RSR20-1(config-if-GigabitEthernet 0/1)#exit
14-RSR20-1(config)#interface serial 2/0
14-RSR20-1(config-if-Serial 2/0)#ip address 220.180.117.3 255.255.255.0
14-RSR20-1(config-if-Serial 2/0)#ip nat outside
14-RSR20-1(config-if-Serial 2/0)#access-list 1 permit 192.168.100.0 0.0.0.255
14-RSR20-1(config)#access-list 1 permit 192.168.100.0 0.0.0.255
failed, for the entry is existed or the sequence number has been allocated!
14-RSR20-1(config)#
```

此处为 Lan 路由的配置，我们在该路由器上配置动态网络地址转换，首先配置一个 NAT 地址池，指定了公网 IP 地址范围为 220.180.117.5 到 220.180.117.100，并且子网掩码是 255.255.255.0。这个地址池将用来为内网设备提供公共 IP 地址。接下来配置了 NAT 路由器让来自内网的流量使用上面配置的地址池来转换源地址，并通过访问控制列表（ACL）进行过滤，即所有通过 ACL 1 允许的内网设备都会使用 nat-208 地址池中的公网 IP 地址进行源地址转换。配置 GigabitEthernet 0/1 接口为内网接口，并标记为 ip nat inside。这个接口连接到 LAN，IP 地址是 192.168.100.5，并且子网掩码为 255.255.255.0。配置了 Serial 2/0 接口为外网接口，并标记为 ip nat outside。这个接口连接到 R2，公网 IP 地址是 220.180.117.3。ACL 1 用于允许从 192.168.100.0/24 的内网设备访问外网，指定了内网地址范围。



Int-route:

```
14-RSR20-2(config)#interface gigabitEthernet 0/1
14-RSR20-2(config-if-GigabitEthernet 0/1)#ip address
% Incomplete command.

14-RSR20-2(config-if-GigabitEthernet 0/1)#ip address 63.5.8.2 255.255.255.0
14-RSR20-2(config-if-GigabitEthernet 0/1)#no shutdown
14-RSR20-2(config-if-GigabitEthernet 0/1)#exit
14-RSR20-2(config)#interface serial 2/0
14-RSR20-2(config-if-Serial 2/0)#ip address 220.180.117.2 255.255.255.0
14-RSR20-2(config-if-Serial 2/0)#no shutdown
14-RSR20-2(config-if-Serial 2/0)#exit
```

此处为 Int 路由的配置，因为该路由器处于因特网中，且没有要求要做地址映射，所以不需要额外的处理。所以，先配置千兆以太网口 0/1，将其的地址配置为 63.5.8.2，子网掩码为 255.255.255.0，配置完毕后，设置其状态为 no shutdown 打开此端口；然后我们再配置路由串口 2/0 的 IP 地址为 220.180.117.2，子网掩码对应为 255.255.255.0；同样的，配置完成后，设置该端口的状态为 no shutdown 来保持连接。

(3) 配置结果如下所示：

Lan-route:

```
14-RSR20-1(config)#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)      Status
Protocol
Serial 2/0                220.180.117.3/24     no address            up
up
SIC-3G-WCDMA 3/0         no address           no address            up
down
GigabitEthernet 0/0      no address           no address            down
down
GigabitEthernet 0/1      192.168.100.5/24     no address            up
up
VLAN 1                   no address           no address            up
down

14-RSR20-1(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.100.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.100.5/32 is local host.
C    220.180.117.0/24 is directly connected, Serial 2/0
C    220.180.117.3/32 is local host.
14-RSR20-1(config)#■
```

可以看到，以上内容都按照我们所期望的进行配置。

```
14-RSR20-2(config)#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)      Statu
s
Serial 2/0                220.180.117.2/24     no address            up
up
Serial 3/0                no address           no address            down
down
GigabitEthernet 0/0      no address           no address            down
down
GigabitEthernet 0/1      63.5.8.2/24         no address            up
up
VLAN 1                   no address           no address            up
down
```

可以看到，以上内容都按照我们所期望的进行配置。

(4) 记录 NAT 转换表



由于在之后我们发现了这个错误，因此先在这里说明

```
14-RSR20-1(config)#ip route 0.0.0.0 0.0.0.0 serial2/0
```

在配置 R1 的最后，我们需要在 R1 上加上这么一条指令，表示 ip 地址最后都从 serial2/0 这个接口出去，若没有该条指令，则最终无法 ping 通主机。

```
14-RSR20-1(config)#ip route 0.0.0.0 0.0.0.0 serial2/0
14-RSR20-1(config)#show ip route
```

```
Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*  0.0.0.0/0 is directly connected, Serial 2/0
C   192.168.100.0/24 is directly connected, GigabitEthernet 0/1
C   192.168.100.5/32 is local host.
C   220.180.117.0/24 is directly connected, Serial 2/0
C   220.180.117.3/32 is local host.
```

可以看到加了该条指令之后，路由表中多了一项：S*，表示从该口通路。

我们发现，在没有 ping 之前，这个转换表中是没有显示任何条目的。

```
14-RSR20-1(config)#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
```

在 ping 之后，这个转换表便显示出了对应的条目：

```
C:\Users\D502>ping -S 192.168.100.254 63.5.8.1

正在 Ping 63.5.8.1 从 192.168.100.254 具有 32 字节的数据:
来自 63.5.8.1 的回复: 字节=32 时间=41ms TTL=126
来自 63.5.8.1 的回复: 字节=32 时间=39ms TTL=126
来自 63.5.8.1 的回复: 字节=32 时间=39ms TTL=126
来自 63.5.8.1 的回复: 字节=32 时间=40ms TTL=126

63.5.8.1 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 = 39ms, 最长 = 41ms, 平均 = 39ms
```

可以看到此时我们局域网内的主机已经 ping 通了处于互联网中的服务器（注意一定要在 Ping 的时候显示转换表条目，否则无法显示）

```
14-RSR20-1(config)#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp220.180.117.35:1    192.168.100.254:1  63.5.8.1           63.5.8.1
```

其中出现了 5 个条目，含义分别如下：

Pro: 代表的是协议类型，像这里展示的是 ICMP 协议，等会在 wireshark 的抓包中也有体现。

Inside Global: 指的是内网设备的**全局地址**，也就是内网主机在外网中的表现地址。这是由我们设置的 NAT 路由器从地址池中动态分配给内部设备的 IP 地址。

Inside Local: 指的是内网设备的**本地地址**，也就是内网主机在内网中的实际地址。

Outside Local: 指的是外部设备在内网主机看来显示的地址。通常是与外部设备交互时使用的一个私有 IP 地址。

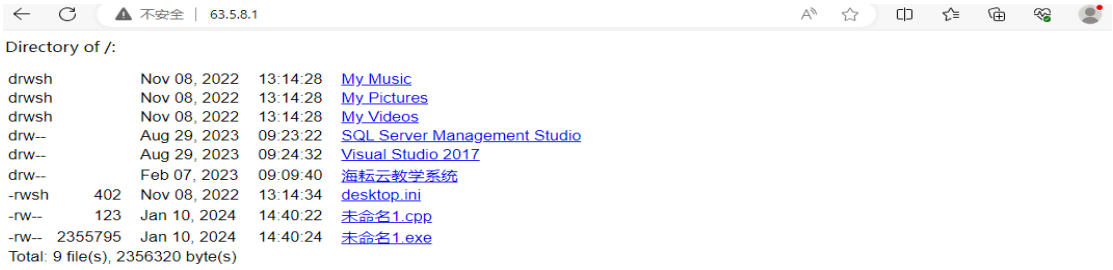
Outside Global: 指的是外部设备的**全局地址**，也就是外网主机的真实公网 IP 地址。

可以看到以上的地址都与我们的预期相符，至此任务一成功完成。

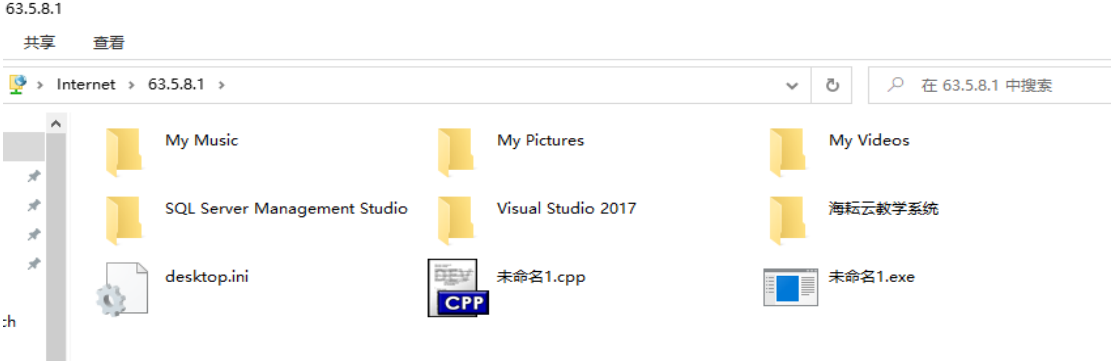


(5) 访问服务器结果

Web 服务器:



FTP 服务器:



可以看到两个服务器均能访问。

(6) Wireshark 抓包分析

客户端 ping 的抓包:

| Source | Destination | Protocol | Lengt | Info |
|-----------------|-----------------|----------|-------|---------------------|
| 192.168.100.254 | 63.5.8.1 | ICMP | 74 | Echo (ping) request |
| 63.5.8.1 | 192.168.100.254 | ICMP | 78 | Echo (ping) reply |
| 192.168.100.254 | 63.5.8.1 | ICMP | 74 | Echo (ping) request |
| 63.5.8.1 | 192.168.100.254 | ICMP | 78 | Echo (ping) reply |

可以看到, 此时我们由内网的 ip 地址 192.168.100.254 向外网中的服务器 ip 地址 63.5.8.1 进行 ping 操作, 采用的协议与之前看到的相同为 ICMP。

服务器端的抓包:

| Source | Destination | Protocol | Lengt | Info |
|----------------|----------------|----------|-------|---------------------|
| 220.180.117.35 | 63.5.8.1 | ICMP | 78 | Echo (ping) request |
| 63.5.8.1 | 220.180.117.35 | ICMP | 74 | Echo (ping) reply |
| 220.180.117.35 | 63.5.8.1 | ICMP | 78 | Echo (ping) request |
| 63.5.8.1 | 220.180.117.35 | ICMP | 74 | Echo (ping) reply |

可以看到, 在服务器这端看到的请求 ip 地址为 220.180.117.35, 也即上面显示的 Inside Local 的 ip 地址, 这就说明了此时的动态 ip 地址转换成功! 此时, 任务一已经顺利完成了。



● 任务二：

在任务二中，我们采用了静态路由地址转换来完成此任务。

- (1) 我们不需要对任务一的代码作出过多修改，只需要进行补充即可。由拓扑图可知，此时我们的服务器本身处于内网中，而处于互联网中的主机需要去访问该服务器，所以我们采用静态的地址转换以模拟真实环境，服务器在外网中的 ip 地址不应该经常变动。那么，我们需要将服务器在外网中的 ip 地址设置为一个不跟路由器端口相同的 ip 地址即可，具体配置过程如下所示：

```
14-RSR20-1(config)#ip nat inside source static 192.168.100.254 220.180.117.4
```

可以看到此时，我们将内网 ip 地址为 192.168.100.254 的服务器的外网地址设置为 220.180.117.4，那么位于外网的主机应该访问该转换地址，并且能够得到相应的应答。

- (2) 记录 NAT 转换表

同任务一，在我们没有进行 ping 操作时，该转换表中并没有存在任何条目，接下来，我们进行 ping 操作：

```
C:\Users\D502>ping -S 63.5.8.1 220.180.117.4

正在 Ping 220.180.117.4 从 63.5.8.1 具有 32 字节的数据:
来自 220.180.117.4 的回复: 字节=32 时间=38ms TTL=126
来自 220.180.117.4 的回复: 字节=32 时间=38ms TTL=126
来自 220.180.117.4 的回复: 字节=32 时间=40ms TTL=126
来自 220.180.117.4 的回复: 字节=32 时间=39ms TTL=126

220.180.117.4 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 = 38ms, 最长 = 40ms, 平均 = 38ms
```

可以看到我们访问的是服务器在外网中的 ip 地址，此时也是 ping 通了；同时，NAT 转换表中也增加了对应的条目

```
14-RSR20-1(config)#show ip nat translation
Pro Inside global      Inside local           Outside local          Outside global
icmp63.5.8.1:1         63.5.8.1:1            220.180.117.4        192.168.100.254
```

可以看到这些内容与我们的预期相一致。

- (3) 访问服务器结果



Web 服务器:

Ftp 服务器:

可以看到我们均访问成功。

(4) Wireshark 抓包分析

内网服务器:

| Source | Destination | Protocol | Lengt | Info |
|-----------------|-----------------|----------|-------|---------------------|
| 63.5.8.1 | 192.168.100.254 | ICMP | 78 | Echo (ping) request |
| 192.168.100.254 | 63.5.8.1 | ICMP | 74 | Echo (ping) reply |

可以看到, 虽然我们处于外网的主机访问的是服务器转换后的 ip 地址, 但是服务器位于内网中的真实地址收到了 ping 的包, 说明静态 ip 地址转换成功

外网主机:

| Source | Destination | Protocol | Lengt | Info |
|---------------|---------------|----------|-------|---------------------|
| 63.5.8.1 | 220.180.117.4 | ICMP | 74 | Echo (ping) request |
| 220.180.117.4 | 63.5.8.1 | ICMP | 78 | Echo (ping) reply |

可以看到, 我们的外网主机成功与服务器在外网的虚拟地址建立连接, 至此实验全部完成。