

实验 1 eNSP 基本操作及 NAT/NAPT 协议仿真实践报告

1. 路由器配置步骤重点

<R1> display current-configuration

[V200R003C00]

```
# sysname R1 //系统视图下命名 R1
# acl number 2001 //当前访问控制列表编号为 2001
    rule 5 permit source 20.1.1.0 0.0.0.255 //配置了一个规则 5 的 20.1.1.0 源 IP 网络地址,
    主机掩码为 0/0/0/255
# nat address-group 1 202.169.10.50 202.169.10.60 //配置了一个从 202.169.10.50~60 的 NAT 地
    址池
# interface GigabitEthernet0/0/0 //开始配置 0 号端口
    ip address 202.169.10.1 255.255.255.0 //设置端口 IP 地址和子网掩码
    arp-proxy enable //启动路由式 Proxy ARP 功能
    nat static global 202.169.10.5 inside 10.1.1.1 netmask 255.255.255.255 //静态 NAT, 在接口下将 10.1.1.1
    转换成 202.169.10.5 地址访问公网
    nat outbound 2001 address-group 1 no-pat //将访问控制列表与地址池关联, 设置静态分配
# interface GigabitEthernet0/0/1
    ip address 10.1.1.254 255.255.255.0 //设置端口 IP 地址和子网掩码
# interface GigabitEthernet0/0/2
    ip address 20.1.1.254 255.255.255.0 //设置端口 IP 地址和子网掩码
# interface NULL0 //设置伪接口, 防止环路
# ip route-static 0.0.0.0 0.0.0.0 202.169.10.2 //配置缺省路由, 减小路由表项规模, 所有数
    据包均通过 202.169.10.2 转发
# Return
```

<R2> display current-configuration

[V200R003C00]

```
# sysname R2
# snmp-agent local-engineid
    800007DB0300000000000000
    snmp-agent
# interface GigabitEthernet0/0/0 //开始配置 0 号端口
    ip address 202.169.10.2 255.255.255.0 //设置端口 IP 地址和子网掩码
# interface LoopBack0 //配置回环测试
    ip address 202.169.20.1 255.255.255.0 //设置端口 IP 地址和子网掩码
# return
```

2. 实验结果

Capturing from Standard input - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	202.169.10.50	202.169.10.2	ICMP	Echo (ping) request (id=0x3)
2	0.015000	202.169.10.2	202.169.10.50	ICMP	Echo (ping) reply (id=0x3)
3	1.046000	202.169.10.51	202.169.10.2	ICMP	Echo (ping) request (id=0x3)
4	1.062000	202.169.10.2	202.169.10.51	ICMP	Echo (ping) reply (id=0x3)
5	2.093000	202.169.10.52	202.169.10.2	ICMP	Echo (ping) request (id=0x3)
6	2.093000	202.169.10.2	202.169.10.52	ICMP	Echo (ping) reply (id=0x3)
7	3.125000	202.169.10.53	202.169.10.2	ICMP	Echo (ping) request (id=0x3)
8	3.140000	202.169.10.2	202.169.10.53	ICMP	Echo (ping) reply (id=0x3)
9	4.187000	202.169.10.54	202.169.10.2	ICMP	Echo (ping) request (id=0x4)
10	4.203000	202.169.10.2	202.169.10.54	ICMP	Echo (ping) reply (id=0x4)
11	1035.265000	HuaweiTe_51:1e:de	Broadcast	ARP	who has 202.169.10.2? Tell
12	1035.281000	HuaweiTe_bb:08:26	HuaweiTe_51:1e:de	ARP	202.169.10.2 is at 00:e0:fc:
13	1037.640000	HuaweiTe_bb:08:26	Broadcast	ARP	who has 202.169.10.51? Tell
14	1037.640000	HuaweiTe_51:1e:de	HuaweiTe_bb:08:26	ARP	202.169.10.51 is at 00:e0:fc:
15	1038.625000	HuaweiTe_bb:08:26	Broadcast	ARP	who has 202.169.10.52? Tell

Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: HuaweiTe_51:1e:de (00:e0:fc:51:1e:de), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 e0 fc 51 1e de 08 06 00 01  .....Q.....
0010  08 00 06 04 00 01 00 e0 fc 51 1e de ca a9 0a 01  .....Q.....
0020  00 00 00 00 00 00 00 ca a9 0a 02 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Standard input: <live capture in progres... Packets: 22 Displayed: 22 Marked: 0 Profile: Default

NAT 地址池静态分配

Capturing from Standard input - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
40	1653.593000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
41	1654.625000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
42	1654.640000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
43	1655.671000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
44	1655.687000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
45	1668.562000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
46	1668.578000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
47	1669.609000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
48	1669.625000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
49	1670.656000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
50	1670.656000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
51	1671.703000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
52	1671.703000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)
53	1672.734000	202.169.10.59	202.169.10.2	ICMP	Echo (ping) request (id=0x0)
54	1672.750000	202.169.10.2	202.169.10.59	ICMP	Echo (ping) reply (id=0x0)

Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: HuaweiTe_bb:08:26 (00:e0:fc:bb:08:26), Dst: HuaweiTe_51:1e:de (00:e0:fc:51:1e:de)

Internet Protocol, Src: 202.169.10.2 (202.169.10.2), Dst: 202.169.10.53 (202.169.10.53)

Internet Control Message Protocol

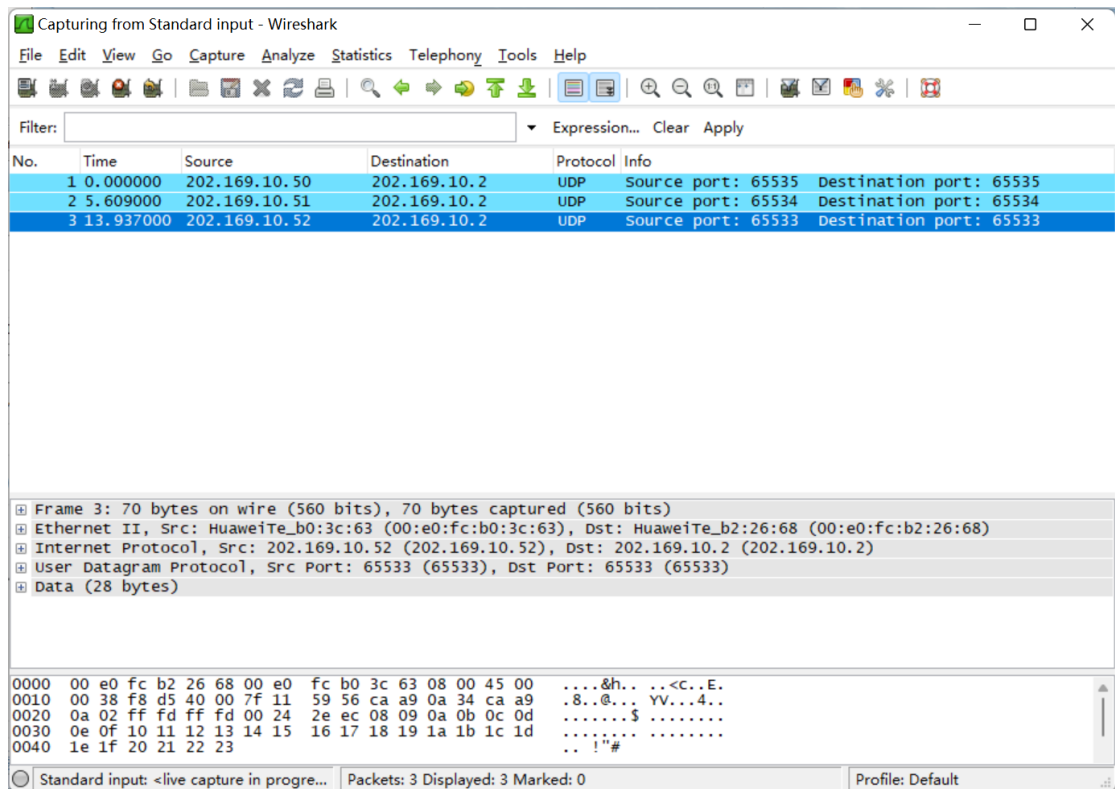
```

0000  00 e0 fc 51 1e de 00 e0 fc bb 08 26 08 00 45 00  ...Q....&...E.
0010  00 3c 00 0c 40 00 ff 01 d2 2a ca a9 0a 02 ca a9  .<.@...*.....
0020  0a 35 00 00 4f 05 3f 75 00 04 08 09 0a 0b 0c 0d  .5..O.?u.....
0030  0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d  .....
0040  1e 1f 20 21 22 23 24 25 26 27  .....!#$%&'

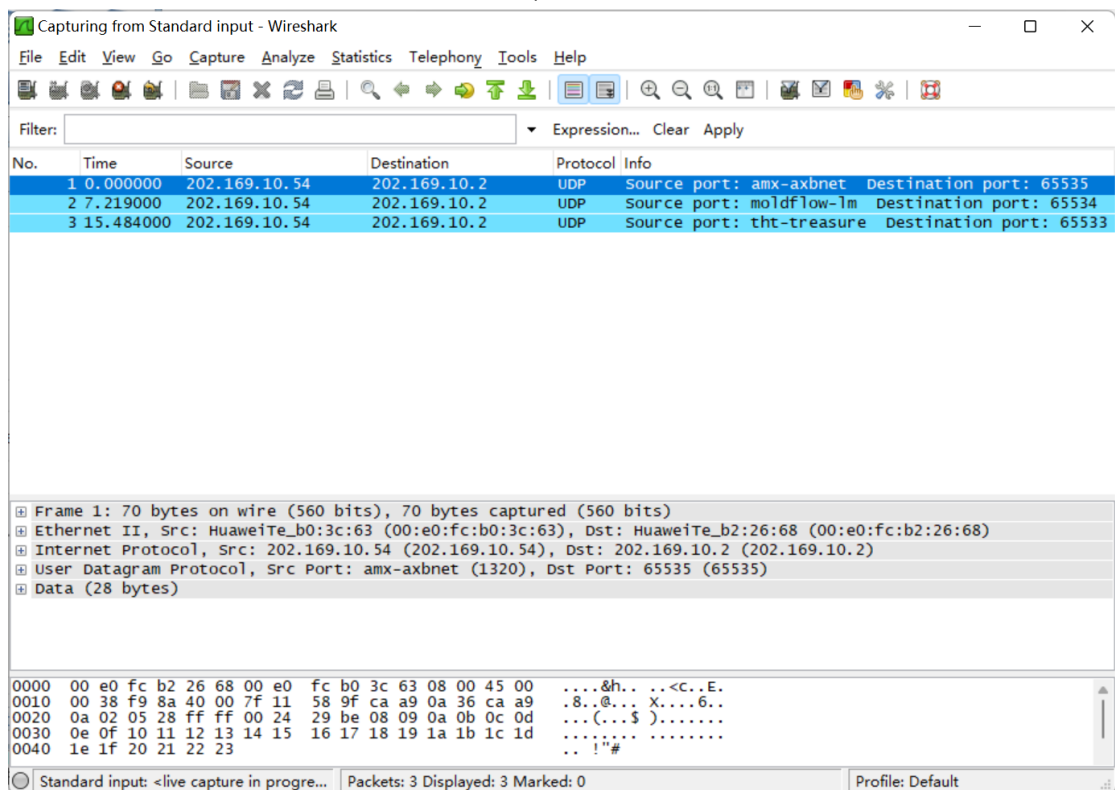
```

Standard input: <live capture in progres... Packets: 54 Displayed: 54 Marked: 0 Profile: Default

NAPT 地址池动态分配



No-pat 状态



Pat 状态

3. 结果分析

首先比较 no-pat 与 pat 状态。No-pat 状态中，使用不同端口号向路由器 R2

发送 UDP 数据报，可以看出对于不同的端口号，R1 都分配了新的 IP 地址，Ping 三次获得了三个不同的 IP 地址。接着我们将 R1 改为 pat 状态，继续用不同的端口号发送三次 UDP，可以发现 IP 地址已经复用，均为 202.169.10.54。

NAT 为网络地址转换，就是替换 IP 报文头部的地址信息。NAT 通常部署在一个组织的网络出口位置，通过将内部网络 IP 地址替换为出口的 IP 地址提供公网可达性和上层协议的连接能力，当私有网主机和公网主机通信的 IP 包经过 NAT 网关时，将 IP 包中的源 IP 或目的 IP 在私有 IP 和 NAT 的公共 IP 之间进行转换。实现是私有 IP 和 NAT 的公共 IP 之间的转换，那么，私有网中同时与公网进行通信的主机数量就受到 NAT 的公共 IP 地址数量的限制。NAT 本身的解决方法是对于较长时间不用的 IP 进行回收，重新分配。

NAPT 为网络地址端口转换，为了克服公共 IP 地址数量的限制，NAT 被进一步扩展到在进行 IP 地址转换的同时进行 Port 的转换，即 NAPT。它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。NAPT 的主要优势在于，能够使用一个全球有效 IP 地址获得通用性。主要缺点在于其通信仅限于 TCP 或 UDP。只要所有通信都采用 TCP 或 UDP，NAPT 就允许一台内部计算机访问多台外部计算机，并允许多台内部主机访问同一台外部计算机，相互之间不会发生冲突。

NAPT 与 NAT 的区别在于，NAPT 不仅转换 IP 包中的 IP 地址，还对 IP 包中 TCP 和 UDP 的端口号进行转换。这使得多台私有网主机利用 1 个 NAT 公共 IP 就可以同时和公网进行通信。正如实验中 NAT 从地址池中依次取出 202.169.10.50 至 202.169.10.60 之内的 IP 逐一分配，很快就会用完。而 NAPT 可以重复使用 202.169.10.59 地址，但是端口号却是不同的，将目的地址查找交给

传输层处理。