实验 1 eNSP 基本操作及 NAT/NAPT 协议仿真实践报告

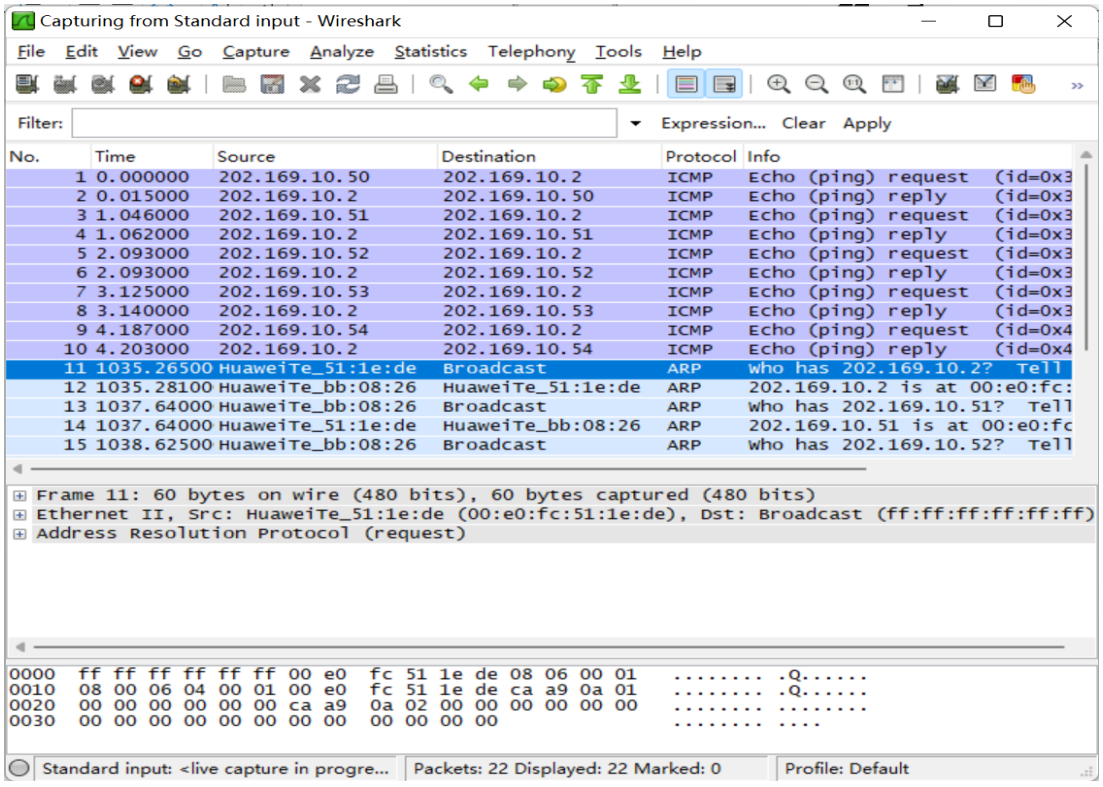
1. 路由器配置步骤重点

<R1> display current-configuration
[V200R003C00]

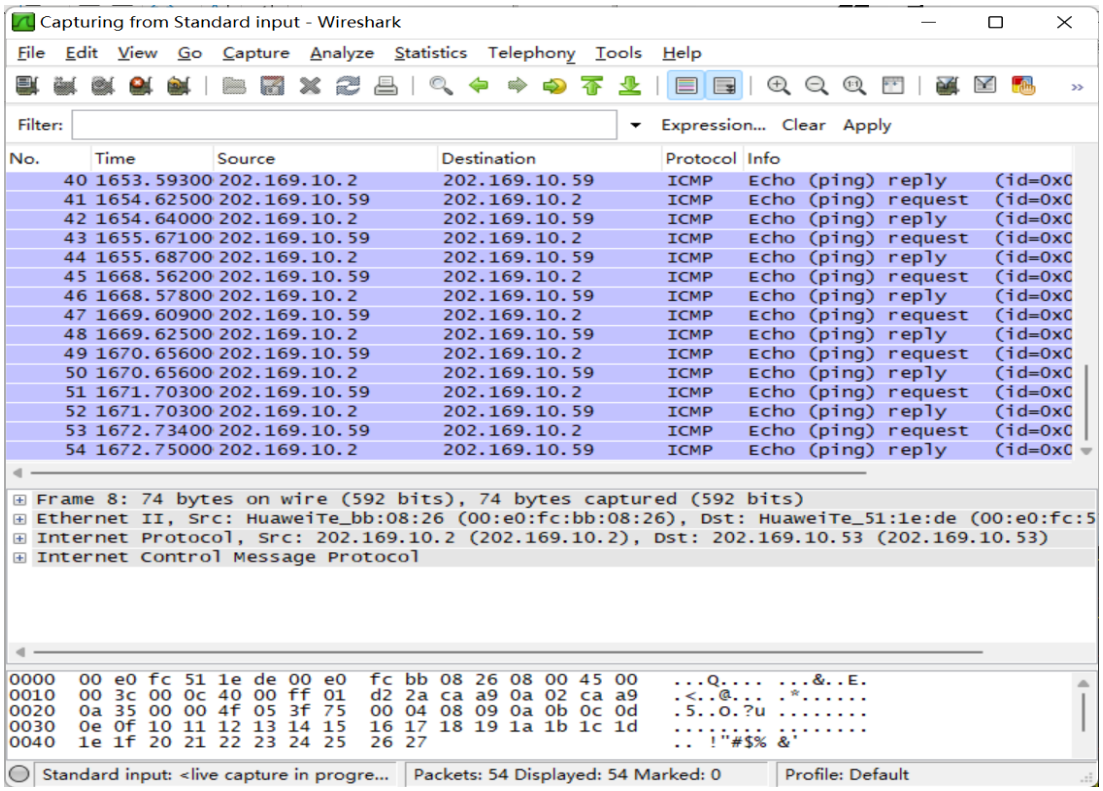
sysname R1 //系统视图下命名 R1
acl number 2001 //当前访问控制列表编号为 2001
rule 5 permit source 20.1.1.0 0.0.0.255 //配置了一个规则 5 的 20.1.1.0 源 IP 网络地址，主机掩码为 0/0/0/255
nat address-group 1 202.169.10.50 202.169.10.60 //配置了一个从 202.169.10.50~60 的 NAT 地址池
interface GigabitEthernet0/0/0 //开始配置 0 号端口
ip address 202.169.10.1 255.255.255.0 //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
800007DB03000000000000
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

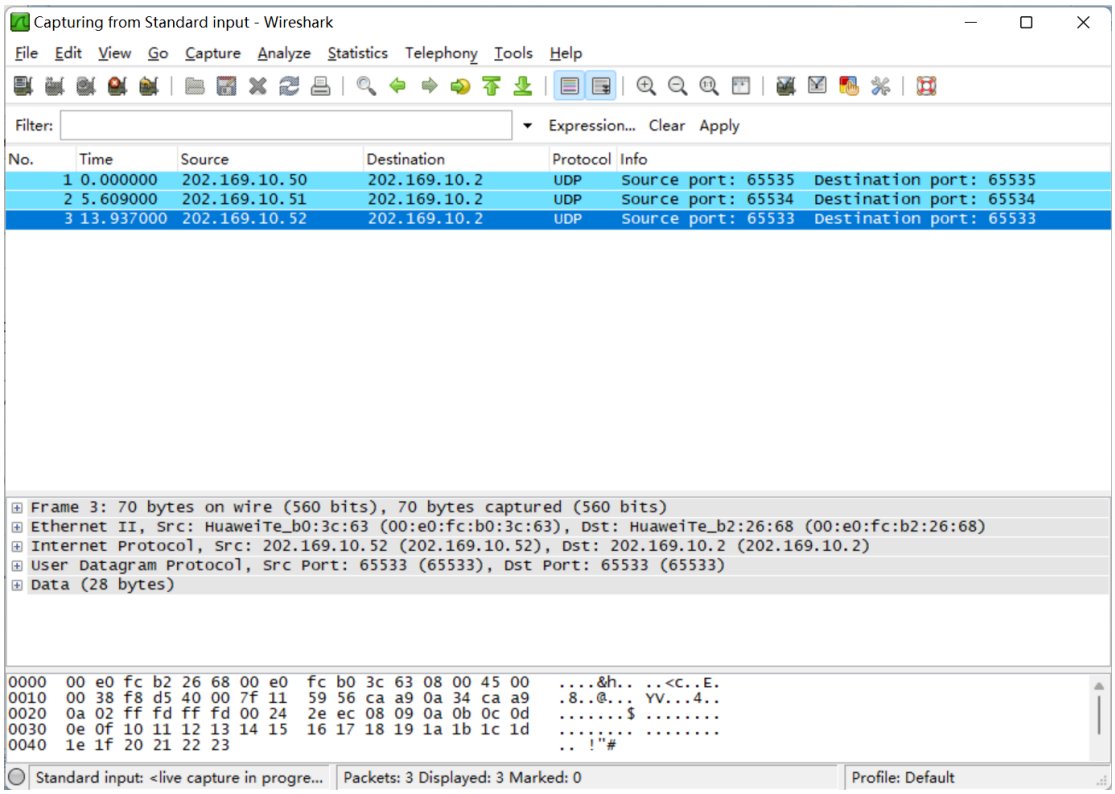
2. 实验结果



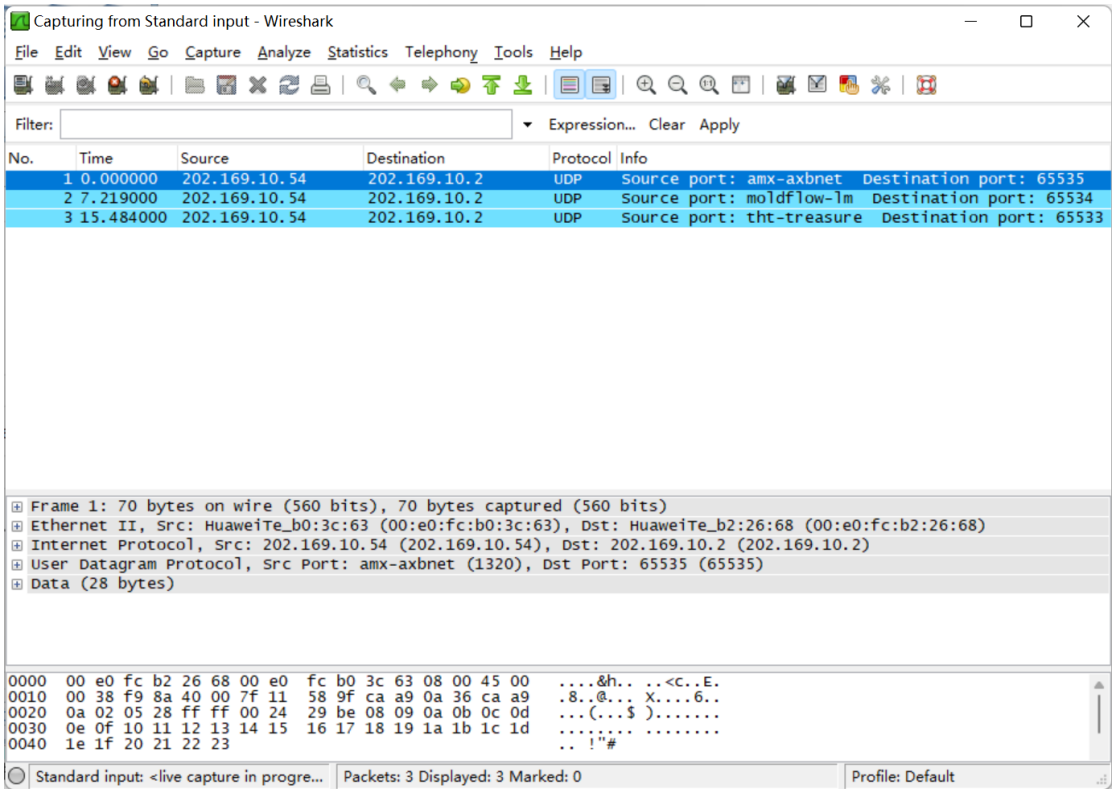
NAT 地址池静态分配



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，当私有网主机和公共网主机通信的 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，私有网中同时与公共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 就可以同时和公共网进行通信。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。