

## 互联阶段 - Internet 互联

### 一、实验目的

1. 学习互联组网
2. 学习 NAT，实现内网 PC 的外网访问

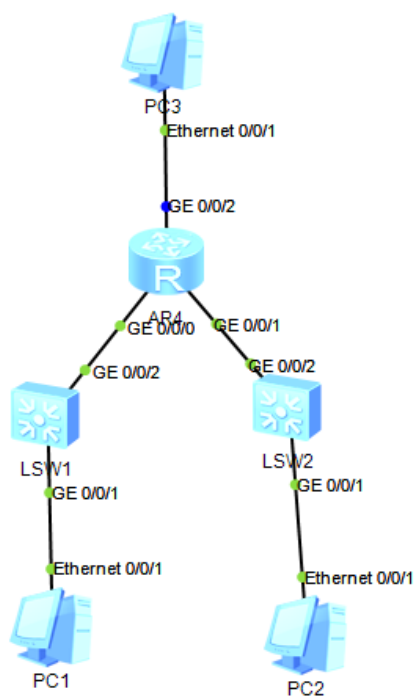
### 二、实验内容

1. 出口互联 (NAT)

### 三、实验步骤

#### 4.1 出口互联 (NAT)

网络拓扑



NATP 配置

```

acl number 2000
 rule 5 permit source 10.25.0.0 0.0.255.255
#
  
```

```
nat address-group 1 100.25.0.254 100.25.0.254
#
interface GigabitEthernet0/0/0
 ip address 10.25.10.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.25.20.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 100.25.0.1 255.255.0.0
 nat outbound 2000 address-group 1
```

## 1. 访问运营商路由器

The image shows two screenshots of a PC Simulator interface, labeled PC1 and PC2. Each window has a title bar and five tabs: 基础配置 (Basic Configuration), 命令行 (Command Line), 组播 (Multicast), UDP发包工具 (UDP Packet Tool), and 串口 (Serial Port). The 命令行 tab is active in both.

**PC1 Screenshot:**

```
PC>ping 100.25.0.2

Ping 100.25.0.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 100.25.0.2: bytes=32 seq=2 ttl=127 time=31 ms
From 100.25.0.2: bytes=32 seq=3 ttl=127 time=47 ms
From 100.25.0.2: bytes=32 seq=4 ttl=127 time=47 ms
From 100.25.0.2: bytes=32 seq=5 ttl=127 time=31 ms

--- 100.25.0.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/39/47 ms
```

**PC2 Screenshot:**

```
PC2>ping 100.25.0.2

Welcome to use PC Simulator!

Ping 100.25.0.2: 32 data bytes, Press Ctrl_C to break
From 100.25.0.2: bytes=32 seq=1 ttl=127 time=32 ms
From 100.25.0.2: bytes=32 seq=2 ttl=127 time=47 ms
From 100.25.0.2: bytes=32 seq=3 ttl=127 time=31 ms
From 100.25.0.2: bytes=32 seq=4 ttl=127 time=31 ms
From 100.25.0.2: bytes=32 seq=5 ttl=127 time=31 ms

--- 100.25.0.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 31/34/47 ms
```

## 2. PC3 抓包查看 NAT 转换后 IP 地址

1 0.000000	HuaweiTe_46:3b:29	Broadcast	ARP	60 Who has 100.25.0.2? Tell 100.25.0.1
2 0.000000	HuaweiTe_ff:63:b4	HuaweiTe_46:3b:29	ARP	60 100.25.0.2 is at 54:89:98:ff:63:b4
3 2.000000	100.25.0.254	100.25.0.2	ICMP	74 Echo (ping) request id=0x0128, seq=2/512, ttl=127 (reply in 4)
4 2.000000	100.25.0.2	100.25.0.254	ICMP	74 Echo (ping) reply id=0x0128, seq=2/512, ttl=128 (request in 3)
5 3.032000	100.25.0.254	100.25.0.2	ICMP	74 Echo (ping) request id=0x0228, seq=3/768, ttl=127 (reply in 6)
6 3.047000	100.25.0.2	100.25.0.254	ICMP	74 Echo (ping) reply id=0x0228, seq=3/768, ttl=128 (request in 5)
7 4.094000	100.25.0.254	100.25.0.2	ICMP	74 Echo (ping) request id=0x0328, seq=4/1024, ttl=127 (reply in 8)

可以发现内网地址被转换为 100.25.0.254

## 3. 查看路由器的 NAT Session 表项

```
<Huawei>dis nat session all
NAT Session Table Information:

Protocol      : ICMP(1)
SrcAddr Vpn   : 10.25.10.2
DestAddr Vpn  : 100.25.0.2
Type Code IcmpId : 0 8 10853
NAT-Info
  New SrcAddr  : 100.25.0.254
  New DestAddr : ----
  New IcmpId   : 10255

Protocol      : ICMP(1)
SrcAddr Vpn   : 10.25.20.2
DestAddr Vpn  : 100.25.0.2
Type Code IcmpId : 0 8 10856
NAT-Info
  New SrcAddr  : 100.25.0.254
  New DestAddr : ----
  New IcmpId   : 10256

Total : 2
```

可以发现 10.25.10.2 与 10.25.20.2 均被转换为 100.25.0.254

## 四、实验体会

### 4.1 出口互联 (NAT)

#### 1. NAT 的转发模型是怎样的？

NAT (Network Address Translation, 网络地址转换) 是一种将私有网络地址映射到公共网络地址的技术。其主要目的是允许多个设备通过一个公共 IP 地址访问外部网络，同时隐藏内部网络结构。NAT 的转发模型可以概括如下：

1. 地址映射：当内部网络设备向外部网络发起连接时，NAT 设备将私有 IP 地址转换为公共 IP 地址，同时修改数据包中的源端口号。
2. 端口转发：NAT 设备为每个连接创建一个映射条目，记录内部 IP 和端口与外部 IP 和端口的对应关系。这些条目保存在一个 NAT 表中。
3. 数据包处理：
  - 出站数据包：数据包从内部网络发送到外部网络时，NAT 设备修改源 IP 地址和源端口号，将其替换为公共 IP 地址和相应的端口号。
  - 入站数据包：数据包从外部网络返回时，NAT 设备根据 NAT 表中的映射条目，将目标 IP 地址和端口号还原为内部 IP 地址和端口号。

## 2. Session 表有哪几个关键 Key? 为什么一会就不见了?

NAT 的 Session 表（会话表）记录了当前活动连接的映射关系，其关键字段包括：

- 源 IP 地址：内部网络设备的 IP 地址。
- 源端口号：内部网络设备使用的端口号。
- 目标 IP 地址：外部网络设备的 IP 地址。
- 目标端口号：外部网络设备使用的端口号。
- 公共 IP 地址：NAT 设备使用的外部网络 IP 地址。
- 公共端口号：NAT 设备分配的端口号。
- 协议类型：如 TCP、UDP 等。

这些 Session 表条目通常会有一个超时机制。如果在一定时间内没有检测到任何流量，NAT 设备会删除该条目以释放资源。原因包括：

- 保持表的大小可控：防止 Session 表过大，占用过多的系统资源。
- 管理有限的端口资源：特别是在端口映射中，释放不再使用的端口号，以便为新连接提供服务。
- 安全性：超时机制有助于减少未及时关闭的会话可能带来的安全隐患。

## 3. ICMP 没有端口号，怎样实现 NAT 的?

ICMP (Internet Control Message Protocol, 互联网控制消息协议) 与 TCP 和 UDP 不同，没有端口号。实现 ICMP 的 NAT 时，主要通过以下方式：

- 标识符和序列号：ICMP 消息（如 ping 请求和响应）包含标识符和序列号字段，NAT 设备可以使用这些字段来唯一标识和跟踪 ICMP 会话。
- NAT 表条目：NAT 设备在处理 ICMP 报文时，会在 NAT 表中创建包含源 IP、目标 IP、标识符、序列号和协议类型（ICMP）的条目。
- 地址和标识符映射：
  - 出站 ICMP 报文：当内部设备发送 ICMP 请求时，NAT 设备修改源 IP 地址，同时可能修改标识符字段，以确保唯一性，并在 NAT 表中记录原始标识符和修改后的标识符的映射关系。
  - 入站 ICMP 报文：当外部设备响应 ICMP 请求时，NAT 设备根据 NAT 表中的条目，将目标 IP 地址和标识符还原为内部设备的 IP 地址和原始标识符。

## 遇见的问题及解决方案

### 1. AR 2220 无法启动

- 除 NAT 实验外 AR 2220 可由 Router 替代
- 解决方案：

#### 1. 关闭基于虚拟化的安全性：

```
bcdedit /set hypervisorlaunchtype off
```

## 2. 关闭内核 DMA 保护

BIOS -> Security -> Virtualization -> Kernel DMA  
Protection Disabled