

《计算机网络实验》实验报告

实验名称：子网划分和 NAT 配置

姓名：胡育玮

学号：171860574

邮箱：yeevee@qq.com

班级：17 级计算机科学与技术系 2 班

一、实验目的

- 1、了解 NAT 的功能和种类
- 2、了解 IPtable 的设置和作用

二、网络拓扑配置

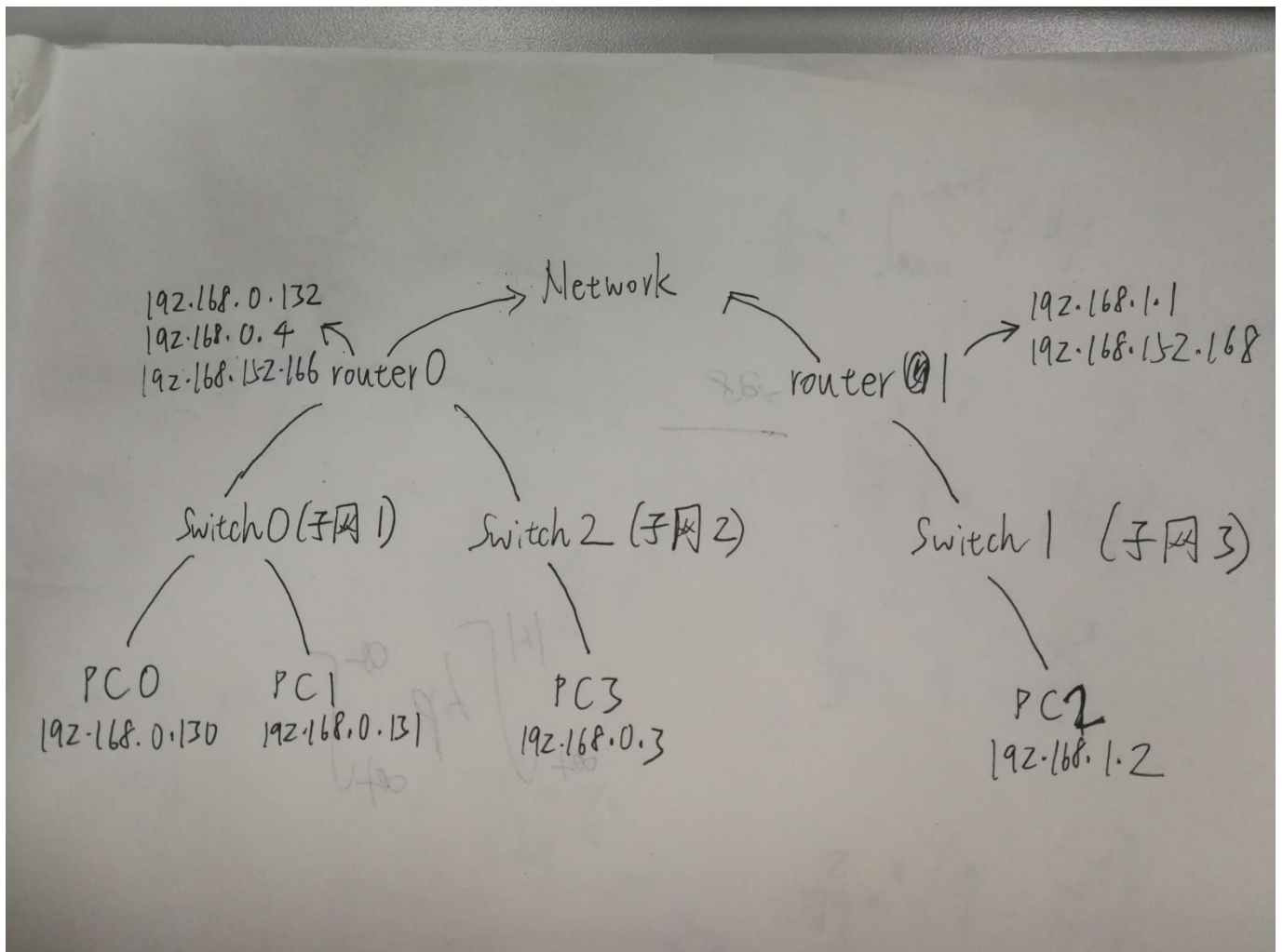
(1) 表格：

节点名	虚拟设备名	IP 地址	netmask
Router0	Ubuntu-32bit	ens33: 192.168.0.132	255.255.255.128
		ens38: 192.168.0.4	255.255.255.128
		ens39: 192.168.152.166	255.255.255.0
Router1	U-572	eth0: 192.168.1.1	255.255.255.0
		eth1: 192.168.152.168	255.255.255.0
PC0	UT-574-PC0	192.168.0.130	255.255.255.128
PC1	UT-575-PC1	192.168.0.131	255.255.255.128
PC2	UT-577-PC2	192.168.1.2	255.255.255.0
PC3	UT-578-PC3	192.168.0.3	255.255.255.128

其中，Router0 的 ens33 网卡与 PC0，PC1 构成子网 1，网段是 192.168.0.128/25，子网掩码是 255.255.255.128；Router0 的 ens38 网卡与 PC3 构成子网 2，网段是 192.168.0.0/25，其子网掩码是 255.255.255.128；Router1 与 PC2 构成子网 3，网段是 192.168.1.0/24，其子网掩码是 255.255.255.0。Router0 与 Router1 通过 VMware 的 NAT 网络互联。

这样划分子网使得子网 1 和子网 2 各自可以支持超过 100 台主机的 IP 地址分配，满足实验的要求。

绘图说明：



(3) 路由规则及网关的设置:

需要注意的是, 实验任务一共有 3 个, 分别是:

1. 配置 3 个子网,配置完后让 PC0, PC2, PC3 两两互 ping 能够 ping 通。
2. 设置 iptables 规则,内网设备可以通过 NAT 跟公网设备通信
3. 比较 1 和 2 的结果,并解释 NAT 所起到的作用。

以下的配置是针对实验任务 1 的,也即以下配置设置好后能使 3 个子网之间的主机互相 ping 通。

1. 对 2 个路由器 router0 和 router1:

Router0 :

① `sudo service network-manager stop` (关闭 DHCP 服务)

② `sudo ifconfig ens33 192.168.0.132 netmask 255.255.255.128`

`sudo ifconfig ens38 192.168.0.4 netmask 255.255.255.128` (设置 IP 地址和子网掩码)

(Router0 的第三张网卡的 IP 地址由 VMware 软件自动分配成 192.168.152.166)

③ `sudo ip route add 192.168.1.0/24 via 192.168.152.168` (设置路由规则)

- ④ `sudo su` （进入 root 用户态）
- ⑤ `echo 1 > /proc/sys/net/ipv4/ip_forward` （允许转发）
- ⑥ `exit` （退出 root 态）

Router1（U-571）:

- ① `sudo service network-manager stop` （关闭 DHCP 服务）
- ② `sudo ifconfig eth0 192.168.1.1 netmask 255.255.255.0` 设置 IP 地址和子网掩码）

（Router1 的第二张网卡的 IP 地址由 VMware 软件自动分配成 192.168.152.168）

- ③ `sudo ip route add 192.168.0.0/24 via 192.168.152.166` （设置路由规则）
- ④ `sudo su` （进入 root 用户态）
- ⑤ `echo 1 > /proc/sys/net/ipv4/ip_forward` （允许转发）
- ⑥ `exit` （退出 root 态）

2. 对普通主机：PC0 – PC3

PC0（UT-574-PC0）:

- ① `sudo ifconfig eth0 192.168.0.130 netmask 255.255.255.128` （设置 IP 地址和子网掩码）

② `sudo route add default gw 192.168.0.132`（设置网关地址）

PC1（UT-575-PC1）：

① `sudo ifconfig eth0 192.168.0.131 netmask 255.255.255.128`（设置 IP 地址和子网掩码）

② `sudo route add default gw 192.168.0.132`（设置网关地址）

PC3（UT-578-PC3）：

① `sudo ifconfig eth0 192.168.0.3 netmask 255.255.255.128`（设置 IP 地址和子网掩码）

② `sudo route add default gw 192.168.0.4`（设置网关地址）

PC2（UT-577-PC2）：

① `sudo ifconfig eth0 192.168.1.2 netmask 255.255.255.0`（设置 IP 地址和子网掩码）

② `sudo route add default gw 192.168.1.1`（设置网关地址）

执行完上述指令，便完成了路由规则的配置，全部 4 台主机（PC）和 2 台路由器之间能够互相 Ping 通。

三、NAT 命令设置

在模拟 router0 的虚拟机上使用 iptables 进行网络地址转换。实验中采用静态 NAT。

在 router0 上使用的 NAT 设置命令：

```
sudo iptables -t nat -A POSTROUTING -o ens39 -s 192.168.0.0/24 -j  
SNAT --to 192.168.152.166
```

上述命令将所有从 router0 的 ens39 网卡出发而去外网的，源地址为 192.168.0.0/24 的包的源地址转换为 192.168.152.166，实现了**静态地址转换**功能。此时，从子网 1 和子网 2 出发前往外网的 ICMP 包的源地址将在经过网关时被更改。

四、数据包截图和协议报文分析

(1) 任务 1：未在 router0 上设置 IPtable，没有开启 NAT，需要实现 PC0，PC2，PC3 两两互 ping：

PC0（192.168.0.130） ping PC3（192.168.0.3）：

```

64 bytes from 192.168.0.3: icmp_req=39 ttl=63 time=0.718 ms
64 bytes from 192.168.0.3: icmp_req=40 ttl=63 time=0.914 ms
64 bytes from 192.168.0.3: icmp_req=41 ttl=63 time=0.812 ms
64 bytes from 192.168.0.3: icmp_req=42 ttl=63 time=0.584 ms
64 bytes from 192.168.0.3: icmp_req=43 ttl=63 time=0.720 ms
64 bytes from 192.168.0.3: icmp_req=44 ttl=63 time=0.565 ms
64 bytes from 192.168.0.3: icmp_req=45 ttl=63 time=0.506 ms
64 bytes from 192.168.0.3: icmp_req=46 ttl=63 time=0.825 ms
64 bytes from 192.168.0.3: icmp_req=47 ttl=63 time=1.79 ms
64 bytes from 192.168.0.3: icmp_req=48 ttl=63 time=0.720 ms
64 bytes from 192.168.0.3: icmp_req=49 ttl=63 time=0.732 ms

```

192.168.0.130	192.168.0.3	ICMP	98 Echo (ping) request	id=0x0460, seq=35/8960, ttl=64 (reply in 373)
192.168.0.3	192.168.0.130	ICMP	98 Echo (ping) reply	id=0x0460, seq=35/8960, ttl=63 (request in 372)

PC0 (192.168.0.130) ping PC2 (192.168.1.2):

```

64 bytes from 192.168.1.2: icmp_req=9 ttl=62 time=0.889 ms
64 bytes from 192.168.1.2: icmp_req=10 ttl=62 time=1.21 ms
64 bytes from 192.168.1.2: icmp_req=11 ttl=62 time=1.72 ms
64 bytes from 192.168.1.2: icmp_req=12 ttl=62 time=0.923 ms
64 bytes from 192.168.1.2: icmp_req=13 ttl=62 time=1.39 ms
64 bytes from 192.168.1.2: icmp_req=14 ttl=62 time=1.05 ms
64 bytes from 192.168.1.2: icmp_req=15 ttl=62 time=1.40 ms

```

192.168.0.130	192.168.1.2	ICMP	98 Echo (ping) request	id=0x0469, seq=13/3328, ttl=64 (reply in 11)
192.168.1.2	192.168.0.130	ICMP	98 Echo (ping) reply	id=0x0469, seq=13/3328, ttl=62 (request in 10)

PC2 (192.168.1.2) ping PC3 (192.168.0.3):

```

64 bytes from 192.168.0.3: icmp_req=53 ttl=62 time=1.10 ms
64 bytes from 192.168.0.3: icmp_req=54 ttl=62 time=0.929 ms
64 bytes from 192.168.0.3: icmp_req=55 ttl=62 time=1.00 ms
64 bytes from 192.168.0.3: icmp_req=56 ttl=62 time=1.23 ms

```

192.168.0.3	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x045b, seq=55/14080, ttl=64 (request in 7)
192.168.1.2	192.168.0.3	ICMP	98 Echo (ping) request	id=0x045b, seq=56/14336, ttl=62 (reply in 10)

可见 ICMP 包的目的地和源地址都是 PC0 和 PC3 的本来
的地址。

(2) 任务 2: 设置 iptables 规则, 内网设备可以通过 NAT 跟
公网设备通信。设置完成之后, 让 PC0, PC2, PC3 两两

互 ping。

需要说明的是，为了达到 NAT 的效果，在 Router0 设置好 IPtable 之前应将 router1 先前设置的转发规则清空：

```
sudo ip route del 192.168.0.0/24 via 192.168.152.166
```

这之后 PC2 无法 ping 通子网 1 和子网 2 的主机：

```
user@ubuntu:~$ ping 192.168.0.130
PING 192.168.0.130 (192.168.0.130) 56(84) bytes of data.
^C
--- 192.168.0.130 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1009ms
user@ubuntu:~$ _
```

PC0 也无法 ping 通子网 3 的主机 PC2：

```
user@ubuntu:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2015ms
```

然后设置好 IPtable，之后尝试用子网 1 和子网 2 中的主机 ping PC2，然后在 Router1 上抓包：

PC0（192.168.0.130） ping PC2（192.168.1.2）：

```
64 bytes from 192.168.1.2: icmp_req=20 ttl=62 time=0.919 ms
64 bytes from 192.168.1.2: icmp_req=21 ttl=62 time=3.13 ms
64 bytes from 192.168.1.2: icmp_req=22 ttl=62 time=0.947 ms
64 bytes from 192.168.1.2: icmp_req=23 ttl=62 time=1.24 ms
```

192.168.1.2	192.168.152.166	ICMP	98	Echo (ping) reply	id=0x046e, seq=22/5632, ttl=63
192.168.152.166	192.168.1.2	ICMP	98	Echo (ping) request	id=0x046e, seq=23/5888, ttl=63
192.168.1.2	192.168.152.166	ICMP	98	Echo (ping) reply	id=0x046e, seq=23/5888, ttl=63
192.168.152.166	192.168.1.2	ICMP	98	Echo (ping) request	id=0x046e, seq=24/6144, ttl=63

可见 NAT 开始起作用，从 PC0 到 PC2 的 ICMP request 的源地址变为设置好的 192.168.152.166，而不是 PC0 本来的

IP 地址。

PC3 (192.168.0.3) ping PC2 (192.168.1.2):

```
64 bytes from 192.168.1.2: icmp_req=10 ttl=62 time=1.21 ms
64 bytes from 192.168.1.2: icmp_req=11 ttl=62 time=1.88 ms
64 bytes from 192.168.1.2: icmp_req=12 ttl=62 time=1.21 ms
64 bytes from 192.168.1.2: icmp_req=13 ttl=62 time=0.947 ms
```

192.168.152.166	192.168.1.2	ICMP	98	Echo (ping) request	id=0x045c, seq=12/3072, ttl=63
192.168.1.2	192.168.152.166	ICMP	98	Echo (ping) reply	id=0x045c, seq=12/3072, ttl=63
192.168.152.166	192.168.1.2	ICMP	98	Echo (ping) request	id=0x045c, seq=13/3328, ttl=63
192.168.1.2	192.168.152.166	ICMP	98	Echo (ping) reply	id=0x045c, seq=13/3328, ttl=63

结果与上面一样。

PC0 (192.168.0.130) ping PC3 (192.168.0.3): 在 router0 上抓包:

```
64 bytes from 192.168.0.3: icmp_req=4 ttl=63 time=0.717 ms
64 bytes from 192.168.0.3: icmp_req=5 ttl=63 time=0.771 ms
64 bytes from 192.168.0.3: icmp_req=6 ttl=63 time=0.708 ms
64 bytes from 192.168.0.3: icmp_req=7 ttl=63 time=0.673 ms
64 bytes from 192.168.0.3: icmp_req=8 ttl=63 time=0.552 ms
```

192.168.0.130	192.168.0.3	ICMP	98	Echo (ping) request	id=0x0471, seq=3/768, ttl=63 (reply in 6)
192.168.0.3	192.168.0.130	ICMP	98	Echo (ping) reply	id=0x0471, seq=3/768, ttl=64 (request in 5)
192.168.0.130	192.168.0.3	ICMP	98	Echo (ping) request	id=0x0471, seq=4/1024, ttl=63 (reply in 8)
192.168.0.3	192.168.0.130	ICMP	98	Echo (ping) reply	id=0x0471, seq=4/1024, ttl=64 (request in 7)

可见由于 PC0 和 PC3 之间互相 PING 不需要访问外网，互相 ping 的包没有经过 router0 的连到外网的 ens39 网卡，故设置的 NAT 没有起作用，PC0 发送的 ICMP 的源地址不变，仍为 PC0 自己的地址。

PC2 (192.168.1.2) ping PC3 (192.168.0.3):

```
user@ubuntu:~$ ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
^C
--- 192.168.0.3 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms
```

此时 PC2 无法 ping 通 PC3.

由此可见，NAT 可以在内网访问外网时进行 IP 地址的转换，起到 IP 地址隐藏的作用，同时不影响内网的通信。