Network Lab Kevin Neumann & Alain C. Mendy

**Lab Report 7**

1.
- **Inside local address**—The IP address assigned to a host on the inside network as visible from inside
the network.

•**Inside global address**—A legitimate IP address assigned by the NIC or service provider that represents one
or more inside local IP addresses to the outside world.

•**Outside local address**—The IP address of an outside host as it appears to the inside network. Not necessarily
a legitimate address, it is allocated from an address space routable on the inside.

•**Outside global address**—The IP address assigned to a host on the outside network by the host owner. The
address is allocated from a globally routable address or network space.

2. PC3 and router 4 can be reached from the public network over the outside address beginning with
200.0.0 because router 2 has a NAT table which converts these addresses to the correct inside addresses.
PC1 and router 1 on the other hand cannot be pinged from PC4 or from PC3 and router 4 because a
network boundary would be crossed with no corresponding NAT table to facilitate the addressing of the
host inside the private network.

3. Ping sent from PC4 to PC3 using address 200.0.0.2:

```
 pings from PC3 succeed
pings from router2 succeed
ping from PC4 to 10.0.1.2 fails
ping from PC4 to 200.0.0.2 succeeds
```

## Exercise 1(c)

1. From PC1 it was possible to ping router 1 since they are on the same subnet. From PC1 it was also
possible to ping PC4. This was possible because PC2 masqueraded the address of PC1 as coming from inside
the public network.
The same goes for pings originating from router1.
2. All telnet sessions were successful but PC2 was able to observe the telnet packets of only telnet sessions
with PC4. It was observed that IP masquerading had occurred on PC2's eth1 link, meaning it told PC4 that
the telnet sessions were coming from 128.143.136.22 even though they weren't. No masquerading occurred on PC2's eth0 link.
3. See file

4. When the PC receives a packet which gets masqueraded, it puts an entry in its NAT table listing the
source address and the masqueraded address. When the answer returns, based on the originating address,
the PC just has to look up the corresponding entry and undo the masquerading to send the packet to the
right host on the private network.

5. Steps taken:

1. Receives packet from inside the network.
2. Puts an entry in the NAT table with the original source address aand the masquerade source address .
3. Changes the headers of the packet accordingly and sends the packet to its destination.
4. Upon receipt of reply, it checks the destination and source addresses of the reply against its NAT table.
5. It changes the destination address in the packet headers to match the original address as listed in the
NAT table.
6. It sends the reply to the correct host.

## Exercise 1(d)

From PC4 to PC2, IP addresses are as usual in the headers only and not to be found in the data payload.
From PC3 to PC2 however, the IP addresses are also included in the payload

Non-masqueraded IP addresses of source and destination are encapsulated in the FTP data, to ensure that
the packets find their way.