Prof. Dr. Christian Schindelhauer
Shyamala.VS, Asha Nagendra, Said Lobo
Freiburg, 25.11.2009

# Practical Exercises
# Communication Systems (Rechnernetze II)
# Network Address Translation and ICMP

Form groups of 3-5 students depending on the number of laptops. From each group exactly one laptop should acts as a router. Among remaining laptops in the group at least one should be behind[1] the router. and at least one should be outside[2] from this network.

**EXERCISE 1**

**On the router side:**

- ✔ Assign ip address to 192.168.x.m
- ✔ Create a virtual interface using *vconfig*. For eg. "vconfig add eth1 10"
- ✔ Assign ip address to this virtual interface. For eg. "ifconfig eth1.10 192.168.y.n". Here the main difference should be noticed is x-->y in ip address. But m and n doesn't matter.

*Now you do the NATting:*

- ✔ Activate/Enable IP forwarding in the kernel using:
  *echo "1" > /proc/sys/net/ipv4/ip_forward* (Note: this command works only as a root).
- ✔ You can check this by "*sysctl -p*"
- ✔ Read iptables manual (*man iptables*) before executing the following commands.
- ✔ *iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE*
  (Note: Here you should replace eth1 with eth0 if you have ethernet interface named eth0)
- ✔ *iptables -A FORWARD -i eth1.k -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT*
  (Note: here eth1.k is virtual interface which you've just created)
- ✔ *iptables -A FORWARD -i eth1 -o eth1.k -j ACCEPT.*

**On the laptop behind the router:**

- ✔ Assign an ip address as 192.168.x.__ (Note that this ip and the router's ip are now in the same domain)
- ✔ Set the default gateway of this laptop to the router. This can be done by
  *sudo route add default gw* (ip address of the router)

**On the laptop external to the network:**

- ✔ Assign ip address to 192.168.y.__ (Note that this ip and the ip address of router's virtual interface looks similar)

- ➔ Now check whether external network can be reachable from one of the laptop behind the router.
- ➔ Open Wireshark on your laptop and look at the packets. What do you observe?

---

[1]The network whose address to be translated for secure communication.
[2]The network which can access the router but not the network behind the router.

**EXERCISE 2**

Configure the MTU in laptop(behind the router) to 900, the router should change the MTU to 500 on the out-going interface. Try to ping outside network and analyse the generated traffic with wireshark. Try to ping with paket size 1400 and analyze the generated traffic again. How many packets would arrive in outside network if your laptop hidden behind a NAT.

- ✔ *ifconfig eth1 mtu 900 (On laptop behind the router)*
- ✔ *ifconfig eth1.k mtu 500 (On router laptop)*

**EXERCISE 3**

Try to ping a neighbour in the same domain with TTL of ”1” and after that try to ping an ip from completely different domain with same TTL. Observe the generated traffic with wireshark. You should now try to produce an ICMP error packet with ”Destination unreachable”. Check in wireshark the field ”type” and ”code” of an ICMP packet. Try to produce two ICMP error packets with ”Destination unreachable” and different ”code” field. Explain the value in the code field.
*(Hint: for TTL=1, ping xxx.xxx.xxx.xxx -t 1)*