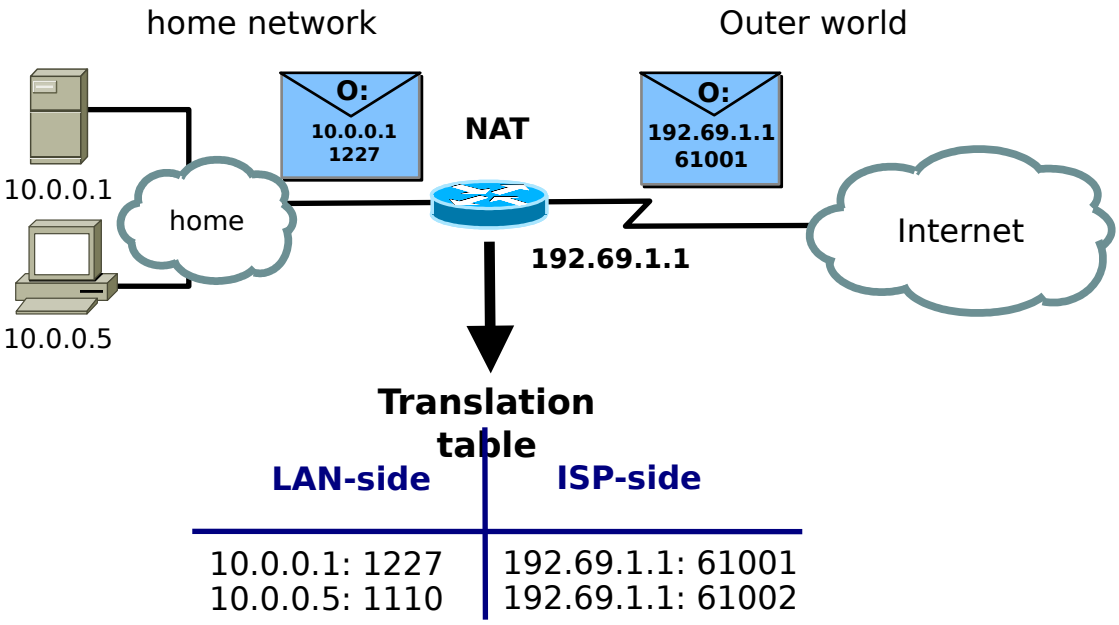
Lab#5: Network Address and Port Translation

You can read Kurose 4.4.2.

1. Intro

Network Address and Port Translation (NAPT, though mostly wrongly called NAT) replaces the source address and source port of UDP and TCP outgoing traffic by others using the translator's public address. Such translation data is stored in a table in memory so the process can be reversed when data is flowing back so it can be delivered to the real sender every time. The picture below shows an example of it.



Exercise#1. We are given the following data to configure our NAT device:

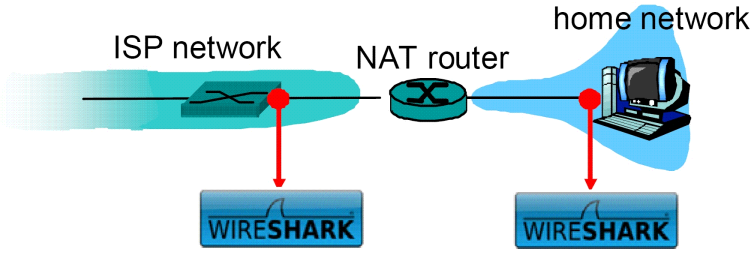
Public IP address:	158.42.180.1
Network mask:	255.255.255.0
Gateway:	158.42.181.250
DNS1:	158.42.249.8
DNS2:	158.42.1.8

a) Once these values are entered, the NAT device reports an invalid IP address for the gateway. Why is that?
b) If both IP addresses are correct, what do we need to change to fix the error?

c) Is it ok to have a DNS server located outside of our network? Why?

2. Traffic analysis

In this section we are going to see the packets that go through a NAT device. For doing that a simultaneous capture on both interfaces of the NAT device is needed. This may be tricky to achieve, so we will use some canned captures of LAN-side traffic in the following files HTTP_LAN_1, HTTP_LAN_2, FTP_LAN_1, SSH_LAN_1, that will be doubled with the version on the ISP_side too.



Exercise#2. Open file HTTP_LAN_1 and answer the following questions:

1. What is the client's IP address? What is the web server's address?
2. How many TCP connections are made?
3. Find the segment containing GET request "GET / HTTP/1.1". What are source and destination ports?
4. What time is received "HTTP 200 OK" response from server? What are the source and destination IP addresses of the datagram? And the source and destination port numbers?
5. What ports are used for the second TCP connection?

Exercise#3. Now let's see the capture of the same traffic on the other side, contained in file HTTP_ISP_1. Please note that time is not accurately synchronized with previous capture.

1. Again, find the first GET request that was sent in previous capture at time 1.338012. What is the time for this same event in this capture in file HTTP_ISP_1? What are IP soruce and destination addresses? What are the source and destination port numbers? Which ones are different from previous capture?
2. What is the public address of NAT router?
3. Does any field of HTTP GET request have been changed? What about changes on the IP header? What these changes are for?
4. Within file HTTP_ISP_1, when does arrive the server's response "HTTP 200 OK"? What are IP source and destination addresses? Are these the same as previous exercise?

Exercise#4. Fill-in the table below with the data gathered from the two previous captures for up to three TCP connections.

LAN-side		ISP-side	
Source IP address	Source Port	Destination IP address	Destination Port

Check destination addresses too.

Exercise#5. In the exercises above we have seen port numbers have not been changed, despite the use of NAT. This is a possibility whenever there are no previous entries on the translation table with that numbers. The following program has been created to force exactly that condition (creating different requests with the same source port number). The same program can be run on two different computers on the LAN-side to force router to have to at least change one of them.

```
import java.net.*;
import java.io.*;

class TCPClient {
public static void main(String args[]) throws UnknownHostException, IOException {

   String mi_IP =  "192.168.1.2";
   Socket s = new Socket("www.redes.upv.es",80, InetAddress.getByName(my_IP), 40000);
   PrintWriter esc= new PrintWriter(s.getOutputStream(), true);
   esc.println("GET / HTTP/1.1");
   esc.println("Host: www.redes.upv.es");
   esc.println();
   while(true);
}}
```

For each computer, the variable my_IP will have the proper value. When this program runs on two different computers of the same LAN, the router will there is already an entry in the translation table using that source port when second one arrives in the router. This will cause the router to have to translate the source port number of the second connection.

Open file HTTP_LAN_2 with Wireshark, containing the traffic created by the computers attached

to the LAN-side of the router running the program above.

1. What is the client's IP address? What is the address of the web server?
2. What are source and destination ports?

Now open file HTTP_ISP_2. This will show you the traffic of the previous program on the ISP side.

1. What is the source port assigned by the router for each connection?
2. How can you tell which is the connection that got its source port replaced? (hint: compare the IP identification field on HTTP_LAN_2 capture and here).

Based on the above questions, fill-in the following table:

LAN-side		ISP-side	
Source IP address	Source Port	Destination IP address	Destination Port

Exercise#6. Have a look to files FTP_LAN_1 and FTP_ISP_1. You will notice that some of the content of the messages is changed by the NAT router. This did not happen before.

1. What are the ftp client and ftp server addresses?
2. How many TCP connections are made? Source and destination port of each one. Why is there more than one?
3. Look at the datagram transmitted on the LAN-side at 4.307125s. Compare that with the one on the ISP-side. Have a look at the segments closing the connection on both sides. What is happening? (ask your teacher if you cannot figure it out).

3. Servers on the LAN-side

NAT enables outgoing connections to leave the LAN and reach the intended servers on the Internet. But it does not work when the server is on the LAN side and the clients are elsewhere on the Internet. This is because incoming traffic will not find an existing entry on the translation table on arrival (as these connections are initiated from the ISP-side) and these datagrams will be silently dropped by the NAT router.

To enable incoming connections from the ISP-side to reach a server on the LAN-side two steps are needed:

1. NAT device needs to be instructed to accept incoming connection requests to specific port numbers. Not onl that, but the private IP address of the server on the LAN-side to handle these requests needs to be configured too. This is called *port forwarding*.

2. We need to be certain that server IP address is not going to change. (In many home networks, the broadband router does include a DHCP server too. The role of that server is to provide IP addresses to computer on the LAN-side using DHCP protocol. The usual policy is to provide any free address to a requester. This might be a problem as could provide different addresses to our server on different occasions). One way of achieving that is to configure the server with a static address (instead of using DHCP).

Exercise#7. We will not configure a NAT router in this lab to perform *port forwarding*. Instead, we will see the packets arriving to such router from the ISP-side to reach an ssh server on the LAN-side. This is contained in files SSH_LAN_1 and SSH_ISP_1.

1. Client and server IP addresses?
2. What are source and destination ports?
3. What differences do you see between LAN-side and ISP-side traffic in this capture? Are messages being modified when being forwarded by the router?