DHCP & NAT Lab

On moodle you have a trace file called “DHCP”, download and open it. Filter out necessary DHCP packets using command “bootp” or “udp.port==67” (68). In the list of filtered packets you should see DHCP discover, offer, request, acknowledgment (and release) packets. Those are related to the phases that occur in DHCP operation (Figure 1).

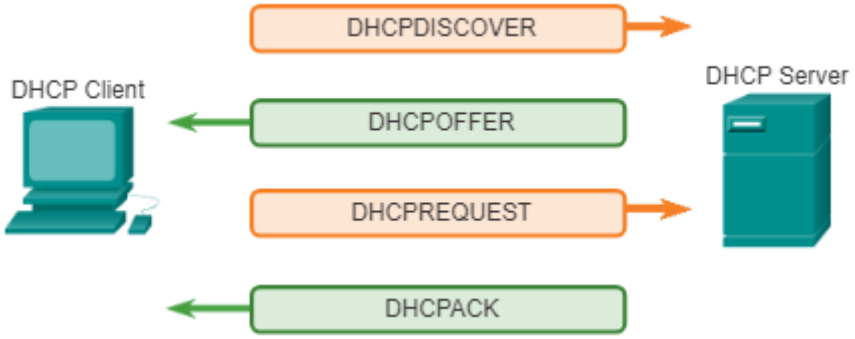

Figure 1 – DHCP operation

After this step you will see only the packets of the DHCP protocol. Answer the following questions:

0) What is the IP address of the DHCP server?

1) Write down the list of DNSs that DHCP server offers

2) Is the client asking for a particular IP address from the server? If yes, which?

3) What is (are) the IP address (es) DHCP server is offering to you?

4) In which option (number and name) in the Bootstrap protocol tree, DHCP server tells its identifier (IP address)?

5) How much time you can use that IP address, according to the information given in the packets?

As you are finished with DHCP trace file, you can close it. On moodle, just below the DHCP trace file you can find two trace files “NAT_HOME_SIDE” and “NAT_ISP_SIDE”.

Look at the picture on the second page, which briefly describes the basic structure and goal of NAT

Answer the following questions:

6) What is the IP address of the client?

The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes).

Find any HTTP GET packet from NAT_HOME_SIDE and also find the similar packet from NAT_ISP_SIDE (their frame sizes must be identical). From these packets:

7) Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.102967. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

8-a) At what time is the corresponding 200 OK HTTP message received from the Google server?

8-b) What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

In the following we'll focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (NAT_ISP_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

9-a) In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file?

9-b) What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)?

9-c) Which of these fields are the same, and which are different, than in your answer to question 7 above?

10-a) In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

10-b) What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

10-c) Which of these fields are the same, and which are different than your answer to question 8 above?

11) Based on this information, fill in the following table:

NAT Translation table	
Local (IP & port)	Global (IP & port)

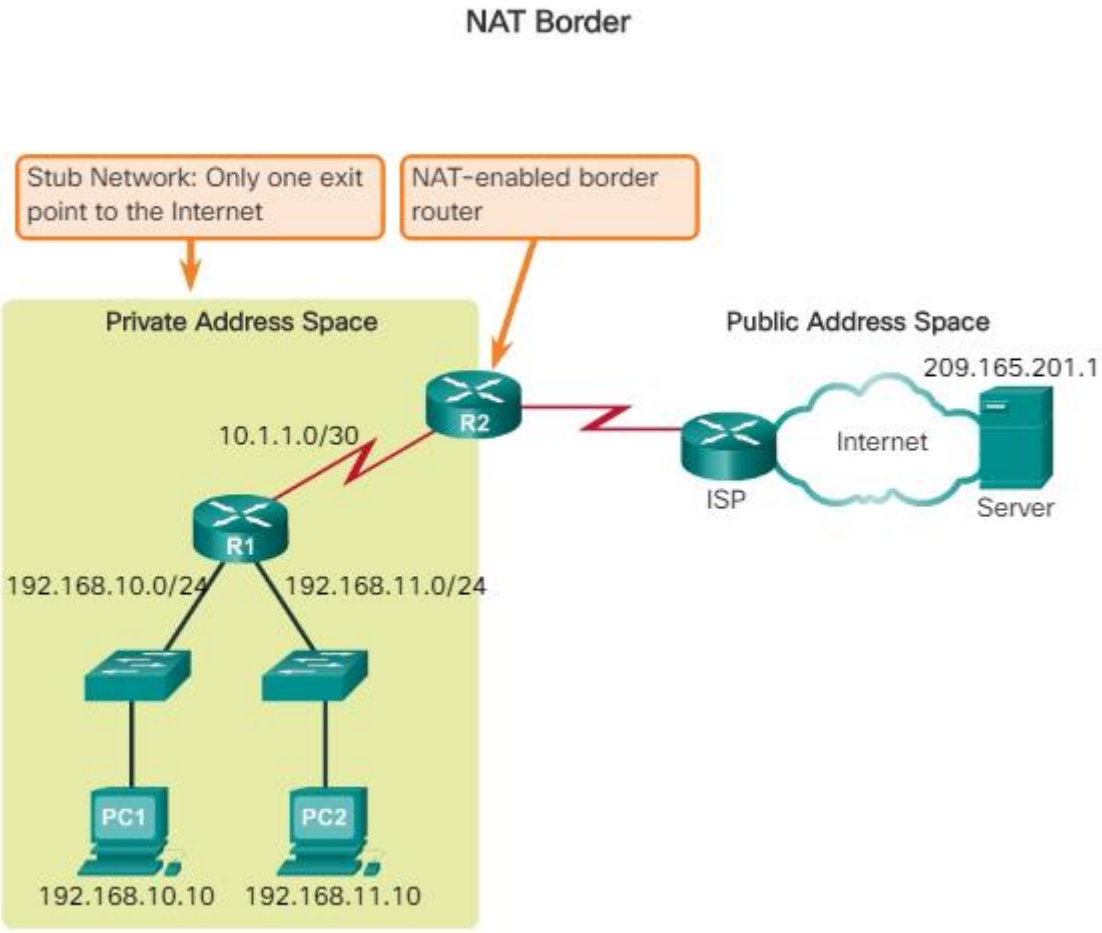

Figure 2 – NAT Border

NAT-enabled routers can be configured with one or more valid public IPv4 addresses. These public addresses are known as the NAT pool. When an internal device sends traffic out of the network, the NAT-enabled router translates the internal IPv4 address of the device to a public address from the NAT pool. To outside devices, all traffic entering and exiting the network appears to have a public IPv4 address from the provided pool of addresses.

A NAT router typically operates at the border of a stub network. A stub network is a network that has a single connection to its neighboring network, one way in and one way out of the network. In the example in the figure, R2 is a border router. As seen from the ISP, R2 forms a stub network.

When a device inside the stub network wants to communicate with a device outside of its network, the packet is forwarded to the border router. The border router performs the NAT process, translating the internal private address of the device to a public, outside, routable address.