# Department of Computer Science

**EE353: Computer Networks**

**Class: BSCS-7AB**

# Lab 11: *NAT*

# Date: 2th Dec, 2019

**Lab Engineer: Engr. Kaleem Ullah**

# Instructor: Dr. Zeeshan

***Name: M. Hasnain Naeem***

***Reg. No: 212728***

***1.0 NAT* Network Address Translation:**

The Internet is expanding at an exponential rate. As the amount of information and resources increases, it is becoming a requirement for even the smallest businesses and homes to connect to the Internet. Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet cheaply and efficiently.

In [computer networking](http://en.wikipedia.org/wiki/Computer_network), **network address translation** (**NAT**) is the process of modifying [IP address](http://en.wikipedia.org/wiki/IP_address) information in [IP packet headers](http://en.wikipedia.org/wiki/IPv4_header) while in transit across a traffic [routing device](http://en.wikipedia.org/wiki/Router_%28computing%29).

The simplest type of NAT provides a one to one translation of IP addresses. [RFC 2663](http://tools.ietf.org/html/rfc2663) refers to this type of NAT as **basic NAT**. It is often also referred to as **one-to-one NAT**. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address need to be changed. The rest of the packet can be left untouched (at least for basic TCP/UDP functionality, some higher level protocols may need further translation). Basic NATs can be used when there is a requirement to interconnect two IP networks with incompatible addressing.

The impetus towards increasing use of NAT comes from a number of factors:

* A world shortage of IP addresses
* Security needs
* Ease and flexibility of network administration

## IP Addresses

Because IP addresses are a scarce resource, most Internet Service Providers (ISPs) will only allocate one address to a single customer. In majority of cases this address is assigned dynamically, so every time a client connects to the ISP a different address will be provided. Big companies can buy more addresses, but for small businesses and home users the cost of doing so is prohibitive. Because such users are given only one IP address, they can have only one computer connected to the Internet at one time. When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. Theoretically, you could have [4,294,967,296 unique addresses](http://www.howstuffworks.com/question549.htm) (232). The actual number of available addresses is smaller (somewhere between 3.2 and 3.3 billion) because of the way that the addresses are separated into classes, and because some addresses are set aside for multicasting, testing or other special uses. This is where NAT comes to the rescue. Network Address Translation allows a single device, such as a [router](http://www.howstuffworks.com/router.htm), to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers. With an NAT gateway running on this single computer, it is possible to share that single address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer is connected.

## Security Considerations

To combat the security problem, a number of firewall products are available. They are placed between the user and the Internet and verify all traffic before allowing it to pass through. This means, for example, that no unauthorized user would be allowed to access the company's file or email server. The problem with firewall solutions is that they are expensive and difficult to set up and maintain, putting them out of reach for home and small business users.

NAT automatically provides firewall-style protection without any special set-up. That is because it only allows connections that are originated on the inside network. This means, for example, that an internal client can connect to an outside FTP server, but an outside client will not be able to connect to an internal FTP server because it would have to originate the connection, and NAT will not allow that.





**Steps for performing this part of lab:**

In this lab, we’ll capture packets from a simple web request from a client PC in a home network to a www.google.com server. Within a home network, the home network router typically provides a NAT service.

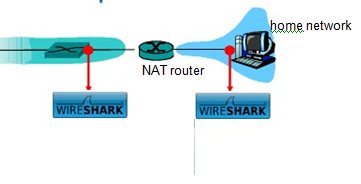


Figure 5: NAT trace collection scenario

Figure 5 shows our Wireshark trace-collection scenario. As in our other Wireshark labs, we collect a Wireshark trace on the client PC in our home network. This file is called NAT\_home\_side. Because we are also interested in the packets being sent by the NAT router into the ISP, we’ll collect a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in Figure 1. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT\_ISP\_side.

Open the NAT\_home\_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file. 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) into the Filter field in Wireshark.

**Questions:**

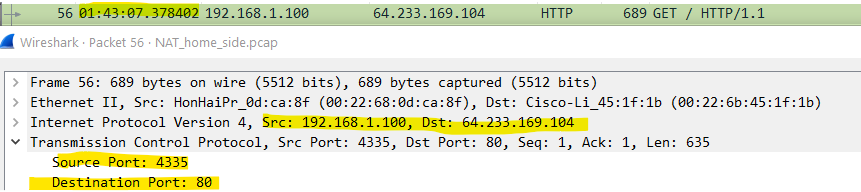
1. What is the IP address of the client?

Client IP: 192.168.1.100



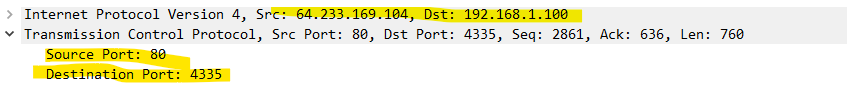
1. Consider now the HTTP GET sent from the client to the Google server (IP address 64.233.169.104) at time 02:43:07.378402. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

**Source IP & Port:** 192.168.1.100**:***4335***Destination IP & Port:** 64.233.169.104**:***80*



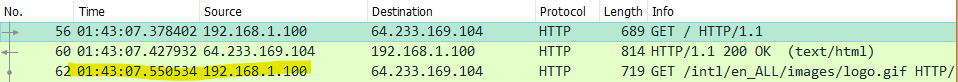
1. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

**Source IP & Port:** 64.233.169.104**:***80***Destination IP & Port:** 192.168.1.100**:***4335*



1. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the TCP connection ready?

TCP connection will be ready after 3-way handshake when both client and server have acknowledged their presence to each other.   
In this case, TCP connection is ready at time: 01:43:07.550534



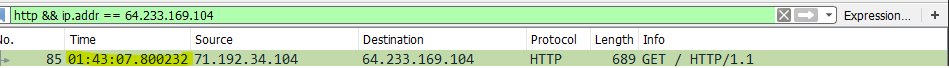
In the following we’ll focus on the two HTTP messages (GET and 200 OK) identified above. Our goal below will be to locate these two HTTP messages in the trace file (NAT\_ISP\_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through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

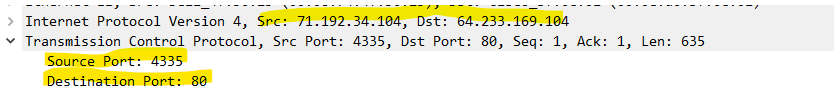
Open the NAT\_ISP\_side. Note that the time stamps in this file and in NAT\_home\_side are not synchronized since the packet captures at the two locations shown in Figure 1 were not started simultaneously.

1. In the NAT\_ISP\_side trace file, find the first HTTP GET message that was sent from the client to the Google server. At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Time of appearance: 01.43.07.800232

**Source IP & Port:** 71.192.34.104.104**:***4335***Destination IP & Port:** 64.233.169.104**:***80*





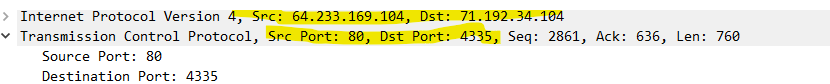
1. Compare these values with the corresponding values in the NAT\_home\_side file and comment whether NAT or NAPT is being used at the NAT router.

NAT is being used. Because, IP and Port are the same on client and ISP side NAT (4334 and 80). NAPT changes the Port along with the IP. But, NAT changes only the IP address of client computers.

1. In the NAT\_ISP\_side trace file, at what time is the 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Receiving Time: 01:43:07.848634

**Source IP & Port:** 64.233.169.104**:***80***Destination IP & Port:** 71.192.34.104:4335

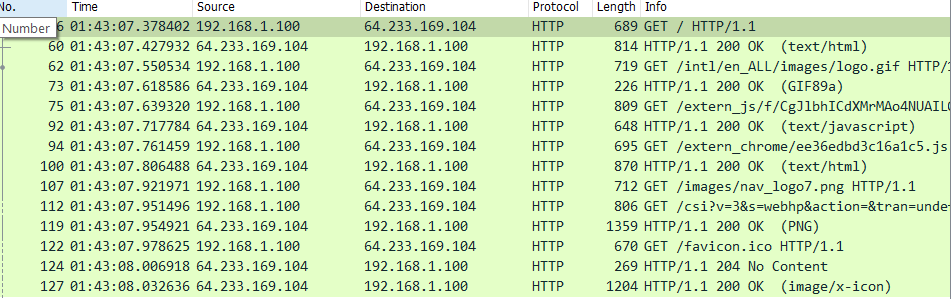


1. Locate the TCP connection(s) made for this HTTP transaction. How many TCP connections have been made? Does the TCP connection addresses also get modified while passing through the NAT router?

Assuming transaction means opening [www.google.com](http://www.google.com)

Although there are 7 OK messages but only 1 TCP connection is made. Because, HTTP/1.1 is, by default, persistent.

Yes, TCP source connection address gets modified when it passes through the NAT router.



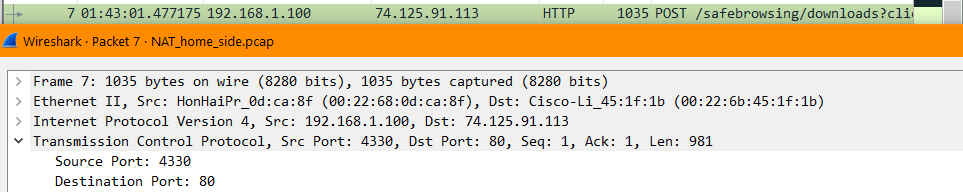
1. List at least two entries that exist in the NAT table of the router.

|  |  |
| --- | --- |
| WAN Side Address | LAN Side Address |
| 71.192.34.104.10 : 4335 | 192.168.1.100 : 4335 |
| 71.192.34.104.10 : 4330 | 192.168.1.100 : 4330 |

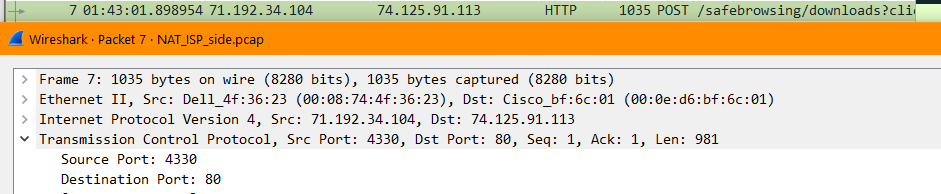
**Using another packet to get 2nd entry for the NAT router table.**

Information of packet is given below.

Client Side



ISP Side



**Conclusion**

IP address assignment and translation are very important aspects in computer networks. Due to limited number of IP addresses in IPV4, NAT mechanism is used to entertain multiple computers through a router.

In this lab, we analyzed the working of NAT by inspecting the packets from ISP and client side.