

A close up of a device

Description automatically generated

COE 371L

Computer Networks I

Fall 2019

Lab #11

Section #2

Title: NAT

Name : Amir Mohideen, Zayed Mohamed

ID: 74559, 75771

Lab – Configuring Dynamic and Static NAT

1. Build the Network and Verify Connectivity
2. Configure and Verify Static NAT

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

* 1. Configure a static mapping.
  2. Specify the interfaces.
  3. Test the configuration.
     1. Display the static NAT table by issuing the **show ip nat translations** command.

What is the translation of the Inside local host address?

**[Report – 1Pt]** 192.168.1.20 = 209.165.200.225

**[Report – 1Pt]** The Inside global address is assigned by?

The router from the NAT pool.

**[Report – 1Pt]** The Inside local address is assigned by?

The administrator for the workstation.

* + 1. From PC-A, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

A NAT entry was added to the table with ICMP listed as the protocol when PC-A sent an ICMP request (ping) to 192.31.7.1 on ISP.

**[Report – 1Pt]** What port number was used in this ICMP exchange? 10

**Note**: It may be necessary to disable the PC-A firewall for the ping to be successful.

* + 1. From PC-A, telnet to the ISP Lo0 interface and display the NAT table.

**Note**: The NAT for the ICMP request may have timed out and been removed from the NAT table.

**[Report – 1Pt]** What was the protocol used in this translation? TCP

What are the port numbers used?

**[Report – 1Pt]** Inside global / local: 1034

**[Report – 1Pt]** Outside global / local: 23

* + 1. Because static NAT was configured for PC-A, verify that pinging from ISP to PC-A at the static NAT public address (209.165.200.225) is successful.
    2. On the Gateway router, display the NAT table to verify the translation.
    3. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

1. Configure and Verify Dynamic NAT
   1. Clear NATs.
   2. Define an access control list (ACL) that matches the LAN private IP address range.
   3. Verify that the NAT interface configurations are still valid.
   4. Define the pool of usable public IP addresses.
   5. Define the NAT from the inside source list to the outside pool.
   6. Test the configuration.
      1. From PC-B, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

What is the translation of the Inside local host address for PC-B?

**[Report – 1Pt]** 192.168.1.21 = 209.165.200.242

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

**[Report – 1Pt]** What port number was used in this ICMP exchange? 20

* + 1. From PC-B, open a browser and enter the IP address of the ISP-simulated web server (Lo0 interface). When prompted, log in as **webuser** with a password of **webpass**.
    2. Display the NAT table.

**[Report – 1Pt]** What protocol was used in this translation? TCP

What port numbers were used?

**[Report]** Inside: 1038 to 1052

**[Report – 1Pt]** Outside: 80

**[Report – 1Pt]** What well-known port number and service was used? Port 80, www or http

* + 1. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.
  1. Remove the static NAT entry.

1. [Report – 4Pts] Reflection
   1. Why would NAT be used in a network?

NAT is used in a network when there aren’t enough public IP addresses and in order to avoid the cost of purchasing public addresses from an ISP. NAT also provides a measure of security by hiding internal addresses from outside networks.

* 1. What are the limitations of NAT?

The limitation is that NAT needs IP information or port number information in the IP header and TCP header of packets for translation. The list of protocols that cannot be used with NAT are SNMP, LDAP, Kerberos version 5.