**Name: ERIC SOMOGYI**

**esomogyi@depaul.edu**

NET463

Lab #1 –NAT

**ASSIGNMENT DOCUMENT**

**Must be done on Packet Tracer**

**Version 2: Updated network Diagram with correct address, corrected AS number**

***Lab Scenario:***

In this lab you will demonstrate how NAT translates IP addresses. As discussed in lecture, NAT translates non-routable private, internal addresses into routable, public addresses. NAT has an added benefit of providing a degree of privacy and security to a network because it hides internal IP addresses from outside networks. In this Lab, you will configure both a static NAT and NAT overload (aka PAT). Also, HSRP enables gateway router redundancy – a function that is critical in business operations.

A diagram of a network

Description automatically generated

**Figure 1: Lab #1 Network Diagram**

***Learning Objectives***

* Configure dynamic NAT *Overload*
* Configure HRSP
* Configure default routes
* Configure EIGRP routing protocol (basic)
* Configure an HTTP server in Packet Tracer
* Test connectivity and debug using *pings*

***Lab Procedure:***

**Configure hostnames, IP addresses, HTTP server**

1. Configure hostname prompt on each router and end device to the appropriate name shown in the network diagram. NOTE: The device name of device (routers and end devices) must be set to include your initials at the end. For example, if the lab includes routers R1 and R2 and hosts Host1 and Host2 and your initials are “AB”, you MUST set the names of these device to R1-AB, R2-AB, Host1-AB and Host2-AB. Prompts in ALL of your screen captures must include your prompt with your initials.
2. Assign IPv4 addresses to all router interfaces as defined in the IPv4 address assignment table.

**IPv4 Address Assignments**

|  |  |
| --- | --- |
| **Network** | **Subnet ID** |
| Branch Office | 192.168.8.0/24 |
| WAN | 166.0.0.0/24 |
| Data Center subnet | 110.0.0.0/24 |
| Link 1 | 177.1.0.0/24 |
| Link 2 | 177.2.0.0/24 |

1. Configure the HTTP server to return “<*your name*> Spring 2024 Lab #1!” as a response to an HTTP request

**Configure static routes and routing protocols**

1. Create default routes in R1, R2, R3, and R4 routers.
2. Configure EIGRP in R2,R3 and R4 to advertise link1, link2, and the Data Center subnet. Use the AS=**463** in our ***router eigrp*** *<AS number>* command. Use ***network*** commands to advertise the networks.

R1(config)#**router eigrp** 463

R1(config-router)#**network** *<subnet id> <wild-card>*

1. All end devices and router interfaces should now be able to successfully ping from one another.

**Configure NAT overloading**

1. Configure NAT overloading in router R1. Create a named standard Access Control List (ACL). To define the internal addresses that are translated to public addresses in the NAT process, create a named standard ACL called R1NAT. This list is used in the NAT configuration steps that follow.

R1(config)#**ip access-list standard** R1NAT

R1(config-std-nacl)#**permit** 192.168.8.00.0.0.255

1. Configure dynamic NAT to allow any host in subnet 192.168.8.0/24 to access the Internet at the same time. Configure NAT with *overload* to accommodate the additional hosts. NAT overload, also called *Port Address Translation (PAT****),*** uses port numbers to distinguish packets from different hosts that are assigned the same public IP address
2. Configure the interfaces on R1 to apply NAT. In interface configuration mode on R1, configure each of the interfaces using the **ip nat {inside | outside}** command.

**Configure HRSP**

1. Configure R3 and R4 routers that are serving as GW routers for the DC subnet with HSRPv1 (for IPv4). This will enable default router redundancy for the subnet. Configure HSRP with the settings below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Network** | **Active Router** | **Standby Router** | **Preempt** |
| DC subnet | R3 | R4 | YES |

***Lab Report / Questions (100pts):***

1. (5%) demonstrated in your screen shots that you used your initials for the host names and router names as specified in step 1 of the lab procedure.

A diagram of a network

Description automatically generated

1. (5%) Enter the command ***show ip route*** for routers R1, R2 and paste the **screenshots** below.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

1. (10%) From host 1, perform an HTTP query to the HTTP server. This should be successful. Paste a **screenshot** of the HTTP response below.

A screenshot of a computer

Description automatically generated

1. (10 pts) Execute a ***show standby brief*** on R3 and R4 and **paste results** here:

A screenshot of a computer

Description automatically generated

1. (10 pts) On Host 1, enter a ***ping -t*** to the web server *ipv4 address.* The ping with the “-t” option should continuously ping. While this ping is executing, go to R3 and perform a shutdown on the port that is connected to the DC subnet. You should find that the ping’s will stop being successful for several minutes and then return successfully. Take a screen shot on the host 1 command prompt of showing this ping behavior and **paste results** here.

A screenshot of a computer

Description automatically generated

1. (5 pts) Execute a ***show standby brief*** on R3 and R4 while the port is still in shutdown and **paste results** here:

A screenshot of a computer

Description automatically generated

1. (5 pts) Explain the reason in several CLEAR sentences the cause of WHY the behavior of the *ping’s* disappearing and then re-appearing resulting from the actions of the port shutdown.

Answer: The reason the ping’s timeout and disappear for a few seconds and then reappear is because that is during the time that the router EIGRP 463 feature on R2 was engaged due to the packets not flowing through R3 since the shutdown was initiated. In the EIGRP routing protocol, it’s dynamic autonomous system was engaged and eventually found another best path to the destination ip address which ended up being through data link 2 which was through Router 4.

1. (5 pts) Remove the port shutdown on R3 and execute a ***show standby brief*** on both R3 and R4 and **paste results** here.

A computer screen shot of a program

Description automatically generated

**A close-up of a computer screen

Description automatically generated**

A screenshot of a computer

Description automatically generated

**NAT Overload procedure and questions:**

1. (15%) You should now be able to ***ping*** from any inside host to the HTTP Server **(**USE the IP address of the R2 router**)** To see the effects of NAT on a specific packet, enter *Simulation mode* in Packet Tracer and observe the packet that originates from a **ping** on Host 1. Click the colored information box associated with that packet as it is passed from Host 1 to R1. By clicking Inbound PDU Details, you should see that the source address is IP address that you assigned. Include a **screenshot** of the results and paste here.
   * 1. A screenshot of a computer

        Description automatically generated
   1. By clicking Outbound PDU Details or R1, you should see that the source address has been translated to the inside global IP address. Include a **screenshot** of the results and paste here.

A screenshot of a computer

Description automatically generated

1. (10%) Based on your above explanation, discuss **why** such a method presents challenges with ***Ping packets*** and how this is generally resolved (hint: think about how Ping packets are encapsulated, that is, are they encapsulated in UDP or TCP?).
   1. Answer: Ping packets use the ICMP protocol. The ICMP protocol operates at the Layer 3 level but it also assists in Layer 4 when delivering error messages and operational information. Also, ICMP packets don’t use port numbers or establish a connection like in UDP or TCP. In layer 3, the ping packets include the ICMP headers and data is incapsulated with the IP datagram. In Layer 2, then the ICMP packet is encapsulated into a frame specific to the data link layer protocol. Then in Layer 1, the data is encapsulated and then transmitted over the physical medium of the wire. This collectively becomes challenging because when a device is accessing the internet from NAT through a singular ip address this requires different techniques for the ping packets to be delivered/responded to from the internal to external networks and it is necessary for data to be translated to the correct format so all the layers work together to read and accomplish the command.
2. (10%) On router R1, display the PAT translation table by entering the command ***show ip nat translations*** and include a **screenshot** of the results and paste here.

A screenshot of a computer

Description automatically generated

1. (10%) For the PAT address translation in router R1, provide an IP address example for each the following:

inside local address: Answer: 192.168.8.2:1600

inside global address: Answer: 166.0.0.1:1600

outside global address: Answer: 166.0.0.2:1601