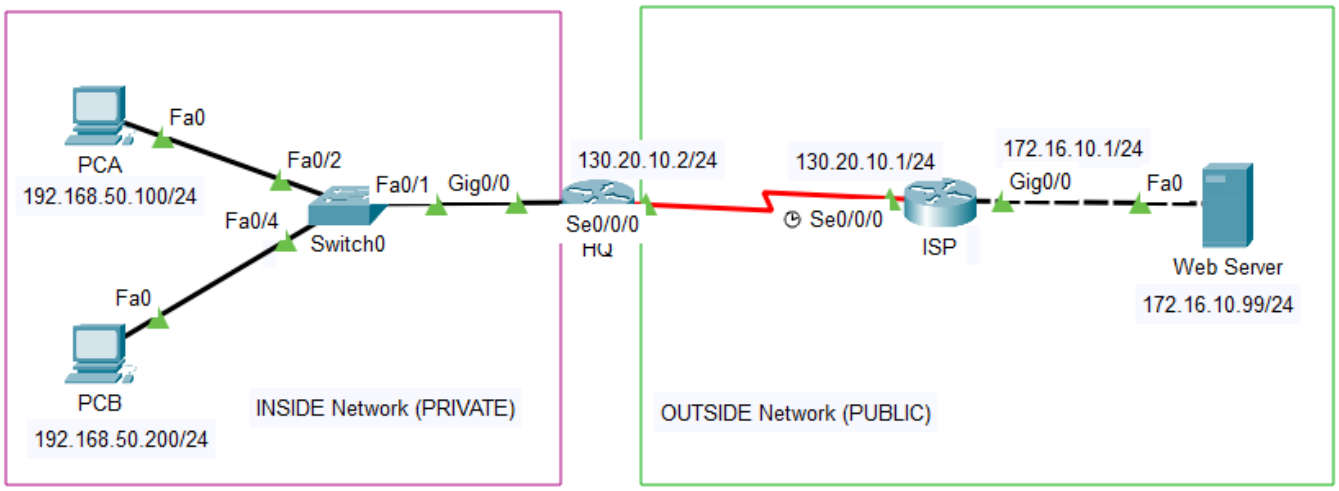
IT325 – IT Elective 2 (Networking)

Laboratory Activity 5 – Configuring NAT and PAT

Student Name: _____ Section: _____ Date: _____

Network Topology



Addressing Table:

Supply the IP Address based on the Network Topology given.

Device	Interface	IP Address	Gateway	Network Address	Subnet Mask
ISP	S0/0/0	130.20.10.1	_	130.20.10.0	255.255.255.252
	G0/0	172.16.10.1	_	10.10.10.0	255.255.255.0
HQ	S0/0/0	130.20.10.2	_	10.10.5.0	255.255.255.252
	G0/1	192.168.50.1	_	192.168.50.0	255.255.255.0
PC A	Fa0/1				
PC B	Fa0/1				
Server	Fa0/1				

Objectives

Part 1: Build and verify physical and logical connectivity

Part 2: Configure Dynamic NAT (PAT) and Static NAT

Part 3: Configure default route.

Part 4: Create an ACL to specify internal addresses for NAT translation.

Part 5: Verify Internet access for internal users and external access to the hosted server.

The network topology diagram was created using Cisco Packet Tracer for Educational purposes only.

Background / Scenario

You are hired as a network engineer at an ISP. Your task is to configure Dynamic NAT (PAT) to allow a **HQ** LAN users to access the Internet through a shared public IP, and set up Static NAT to make **ISP**'s internal server accessible to external users. Ensure seamless internet access for the customer and public availability of the hosted server.

Required Resources

- 2 Routers
- 1 Switch
- 3 PCs
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Assign a device name to each router.

	CLI Mode	Command
HQ		
ISP		

b. Assign **ustp** as the privileged EXEC encrypted password *Just **write** the configuration using the **Company** Router then do the same on the Branch router.*

	CLI Mode	Command
HQ & ISP		

c. Assign **bsit** as the console password and enable login. *Just **write** the configuration using the **Company** Router then do the same on the Branch router.*

	CLI Mode	Command
HQ & ISP		

d. Assign **it325** as the VTY password and enable login. *Just **write** the configuration using the **Company** Router then do the same on the Branch router.*

	CLI Mode	Command
HQ & ISP		

e. Encrypt the plaintext passwords. *Just **write** the configuration using the **Company** Router then do the same on the Branch router.*

	CLI Mode	Command
HQ & ISP		

f. Create a banner that warns anyone accessing the device that unauthorized access is prohibited. *Just **write** the configuration using the **Company** Router then do the same on the Branch router.*

	CLI Mode	Command
HQ & ISP		

g. Save the running configuration to the startup configuration file. *Just **write** the configuration using the **Company** Router then do the same on the Branch router.*

	CLI Mode	Command
HQ & ISP		

Part 2: Configure Interfaces.

Step 1: Configure interface addresses on each router.

a. Configure interface addresses on each router as shown in the Addressing Table above.

	CLI Mode	Command
HQ		

	CLI Mode	Command
ISP		

Part 3: Configure Static and Dynamic NAT (PAT – NAT Overload)

Step 1: Configure Inside and Outside NAT on the appropriate interface of router.

	CLI Mode	Command
ISP		

	CLI Mode	Command
HQ		

Step 2: Create an ACL to Permit Private IP Range (LAN) for HQ router.

	CLI Mode	Command
HQ		

Step 3: Implement NAT

a. Configure Static NAT Mapping in ISP

	CLI Mode	Command
ISP		

b. Configure Dynamic NAT overload in HQ

HQ	CLI Mode	Command

Part 4: Configure default route

ISP	CLI Mode	Command

HQ	CLI Mode	Command

Part 5: Verify NAT Translation

Step 1: Connectivity Verification

a. Assign IP Address, Gateway and Subnet Masks to PC A, PC B and Server.

Device	IP Address	Gateway IP	Subnet Mask
PC A			
PC B			
Server			

b. Test Connectivity. ALL should be Successful. *(Instructor checks and write on remarks*)

Source	Protocol	Destination	Remarks
PC A	Ping	ISP (G0/0)	
PC B	Ping	ISP (G0/0)	

Write the 1 line reply received from an ICMP command (PCB *ping* ISP(G0/0)

c. Verify NAT Translation.

Source	Protocol	Destination	Remarks
Server	Ping	PCA	
Server	Ping	PCB	

Write the 1 line reply received from an ICMP command (Server *ping* PCB)

REFLECTION:

What have I learned from this activity?