**Lab 10**

**Experiment name: Configuring Network Address Translation (NAT) using Static NAT in Cisco Packet Tracer**

**Apparatus Required:**

1. **Two Routers** (e.g., Cisco 2811)
2. **One Switch** (Layer 2 Switch – e.g., 2960)
3. **Two PCs** (inside private LAN)
4. **Two Servers** (representing public/external network services)
5. **Straight-through Ethernet cables**
6. **Serial cable** (for Router-to-Router connection)

**Tools Used:**

* **Cisco Packet Tracer** (for network simulation)
* **Router CLI** (for NAT configuration)
* **PC and Server desktop utilities** (Command Prompt, Web Browser, Ping for testing)

**Theory:**

The shortage of IPv4 addresses and the need for private networks to communicate with public networks led to the development of **Network Address Translation (NAT)**.Network Address Translation (NAT) allows private IP addresses used inside a network to be translated into public IP addresses for external communication. This allows multiple devices within a private network to access external resources while conserving public IP addresses.

NAT can operate in different modes: **Static NAT, Dynamic NAT, and PAT (Port Address Translation)**. Among these, **Static NAT** is the simplest form. It establishes a permanent, one-to-one mapping between an internal private address and an external public address. Unlike Dynamic NAT or PAT, where mappings may change, Static NAT ensures consistency, making it especially useful for devices like **web servers, email servers, or application servers** that must always be reachable at the same public IP address. Static NAT provides a fixed one-to-one mapping between private IP addresses (inside local) and public IP addresses (inside global).

**NAT Commands:**

1. **ip nat inside source static [inside-local] [inside-global]**

* This command creates a **static one-to-one mapping** between a private (inside local) IP address and a public (inside global) IP address.
* Example: ip nat inside source static 192.168.1.2 1.1.1.10

Here, the private IP 192.168.1.2 (PC in LAN) is permanently mapped to public IP 1.1.1.10.

2. **ip nat inside**

* Applied under an interface configuration mode.
* Defines that the selected interface belongs to the **inside network (LAN side)** where private IP addresses exist.
* Example:

interface fa0/0

ip nat inside

3.**ip nat outside**

* Applied under an interface configuration mode.
* Defines that the selected interface belongs to the **outside network (WAN/public side)** where public IP addresses exist.
* Example:

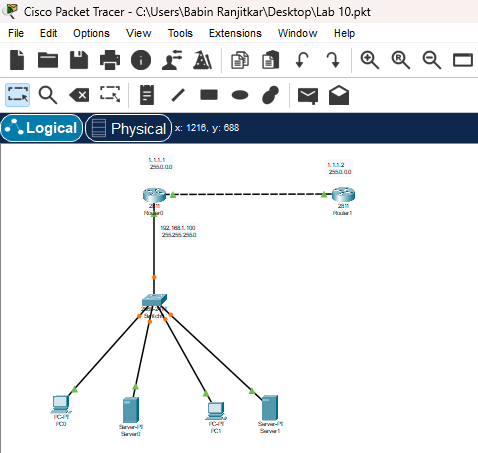
interface fa0/1

ip nat outside

4.**show ip nat translations**

* A **verification command** used in privileged EXEC mode.
* Displays the NAT table with mappings of inside local to inside global addresses.
* Useful to confirm whether static NAT mappings are correctly configured and active.

**Lab Diagram:**



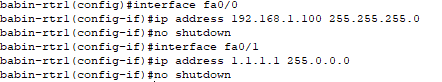
**Procedure:**

1**. Network Setup:**

* Connect PCs to **Switch**, and Switch to **Router1 (inside router)**.
* Connect **Router1 to Router2** using a serial connection.

**2. Configuring IP Addresses on Router Interfaces**

On router1(suv-rtr1):



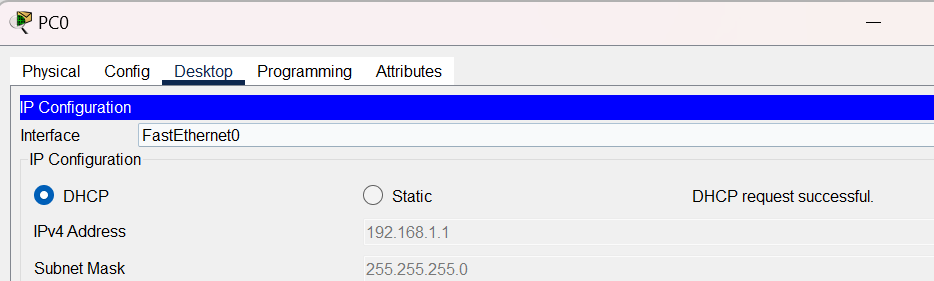
In router2(suv-rtr2):

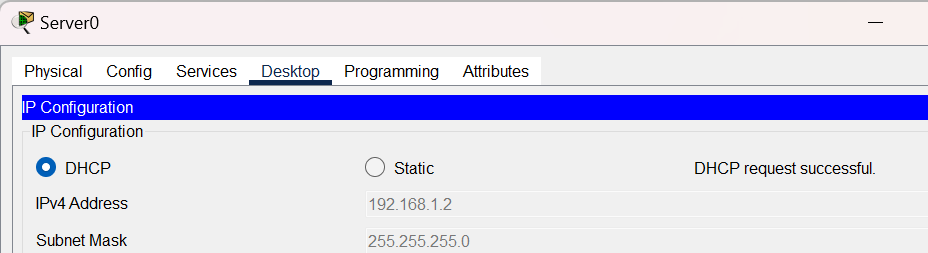


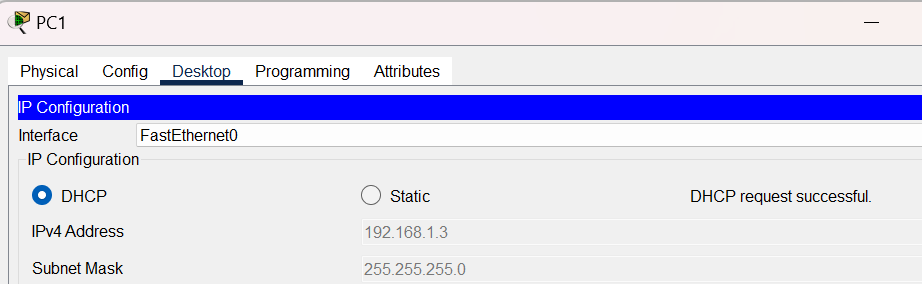
**3. Configuring DHCP for PCs and Servers**

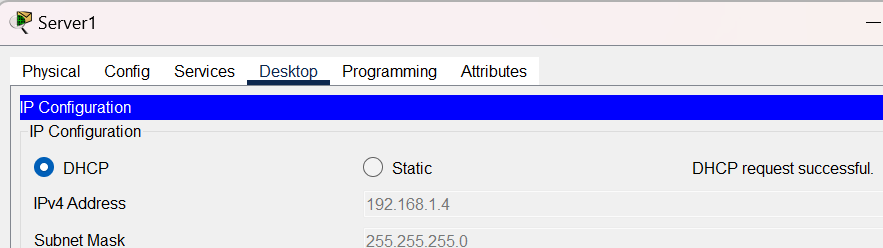


Now ,configuring DHCP in each end device:



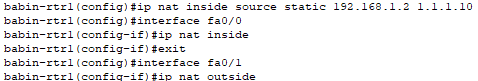






**4. Configuring Static NAT**

In router1(suv-rtr1):

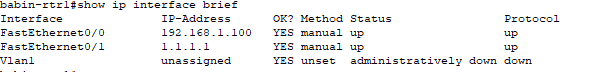


**Testing:**

**1. Verifying NAT Configuration on Router1:**



**2.IP Brief:**



**Conclusion**

In this lab, Static NAT was successfully configured on Router1 to provide a fixed one-to-one mapping between private IP addresses of PCs and public IP addresses. The NAT configuration allowed internal devices to communicate with external servers while maintaining consistent public IP addresses. Verification using show ip nat translations confirmed that the mappings were active, and the show ip interface brief command ensured that all relevant interfaces were correctly configured and operational.

This experiment demonstrated the importance of NAT in conserving public IP addresses, enabling secure communication between private and public networks, and ensuring accessibility of specific devices like servers from external networks.