**THE STATE UNIVERSITY OF ZANZIBAR(SUZA)**



**DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOY**

**COURSE CODE INF2103**

**COURSE TITLE DATA COMMUNICATION AND COMPUTER NETWORK**

**LECTURER DR OMAR**

**GROUP NO 13**

|  |  |
| --- | --- |
| **STUDENTS NAME** | **REG NO** |
| OMAR RAMADHAN ALLY | BITAM/11/23/051/TZ |
| ABDUL-GHAFOUR ABDU SOUD | BITAM/11/23/082/TZ |
| HAFSA SAID ALI | BITAM/11/23/003/TZ |
| IBRAHIM HAJI FAKI | BCS/18/23/028/TZ |
| MARYAM OMAR AHMED | BITAM/11/23/091/TZ |
| ALUWIYA GHARIB | BITAM/11/23/066/TZ |
| ABDUL-RAHMAN SILIMA HAJI | BITAM/11/23/086/TZ |
| KOHEN JOSEPH RICHARD | BITAM/11/23/070/TZ |

**QUESTION NO 13**

Perform configuration of a router that implements Network Address Translation (NAT) either dynamic or static. It should allow multiple devices to access the internet via a single public IP address. Verify the configuration on the devices by testing internet access on a NAT. Write and submit a report on the configuration, flow of data packets and any challenges you faced.

**SUBMISSION DATE** 17/01/2025 Friday

Network Address Translation (NAT) is a method used in networking that allows multiple devices on a local network to share a single public IP address for accessing the internet. This is particularly useful in conserving the number of public IP addresses used and enhancing security by hiding internal IP addresses.

Types of NAT

There are two primary types of NAT:

* Static NAT: Maps a single private IP address to a single public IP address.
* Dynamic NAT: Maps a private IP address to any available public IP address from a pool.

For this configuration, we will implement Dynamic NAT, which is more suitable for networks with multiple devices needing internet access.

Router Configuration Steps

The following steps outline how to configure dynamic NAT on a Cisco router:

### Step 1: Access the Router

Connect to your Cisco router using console access or SSH, and enter privileged EXEC mode:

enable

### Step 2: Define the Inside and Outside Interfaces

Identify which interface will be connected to the internal network (inside) and which will connect to the internet (outside). For example, if GigabitEthernet0/0 is the inside interface and GigabitEthernet0/1 is the outside interface:

configure terminal

interface GigabitEthernet0/0

ip nat inside

exit

interface GigabitEthernet0/1

ip nat outside

exit

### Step 3: Configure an Access Control List (ACL)

Create an ACL that defines which internal IP addresses can be translated. For instance, if you want to allow all hosts in the 192.168.1.0/24 subnet:

access-list 1 permit 192.168.1.0 0.0.0.255

### Step 4: Define the NAT Pool

Define a pool of public IP addresses that can be assigned dynamically. If you have one public IP address, you can define it as follows:

ip nat pool MY\_NAT\_POOL 203.0.113.10 203.0.113.10 netmask 255.255.255.255

If you had multiple public addresses, you would specify them accordingly.

### Step 5: Configure Dynamic NAT

Link the defined ACL with the NAT pool:

ip nat inside source list 1 pool MY\_NAT\_POOL overload

The overload keyword allows multiple devices on the inside network to share a single public IP address through Port Address Translation (PAT).

### Step 6: Save Configuration

After completing your configuration, save it to ensure it persists after reboots:

end

write memory

Verification of Configuration

To verify that NAT is working correctly, use these commands:

Check NAT translations:

show ip nat translations

Check statistics related to NAT:

show ip nat statistics

Test internet connectivity from an internal device by pinging an external site like Google:

ping www.google.com

If successful, this indicates that your configuration is correct.

Flow of Data Packets

When an internal device sends data packets destined for an external server:

The packet leaves the internal device with its private source IP.

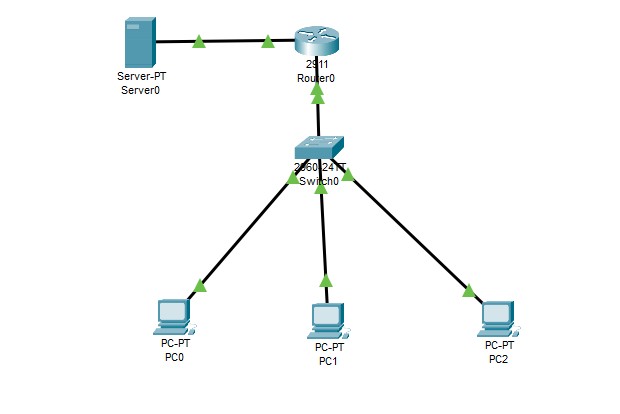
The router intercepts this packet and replaces its source IP with one from its configured NAT pool.

The packet then travels over the internet with this new source IP.

When responses come back from external servers, they are sent back to the router’s public IP.

The router translates this back into the corresponding private IP based on its translation table before forwarding it back to the original device.

**Demonstration Of NAT**

****

Challenges Faced

During configuration and testing, some common challenges may include:

Misconfiguring interfaces leading to no connectivity.

Incorrect ACL entries preventing desired traffic from being translated.

Not saving configurations leading to loss after reboot.

Troubleshooting connectivity issues due to firewall settings or ISP restrictions.

In conclusion, configuring dynamic NAT on a Cisco router allows multiple devices within a local network to access external resources using a single public-facing IP address effectively.