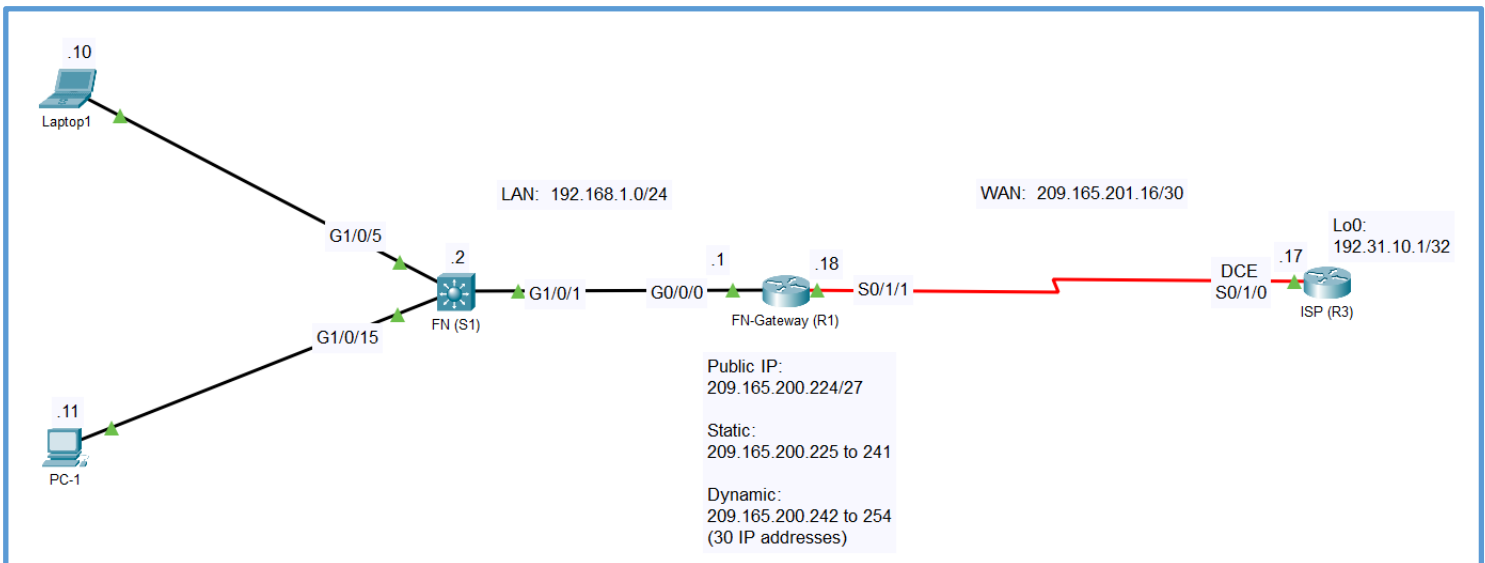


# Project : CCNA OBJECTIVE

## PART –1

### Lab Activity – Static and Dynamic NAT Configuration:

- There is one LAN and WAN in the topology below. Please develop the following topology on the physical pod/rack in the lab room.



### Required Resources:

- One Layer-3/Multilayer Switches (Cisco Catalyst 1000 Series with Cisco IOS Release 15.1+ image)
- Two routers (Cisco 4221 with Cisco IOS Release 17.6+ image)
- One PC and one laptop (Windows with Terminal Emulation Program)
- Cables:
  - Console cables to configure the Cisco IOS devices through the console port.
  - Ethernet and serial cables as shown in the topology.

### Addressing Table:

| Device     | Interface | IP Address     | Subnet Mask / CIDR | Default Gateway |
|------------|-----------|----------------|--------------------|-----------------|
| FN-S1      | VLAN 55   | 192.168.1.2    | 255.255.255.0      | 192.168.1.1     |
| FN-Gateway | G0/0/0    | 192.168.1.1    | 255.255.255.0      | N/A             |
|            | S0/1/1    | 209.165.201.18 | 255.255.255.252    | N/A             |
| ISP        | S0/1/0    | 209.165.201.17 | 255.255.255.252    | N/A             |
|            | Lo0       | 192.31.10.1    | 255.255.255.255    | N/A             |
| Laptop1    | N.I.C.    | 192.168.1.10   | 255.255.255.0      | 192.168.1.1     |
| PC-1       | N.I.C.    | 192.168.1.11   | 255.255.255.0      | 192.168.1.1     |

### Lab Description:

- In this lab, please build a LAN and WAN based simple network.
  - LAN with one switch and two hosts
  - Site-to-site WAN with two routers

For this lab consideration, the ISP has allotted 30 public IP addresses to the company from the address space of 209.165.200.224/27. The first 17 addresses are for static NAT from 209.165.200.225 to 241, and the remaining 13 addresses are for dynamic NAT from 209.165.200.242 to 254.

- You are also required to do the basic configuration on the following devices:
  - Switch:
    - Hostnames
    - SVI
    - Default gateway
    - Login banner
    - DNS lookup (disable)
  - Routers:
    - Hostnames
    - IP addressing
    - Login banner
    - DNS lookup (disable)
  - PC and Laptop:
    - IP address, subnet mask, default gateway

### Instructions:

Step 1: Set up the network topology.

- Develop the topology by using all the physical devices mentioned above and cable them all together:

Step 2: Configure and verify basic switch settings on all switches.

- Console into the switch and enter the global configuration mode:

Step 3: Configure and verify basic router settings on all routers.

- Console into the router and enter the global configuration mode:

Step 4: Configure the PC and laptop hosts as per the addressing table.

Step 5: Configure static routing on both routers as below:

- FN-Gateway router:
- ISP router:

Step 6: Configure static NAT on the FN-Gateway router.

Step 7: Verification:

- Using the command line at Laptop1, ping the IP addresses of:
  - G0/0/0 and S0/1/1 interfaces of FN-Gateway router (R1).
  - **S0/1/0 interface of the ISP router (R3).**
  - Virtual Interface VLAN 55 of switch FN (S1).
  - PC-A.
- Show “ip nat translations” on Gateway router (inside global and inside local addresses should be visible).
- Ping the Lo0 interface of the ISP router from Laptop1.
- “Show ip nat translations” on Gateway router (inside global, inside local, outside local, outside global).
- Ping from the ISP router to Laptop1.
- “Show ip nat translations” (on Gateway router)
- “Show ip nat statistics”

Step 8: Configure dynamic NAT on FN-Gateway router:

Step 9: Verify the connectivity.

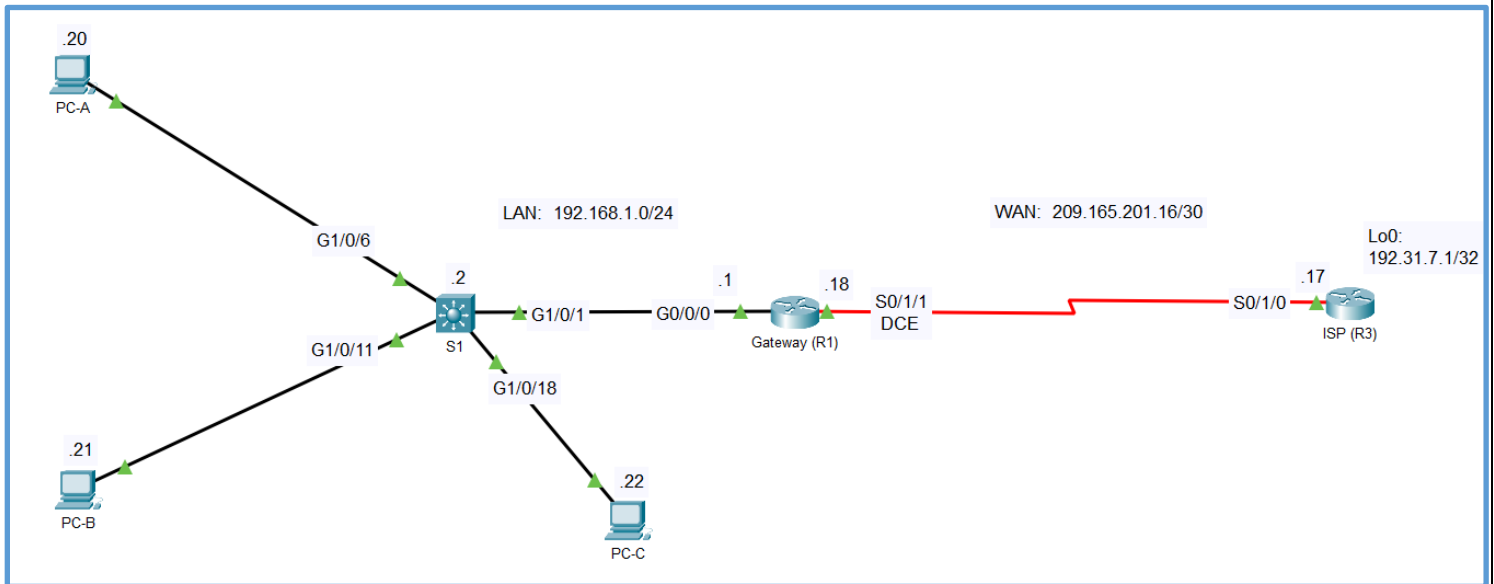
- Using the command line at Laptop1, ping the Lo0 interface of the ISP router.
- Using the command line at PC-A, ping the Lo0 interface of the ISP router.
- Check and verify the output of the following commands.
  - show ip nat statistics
  - show ip nat translations
- Ping Laptop1 and PC-A from the ISP router – Should not work

NOTE: All the above-mentioned pings must work, otherwise troubleshoot the network.

## Part 2:

### Configuring Port Address Translation (PAT)

#### Topology:



#### Addressing Table:

| Device       | Interface    | IP Address     | Subnet Mask     | Default Gateway |
|--------------|--------------|----------------|-----------------|-----------------|
| Gateway (R1) | G0/0/0       | 192.168.1.1    | 255.255.255.0   | N/A             |
|              | S0/1/1       | 209.165.201.18 | 255.255.255.252 | N/A             |
| ISP (R3)     | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252 | N/A             |
|              | Lo0          | 192.31.7.1     | 255.255.255.255 | N/A             |
| PC-A         | NIC          | 192.168.1.20   | 255.255.255.0   | 192.168.1.1     |
| PC-B         | NIC          | 192.168.1.21   | 255.255.255.0   | 192.168.1.1     |
| PC-C         | NIC          | 192.168.1.22   | 255.255.255.0   | 192.168.1.1     |

## Background / Scenario

Your company is allotted the public IP address range of 209.165.200.224/29 by the ISP. This provides the company with six public IP addresses. Dynamic NAT pool overload uses a pool of IP addresses in a many-to-many relationship. The router uses the first IP address in the pool and assigns connections using the IP address plus a unique port number. After the maximum number of translations for a single IP address have been reached on the router (platform and hardware specific), it uses the next IP address in the pool. NAT pool overload is a form port address translation (PAT) that overloads a group of public IPv4 addresses.

In Part 2, the ISP has allocated a single IP address, 209.165.201.18, to your company for use on the internet connection from the company Gateway router to the ISP. You will use the PAT to convert multiple internal addresses into one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

## Required Resources:

- One Layer-3/Multilayer Switches (Cisco Catalyst 1000 Series with Cisco IOS Release 15.1+ image)
- Two routers (Cisco 4221 with Cisco IOS Release 17.6+ image)
- Three PCs (Windows with Terminal Emulation Program)
- Cables:
  - Console cables to configure the Cisco IOS devices through the console port.
  - Ethernet and serial cables as shown in the topology.

## Step 1: Build the Network and Verify Connectivity

In Step 1, you will set up the network topology and configure basic settings such as the interface IP addresses, static routing, device access, and passwords.

1. Cable the network as shown in the topology.
2. Configure PC hosts.
3. Initialize and reload the routers and switches.
4. Configure basic settings for each router.
5. Configure static routing.
  - Create a static route from the ISP router to the Gateway router.
  - ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**
  - Create a default route from the Gateway router to the ISP router.
  - Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**
  - Verify network connectivity.
  - From the PC hosts, ping the G0/0/0 interface on the Gateway router.  
Troubleshoot if the pings are unsuccessful.
  - Verify the static routes are configured correctly on both routers.

## **Step 2: Configure and Verify NAT Pool Overload**

In Step 2, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the six usable addresses in the 209.165.200.224/29 range.

6. Define an access control list that matches the LAN private IP addresses.
7. Define the pool of usable public IP addresses.  
Gateway(config)# **ip nat pool public\_access 209.165.200.225  
209.165.200.230 netmask 255.255.255.248**
8. Define the NAT from the inside source list to the outside pool.
9. Specify the interfaces.
10. Verify the NAT pool overload configuration.

From each PC host, ping the 192.31.7.1 address on the ISP router.

### **Step 3: Configure and Verify PAT**

In Step 3, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all the commands in Step 2 will be reused in Step 3.

**11. Clear NATs and statistics on the Gateway router.**

**12. Verify the configuration for NAT.**

**13. Remove the pool of useable public IP addresses.**

**14. Remove the NAT translation from inside source list to outside pool.**

**15. Associate the source list with the outside interface.**

**16. Test the PAT configuration.**

- From each PC, ping the 192.31.7.1 address on the ISP router.
- Display NAT statistics on the Gateway router.

Gateway# **show ip nat statistics**

- Display NAT translations on Gateway.

Gateway# **show ip nat translations**