# Computer Networks Lab
## Spring 2024
## Week 13

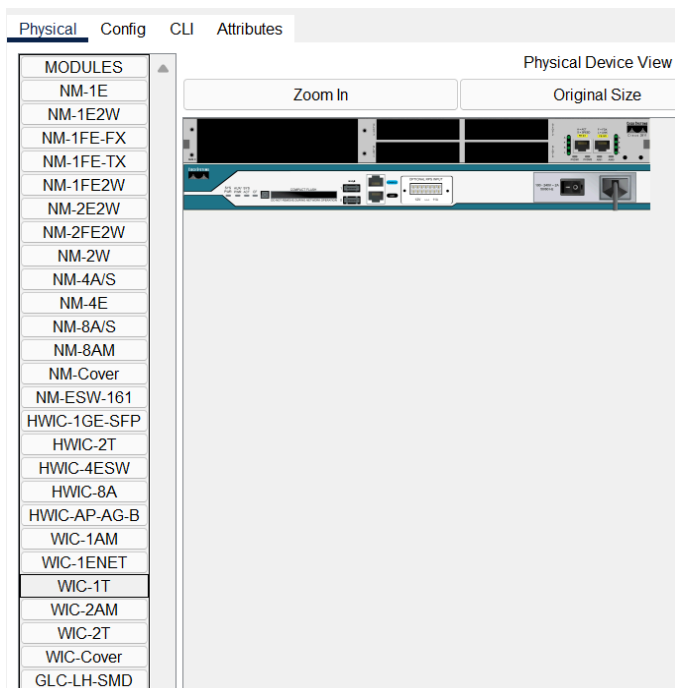# NAT and Access List

**Router in use:**



2811
Router2

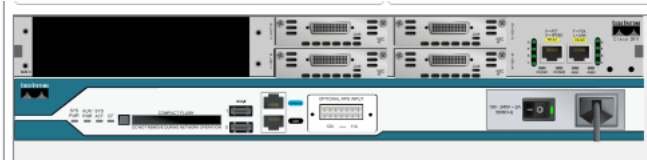**How to add and use Serial Cable:**

1. Go to the physical portion of the router.
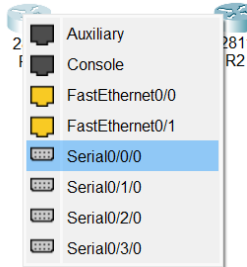2. Turn off the router.



3. Choose WIC-1T

4. Add ports according to need, and turn on the router



5. To connect two routers using serial cable, use Serial DTE wire 
6. Connect one's serial port with the other router's



7. And you will have a connection like:



8. Add ip address, turn on the ports and you are good to go.


# NAT (Network Address Translation)

Border routers are typically configured for NAT. H. A router with an interface on the local (internal) network and an interface on the global (external) network. When a packet leaves the local (internal) network, NAT translates its local (private) IP address to a global (public) IP address. Global (public) IP addresses are translated to local (private) IP addresses when packets enter the local network. When NAT runs out of addresses, i. H. if there are no more addresses in the configured pool, the packet is dropped and an Internet Control Message Protocol (ICMP) host unreachable packet is sent to the destination.


## Term in NAT:

1. Inside Local: It is a region inside the Enterprise's network where the hosts have Private IP addresses.
2. Inside Global: It is also a region inside the Enterprise network, but Public IP addresses are used in this region (this region is usually connected to the outside network or Internet).
3. Outside Local: It is a region that is generally part of the Enterprise network but in a public Internet (or outside the Enterprise Network). The hosts of the Outside Local region have private IP addresses.
4. Outside Global: It is a part of the Enterprise network in a public Internet where Public IP addresses is used.

# Walk Through Task:

**Step 1**: Create a topology as such:
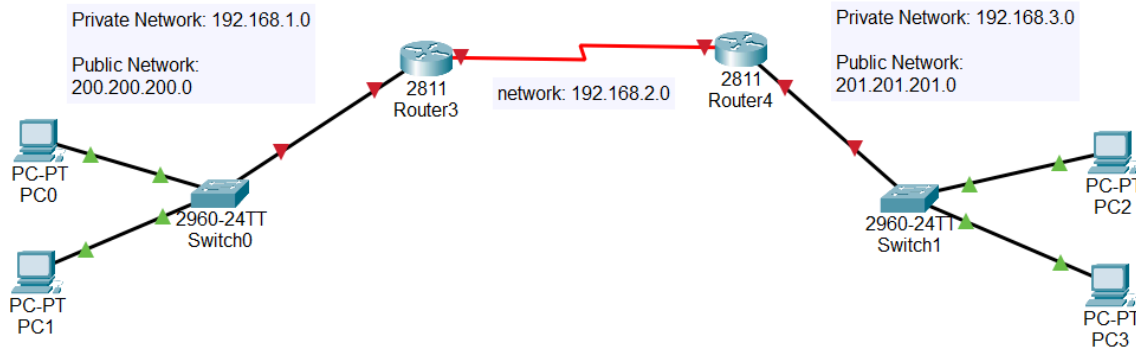


**Step 2**: Assign ip addresses to the PC accordingly as mentioned in the image above with the accurate default gateway.
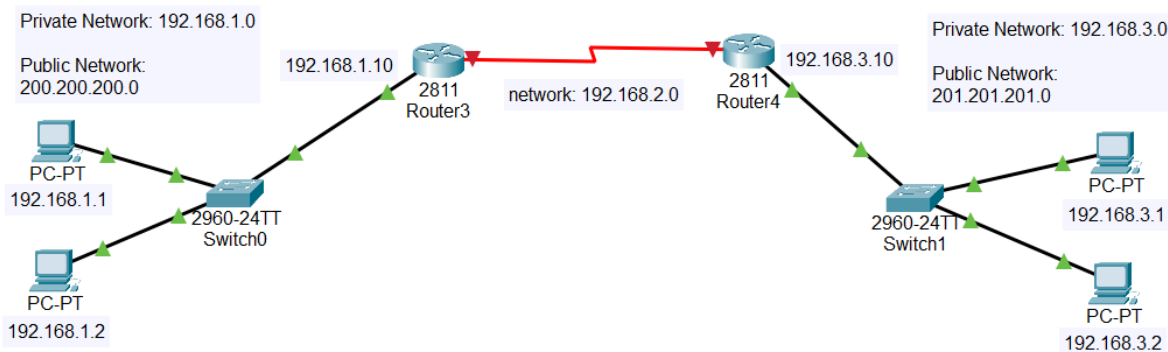


**Step 3**: Assign IP address to the ports of the router connecting with each other, let the network be 192.168.2.0.

**For router on the left**

**Step 3.1:** go to the router's CLI

**Step 3.2:** type '**en**'

**Step 3.3:** type '**config t**' to access configuration terminal

**Step 3.4:** access the interface connected to the other router (in this case its serial 0/0/0)

**Step 3.5:** add ip address by using the command '**ip address 192.168.2.1 255.255.255.0**'. Here 192.168.2.1 is the ip address, while 255.255.255.0 is the subnet mask.

**Step 3.6:** '**no shutdown**' the interface.

```
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

**For router on the right**

**Step 3.1:** go to the router's CLI

**Step 3.2:** type 'en'

**Step 3.3:** type 'config t' to access configuration terminal

**Step 3.4:** access the interface connected to the other router (in this case its serial 0/0/0)

**Step 3.5:** add ip address by using the command 'ip address 192.168.2.2 255.255.255.0'. Here 192.168.2.2 is the ip address, while 255.255.255.0 is the subnet mask.

**Step 3.6:** 'no shutdown' the interface.

```
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

**Step 4**: Once routing is done, apply Nat using the following steps

**Step 4.1:** go to the router's CLI

**Step 4.2:** type 'en'

**Step 4.3:** type 'config t' to access configuration terminal

**Step 4.4:** use the command ip nat inside source static private_ip_address public_ip_address

**Step 4.5:** access the interface that is connected to the private network

**Step 4.6:** mention that specific interface for inside nat using the command ip nat inside

**Step 4.7:** access the interface that is connected to the other router

**Step 4.8:** mention that specific interface for inside nat using the command ip nat outside

```
Router(config)#ip nat inside source static 192.168.1.1  200.200.200.1
Router(config)#ip nat inside source static 192.168.1.2  200.200.200.2
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip nat outside
Router(config-if)#
```

Repeat the steps for the other router as well.

```
Router(config)#
Router(config)#ip nat inside source static 192.168.3.1 201.201.201.1
Router(config)#ip nat inside source static 192.168.3.2 201.201.201.2
Router(config)#ip nat inside source static 192.168.3.10 201.201.201.10
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip nat outside
Router(config-if)#
```

**Step 5**: To check NAT configuration, go to the admin terminal and type the command **show ip nat translation**

```
Router#
Router#show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
---  201.201.201.10     192.168.3.10       ---                ---
---  201.201.201.1      192.168.3.1        ---                ---
---  201.201.201.2      192.168.3.2        ---                ---

Router#
```

```
Router#
Router#show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
---  200.200.200.1      192.168.1.1        ---                ---
---  200.200.200.2      192.168.1.2        ---                ---

Router#
```
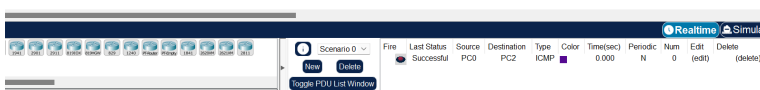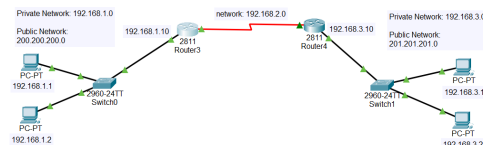
**Step 6**: Apply static on both of the routers as shown in the image below

```
Router(config)#
Router(config)#ip route 201.201.201.0 255.255.255.0 192.168.2.2
```

```
Router(config)#ip route 200.200.200.0 255.255.255.0 192.168.2.1
```

**Step 7:** Send packets to check the working of the topology

# ACL (Access Control List)

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

## Features of ACL:

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.
4.

## Walk Through Task:

**Step 1**:Continuing from the topology created in the previous section

**Step 2**: Use the command **access-list acees_list_number deny/permit network wildcard_mask** , as shown in the image below.

```
Router(config)#access-list 10 deny 201.201.201.1 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#show access-list 10
Standard IP access list 10
    deny 201.201.201.0 0.0.0.255
    permit any

Router#
```