

## Experiment No: 01

**Experiment Name:** Configuring a DHCP service on a generic server

### Objectives:

To achieve a clear understanding of how DHCP works, including its role in automatically assigning IP addresses and network configuration parameters to devices on a network.

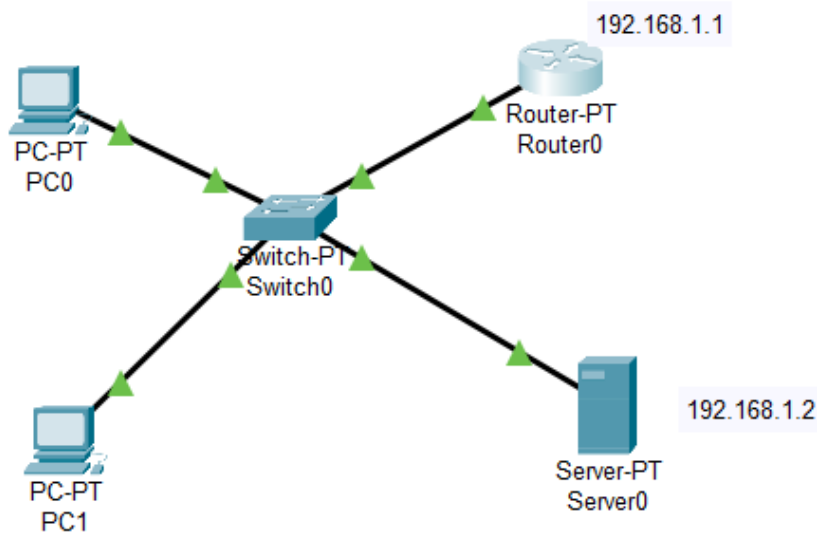
### Theory:

Dynamic Host Configuration Protocol (DHCP) is a protocol that enables the automatic allocation of IP addresses and other network configuration settings to devices on a network. This eliminates the need for manual IP configuration and enhances the efficiency of network management. In this lab, we utilized Cisco Packet Tracer to simulate the configuration of a DHCP server and observe its functionality in assigning IP addresses to client devices.

### Equipment:

- Cisco Packet Tracer software
- Virtual network environment within Cisco Packet Tracer
- Router (PT-router)
- Switches (PT-switch)

### Network Configuration:



### Working procedure:

**Setting up the DHCP server:** Take two pc, a Switch, Router, Server in Cisco packet tracer and connect them with wires according to above network configuration.

**Router Config:** Double click on Router and select CLI then run command below,

- enable
- configure terminal
- interface FastEthernet0/0
- ip add 192.168.1.1 255.255.255.0
- no shutdown
- exit

**Server Config:** Double click on server then select Desktop > IP configuration then setup IP follow the image below,

The screenshot shows the 'IP Configuration' tab. Under 'IP Configuration', the 'Static' radio button is selected. The IPv4 Address is 192.168.1.2, Subnet Mask is 255.255.255.0, and Default Gateway is 192.168.1.1. Under 'IPv6 Configuration', the 'Static' radio button is also selected, with an IPv6 Address of FE80::209:7CFF:FEC9:D810.

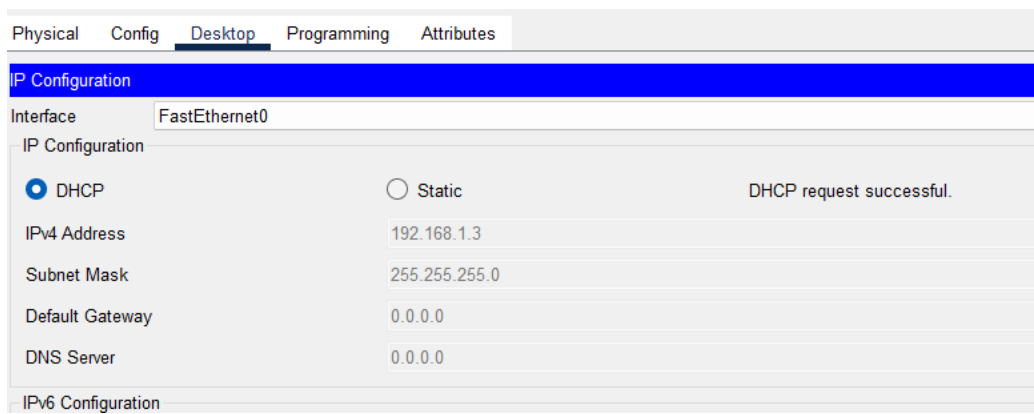
Then select Services > DHCP and setup services according to the image below, then click On and save,

The screenshot shows the 'DHCP' configuration window. The 'Service' is set to 'On'. The 'Interface' is 'FastEthernet0'. The 'Pool Name' is 'serverPool1'. The 'Default Gateway' is 192.168.1.1. The 'DNS Server' is 0.0.0.0. The 'Start IP Address' is 192.168.1.1 and the 'Subnet Mask' is 255.255.255.0. The 'Maximum Number of Users' is 156. The 'TFTP Server' and 'WLC Address' are both 0.0.0.0.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool1	192.168.1.1	0.0.0.0	192.168.1.1	255.255.255.0	156	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1.0	255.255.255.0	512	0.0.0.0	0.0.0.0

## Result:

Double click on any pc on the network and select Desktop > IP configuration > DHCP then automatic request the IP and I will be getting that PC0 IP (e.g. 192.168.1.3).



## Discussion:

The lab successfully demonstrated the configuration and functionality of a DHCP server using Cisco Packet Tracer. DHCP greatly simplifies IP address management and enhances network scalability. By configuring the router's DHCP services, we observed the automatic IP address assignment process in action. The ability to monitor DHCP logs and track IP assignments provides valuable insights into network activities.

## Experiment No: 02

**Experiment Name:** Basic RIP configuration in packet tracer.

### Objective:

To provide hands-on experience in setting up and configuring RIP, a distance-vector routing protocol, to facilitate routing between interconnected networks.

### Theory:

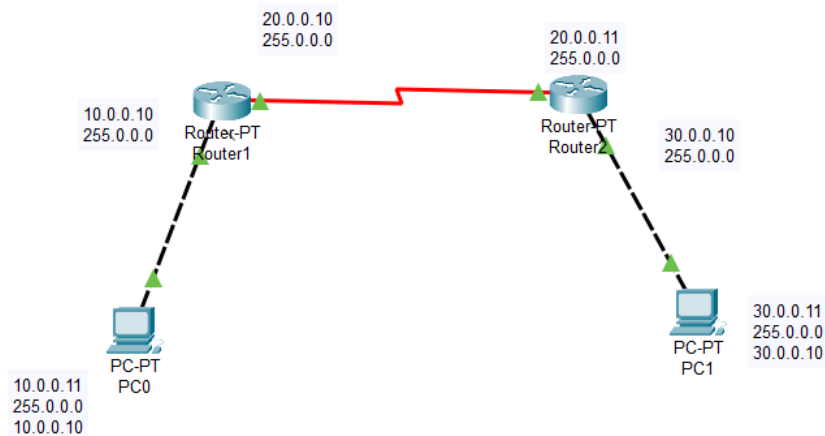
The Routing Information Protocol (RIP) is a distance-vector routing protocol used to exchange routing information between routers in a network. In this lab, we utilized Cisco Packet Tracer to simulate the configuration of RIP on routers to enable automatic routing decisions and communication between networks.

RIP sends the entire routing table every 30 seconds, which can consume a lot of network bandwidth

### Equipment:

- Cisco Packet Tracer software
- Virtual network environment within Cisco Packet Tracer
- Router (PT-router)
- Switches (PT-switch)

### Network Configuration:



### Working procedure:

1. Build the network topology above.
2. Configure IP addresses on the PCs and the routers.

Click Router 1>CLI and run command below,

- enable
- interface FastEthernet0/0
- ip address 10.0.0.10 255.0.0.0
- no shutdown
- exit
  
- interface serial 2/0
- ip address 20.0.0.10 255.0.0.0
- no shutdown
- exit

Click Router 2>CLI and run command below,

- enable
- interface FastEthernet0/0
- ip address 30.0.0.10 255.0.0.0
- no shutdown
- exit
  
- interface serial 2/0
- ip address 20.0.0.11 255.0.0.0
- no shutdown
- exit

### IP configuration on PCs

Click PC->Desktop->IP Configuration. On each PC assign these addresses:

**PC0:** IP address: 10.0.0.11 Subnet mask 255.0.0.0 Default Gateway 10.0.0.10

**PC1:** IP address: 30.0.0.11 Subnet mask 255.0.0.0 Default Gateway 30.0.0.10

### 3. Configure **RIP** on the routers

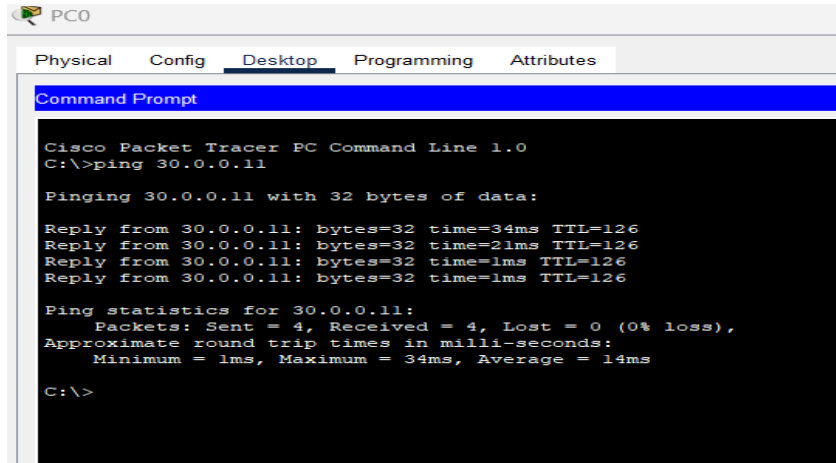
#### **Router1**

- router rip
- network 10.0.0.0
- network 20.0.0.0

## Router2

- router rip
- network 20.0.0.0
- network 30.0.0.0

## Result:



```
PC0
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.11

Pinging 30.0.0.11 with 32 bytes of data:

Reply from 30.0.0.11: bytes=32 time=34ms TTL=126
Reply from 30.0.0.11: bytes=32 time=21ms TTL=126
Reply from 30.0.0.11: bytes=32 time=1ms TTL=126
Reply from 30.0.0.11: bytes=32 time=1ms TTL=126

Ping statistics for 30.0.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 34ms, Average = 14ms

C:\>
```

## Discussion:

The lab effectively demonstrated the configuration and functionality of the Routing Information Protocol (RIP) using Cisco Packet Tracer. RIP is a distance-vector protocol that facilitates routing decisions in smaller networks. By configuring RIP and monitoring routing tables, we confirmed that routers were able to exchange routing information and make informed routing decisions.

## Experiment No: 03

### Experiment Name: VLAN configure on switches and interVLAN Routing in Packet Tracer

#### Theory:

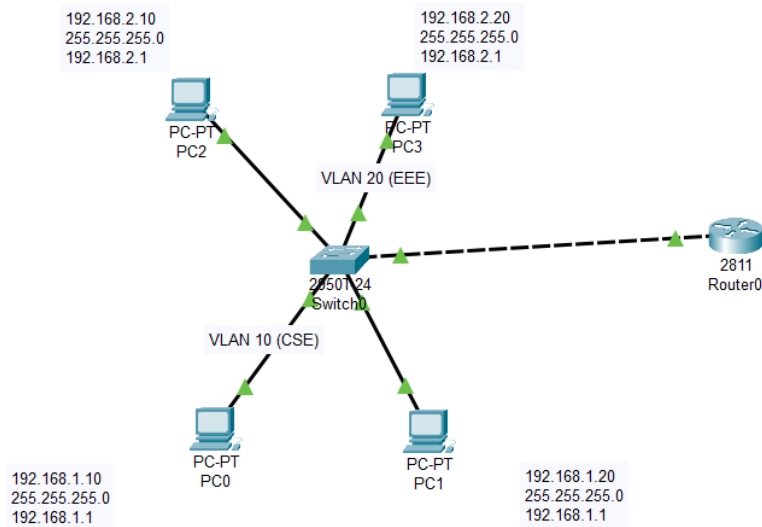
A Virtual LAN (VLAN) is simply a logical LAN, just as its name suggests. VLANs have similar characteristics with those of physical LANs, only that with VLANs, you can logically group hosts even if they are physically located on separate LAN segments. VLAN as a separate subnet or broadcast domain. For this reason, to move packets from one VLAN to another, we have to use a router or a layer 3 switch

VLANs are configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. For this tutorial, we'll configure 2 VLANs on a switch. We'll then proceed and configure a router to enable communication between the two VLANs.

#### Equipment:

- Cisco Packet Tracer software
- Virtual network environment within Cisco Packet Tracer
- Router (PT-router)
- Switches (PT-switch)

#### Network Configuration:



#### Working procedure:

1. In Cisco Packet Tracer, create the network topology as shown above:
2. Create 2 VLANs on the switch: VLAN 10 and VLAN 20. You can give them custom names.

- enable
- configure terminal
- vlan 10
- name cse
- vlan 20
- name eee
- exit

3. Assign switch ports to the VLANs. VLAN is viewed as separate broadcast domain. configure switch interfaces fa 0/1 through fa 0/4 as access ports to connect to our PCs. Here, interfaces fa 0/1 and fa 0/2 are assigned to VLAN 10 while interfaces fa 0/3 and fa 0/4 are assigned to VLAN 20.

- interface FastEthernet0/1
- switchport mode access
- switchport access vlan 10
- exit
  
- interface FastEthernet0/2
- switchport mode access
- switchport access vlan 10
- exit
  
- interface FastEthernet0/3
- switchport mode access
- switchport access vlan 20
- exit
  
- interface FastEthernet0/4
- switchport mode access
- switchport access vlan 20
- exit
  
- interface range fa0/1-4
- switchport mode access
- exit

4. Switch *Interface* fa0/5 will be configured as trunk port, as it will be used to carry traffic between the two VLANs via the router.

- int fa 0/5
- switchport mode trunk

5. Assign static IP addresses to the four PCs which are located in the separate VLANs. PC1 and PC2 fall in VLAN 10 while PC3 and PC4 fall in VLAN 20.

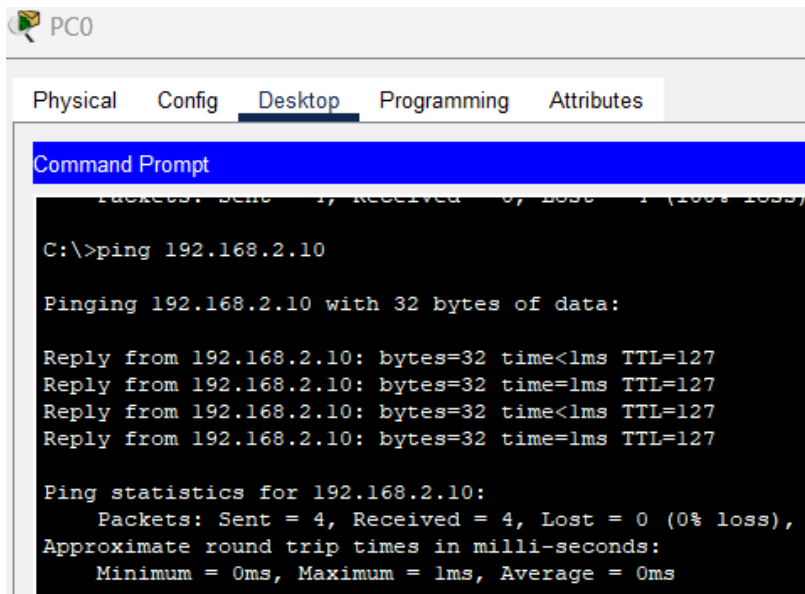


- ⇒ **PC0:** IP address 192.168.1.10 Subnetmask 255.255.255.0 Default gateway 192.168.1.1
- ⇒ **PC1:** IP address 192.168.1.20 Subnetmask 255.255.255.0 Default gateway 192.168.1.1
- ⇒ **PC2:** IP address 192.168.2.10 Subnetmask 255.255.255.0 Default gateway 192.168.2.1
- ⇒ **PC3:** IP address 192.168.2.20 Subnet mask 255.255.255.0 Default gateway 192.168.2.1

## 6. Configure inter-VLAN routing on the router

- enable
- config terminal
- 
- int fa0/0
- no shutdown
- 
- int fa0/0.10
- encapsulation dot1q 10
- ip add 192.168.1.1 255.255.255.0
- 
- int fa0/0.20
- encapsulation dot1q 20
- ip add 192.168.2.1 255.255.255.0

## Result:



## Discussion:

The lab effectively demonstrated the configuration and functionality of Virtual LANs (VLANs) using Cisco Packet Tracer. VLANs allow for logical segmentation of a network to improve performance and security. By creating VLANs and observing communication between devices within and across VLANs, we confirmed the effectiveness of VLAN segmentation.

## Experiment No: 04

### Experiment Name: Static NAT configuration in Packet Tracer

#### Objective:

To provide hands-on experience in setting up and configuring Static NAT, a method of translating private IP addresses to public IP addresses for specific devices.

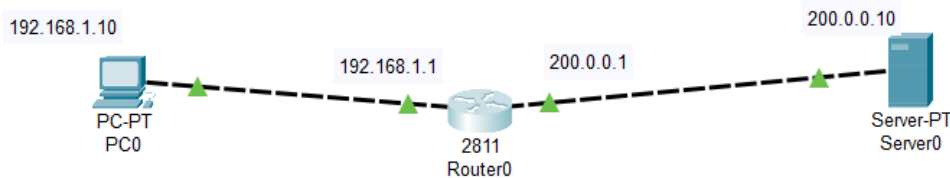
#### Theory:

Network Address Translation (NAT) is a technique used to map private IP addresses to public IP addresses, enabling devices with private addresses to communicate with devices on public networks such as the internet. Static NAT involves configuring a fixed one-to-one mapping between private and public IP addresses. In this lab, we used Cisco Packet Tracer to simulate the configuration of Static NAT and observe its impact on network communication.

#### Equipment:

- Cisco Packet Tracer software
- Virtual network environment within Cisco Packet Tracer
- Router (PT-router)
- Server

#### Network Configuration:



#### Working procedure:

1. First build the network topology according to above network
2. Then configure basic IP addressing on the router, PC and server.

##### Router

- enable
- config terminal

- int fa 0/0
- ip add 192.168.1.1 255.255.255.0
- no shutdown
- exit
  
- int fa 0/1
- ip add 200.0.0.1 255.255.255.0
- no shutdown
- exit

⇒ **PC0:** IP add 192.168.1.10 Subnet mask 255.255.255.0 Default gateway 192.168.1.1

⇒ **Server:** IP add 200.0.0.10 Subnet mask 255.255.255.0 Default gateway 200.0.0.1

Now, to configure static NAT on the router, these are the steps:

- ⇒ Configure private/public IP address mapping using IP NAT inside source static PRIVATE\_ID PUBLIC\_ID command.
- ⇒ Configure the router's inside interface using IP NAT inside command.
- ⇒ Configure the router's outside interface using IP NAT outside command.

Here are the configuration commands:

- ip nat inside source static 192.168.1.10  
155.21.21.10
- int fa0/0
- ip nat inside
- exit
  
- int fa0/1
- ip nat outside

## Result:

```
Router#show ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 155.21.21.10:2     192.168.1.10:2   200.0.0.10:2      200.0.0.10:2
icmp 155.21.21.10:3     192.168.1.10:3   200.0.0.10:3      200.0.0.10:3
icmp 155.21.21.10:4     192.168.1.10:4   200.0.0.10:4      200.0.0.10:4
--- 155.21.21.10       192.168.1.10     ---               ---
Router#
```

## Discussion:

The lab effectively demonstrated the configuration and functionality of Static Network Address Translation (NAT) using Cisco Packet Tracer. Static NAT allows for the translation of private IP addresses to public IP addresses on a one-to-one basis, enabling internal devices to communicate with external networks.

## Experiment No: 05

### Experiment Name: Dynamic NAT configuration in Packet Tracer

#### Objective:

To provide hands-on experience in setting up and configuring Dynamic NAT, a method of translating multiple private IP addresses to a pool of public IP addresses.

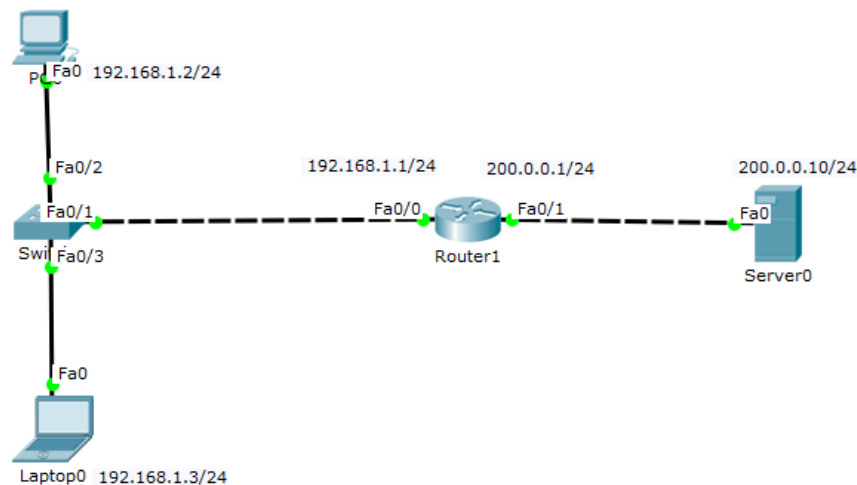
#### Theory:

In dynamic NAT, the router will dynamically pick a public address from the pool. The dynamic mapping entry will stay in the NAT translations as long as the traffic is being exchanged. Otherwise, after a period of no traffic flow, the global IP address will be reused for new translations.

#### Equipment:

- Cisco Packet Tracer software
- Virtual network environment within Cisco Packet Tracer
- Router (PT-router)
- Server

#### Network Configuration:



#### Working procedure:

1. First build the network topology according to above network
2. Then configure basic IP addressing on the router, PC and server.

### **Router**

- **enable**
- **config terminal**
- **int fa 0/0**
- **ip add 192.168.1.1 255.255.255.0**
- **no shutdown**
  
- **exit**
- **int fa 0/1**
- **ip add 200.0.0.1 255.255.255.0**
- **no shutdown**
- **exit**

- ⇒ PC Ip add 192.168.1.2 Default gateway 192.168.1.1(int fa0/0 )
- ⇒ Laptop Ip add 192.168.1.3 Default gateway 192.168.1.1(int fa0/0)
- ⇒ Server IP add 200.0.0.10 Default gateway 200.0.0.1 (int fa0/1)

**Now, to configure Dynamic NAT on the router we'll need to:**

- ⇒ Configure the router's inside address using IP NAT inside command.
- ⇒ Configure the router's outside address using IP NAT outside command.
- ⇒ Create an access list of inside source addresses to be translated.
- ⇒ Configure the pool of global IP addresses using the command IP NAT pool POOL\_NAME FIRST\_IP LAST\_IP netmask SUBNET\_MASK
- ⇒ Enable dynamic NAT on the router using IP Nat inside source list ACL\_NUMBER pool POOL\_NAME

**Here are the dynamic NAT configurations:**

- **int fa 0/0**
- **ip nat inside**
- **exit**
- **int fa 0/1**
- **ip nat outside**
- **exit**
- **access list 1 permit 192.168.1.0 0.0.5**
- **exit**
- **ip nat pool mypool 155.21.21.10 155.21.21.15**  
**netmask 255.255.0.0**
- **exit**
- **ip nat inside source list 1 pool mypool**

## Result:

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local
-----
icmp 155.21.21.10:10   192.168.1.2:10    200.0.0.10:10
200.0.0.10:10
icmp 155.21.21.10:11   192.168.1.2:11    200.0.0.10:11
200.0.0.10:11
icmp 155.21.21.10:12   192.168.1.2:12    200.0.0.10:12
200.0.0.10:12
icmp 155.21.21.10:9    192.168.1.2:9     200.0.0.10:9
200.0.0.10:9
```

## Discussion:

The lab effectively demonstrated the configuration and functionality of Dynamic Network Address Translation (NAT) using Cisco Packet Tracer. Dynamic NAT allows for the sharing of a limited number of public IP addresses among multiple devices within a private network.



## Router

- enable
- config terminal
- int fa 0/0
- ip add 192.168.1.1 255.255.255.0
- no shutdown
  
- exit
- int fa 0/1
- ip add 200.0.0.1 255.255.255.0
- no shutdown
- exit

## Host IP configurations

- ⇒ **Laptop1:** IP add: 192.168.1.2 Default gateway: 192.168.1.1
- ⇒ **Laptop2:** IP add: 192.168.1.3 Default gateway 192.168.1.1
- ⇒ **Internet Server:** IP add: 200.0.0.10/24 Default gateway: 200.0.0.1

## Now, to configure PAT on the router:

- ⇒ Configure an inside interface on the router using IP NAT inside command.
- ⇒ Configure an outside interface on the router using IP NAT outside command.
- ⇒ Create an access-list of private IP addresses to be translated using the command access
- ⇒ Enable PAT on the router using the command IP NAT inside source list ACL\_NUMBER interface INTERFACE\_TYPE overload.

## Here are the PAT configuration commands for the router:

- int fa 0/0
- ip nat inside
- exit
  
- int fa 0/1
- ip nat outside
- exit
  
- access-list 1 permit 192.168.1.2 0.0.0.255
- ip nat inside source list 1 int fa0/1 overload



## Result:

---

```
Router#sh ip nat tra
Pro  Inside global      Inside local      Outside local
-----
icmp 200.0.0.1:5        192.168.1.2:5    200.0.0.10:5
200.0.0.10:5
icmp 200.0.0.1:6        192.168.1.2:6    200.0.0.10:6
200.0.0.10:6
icmp 200.0.0.1:7        192.168.1.2:7    200.0.0.10:7
200.0.0.10:7
icmp 200.0.0.1:8        192.168.1.2:8    200.0.0.10:8
200.0.0.10:8

Router#sh ip nat tra
Pro  Inside global      Inside local      Outside local
-----
icmp 200.0.0.1:1        192.168.1.3:1    200.0.0.10:1
200.0.0.10:1
icmp 200.0.0.1:2        192.168.1.3:2    200.0.0.10:2
200.0.0.10:2
icmp 200.0.0.1:3        192.168.1.3:3    200.0.0.10:3
200.0.0.10:3
icmp 200.0.0.1:4        192.168.1.3:4    200.0.0.10:4
200.0.0.10:4
```

## Discussion:

The lab effectively demonstrated the configuration and functionality of Port Address Translation (PAT) using Cisco Packet Tracer. PAT enables multiple devices within a private network to share a single public IP address, distinguishing connections using unique port numbers.

## Experiment No: 07

### Experiment Name: Basic OSPF Configuration

#### Objective:

To provide hands-on experience in setting up and configuring OSPF, an interior gateway routing protocol, to enable dynamic routing and efficient path selection in a network.

#### Theory:

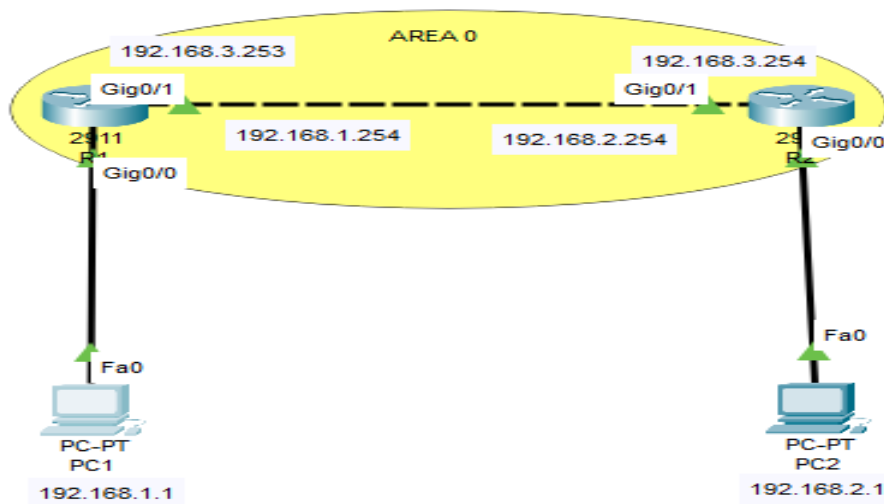
The Open Shortest Path First (OSPF) routing protocol is a dynamic routing protocol that uses link-state information to determine the best path for data transmission in a network.

In the OSPF networks, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router and system in the area generates its link-state advertisements that it receives from all the other routers or systems in the same area and LSAs that itself generates.

#### Equipment:

- Cisco Packet Tracer software
- Virtual network environment within Cisco Packet Tracer
- Router

#### Network Configuration:



#### Working procedure:

1. First build the network topology according to above network
2. Then configure basic IP addressing on the router, PC and server.

### **Router1**

- enable
- configure terminal
- hostname R1
  
- interface GigabitEthernet0/0
- ip address 192.168.1.254 255.255.255.0
- no shutdown
  
- interface g0/1
- ip address 192.168.3.253 255.255.255.0
- no shutdown
- exit

### **Router2**

- enable
- configure terminal
- hostname R2
  
- interface GigabitEthernet0/0
- ip address 192.168.2.254 255.255.255.0
- no shutdown
  
- interface g0/1
- ip address 192.168.3.254 255.255.255.0
- no shutdown
- exit

### **Host IP configurations**

- ⇒ **PC1:** IP add: 192.168.1.1    Default gateway: 192.168.1.254
- ⇒ **PC2:** IP add: 192.168.2.1    Default gateway 192.168.2.254

**Here are the OSPF configuration commands for the router:**

### **Router1**

- router ospf 1
- network 192.168.1.0 0.0.0.255 area 0
- network 192.168.3.0 0.0.0.255 area 0
- exit

### **Router2**

- router ospf 2
- network 192.168..0 0.0.0.255 area 0
- network 192.168.3.0 0.0.0.255 area 0
- exit

### **Result:**

OSPF was successfully configured on the network. Neighbor relationships were established between R1 and R2, as well as R2 and R3. OSPF calculated the shortest paths to all networks and updated the routing tables accordingly.

### **Discussion:**

OSPF is a robust routing protocol that uses a link-state routing algorithm to calculate shortest paths. OSPF configuration involves defining network segments and areas. Neighbor relationships are essential for OSPF to function correctly.