

PRACTICAL NO : 1

Q1: Identify the network address and subnet mask for the IP Address 192.168.1.0

- > Given IP Address is 192.168.1.0
- > The subnet mask is 255.255.255.0 (as it belongs to class C)

In binary form:

11111111.11111111.11111111.00000000

In this the first 24 bits represent the network part & last 8 bits represent host part

Q2: Create 4 subnets:

- > To create 4 subnets we need to borrow two bits from the host part.

$$2^2=4$$

So the new subnet mask is 255.255.255.192

Binary form: 11111111.11111111.11111111.11000000

- > 26 bits for the network part & 6 bits for host part

Total no of subnet 4

Combining 2 or more subnet will give us the Supernet

Total no of usable IP address in each subnet is 64-2 because 1 address is for network and 1 for broadcast.

$$64-2=62 \text{ IP address are usable}$$

CIDR format = Class Inter Domain Representation.

- > new subnet mask 255.255.255.192/26
- > The 1st Subnet is 192.168.1.0/26
- > The 2nd Subnet is 192.168.1.64/26

Subnet 1: 192.168.1.0 -> Network address

usable host address 192.168.1.62/26

Broadcast address 192.168.1.63/26

Subnet 2: 192.168.1.64

1st host address 192.168.1.65

last host address 192.168.1.126/26

broadcast address 192.168.1.127

Subnet 3: 192.168.1.128

1st address is 192.168.1.129

last address is 192.168.1.190

broadcast address 192.168.1.191

Subnet 4: 192.168.1.192

1st host address 192.168.1.193

last address 192.168.1.254

broadcast address 192.168.1.255

Q3. A network Address 192.168.1.0/24 create a subnet mask with subnet 1 consisting of 50 subnet 2 with 20, and subnet 3 with 10.

Since the no of host bit is determine on the IP address... IP address formula to calculate no of bits required to satisfy each subnet IP address is $2^3 \geq n$ of IP address required + 2

while $n=3$ the no of host bits and

addr +2 represent $n/(6)$

Subnet 1 of 50 ip address i.e 2^6 \ge 64 with 62 usable IP addresses we need to 6 host bits. therefore Subnet mask is 255.255.255.192/26

$2^5=32$, 30 usable

Subnet mask is 255.255.255.224/27

$2^4=16$

Subnet mask 255.255.255.240/28

Subnet 1:

Subnet mask: 255.255.255.192/26

network address 192.168.1.0/26

host address 192.168.1.1/26

last host address 192.168.1.30/26

usable IP address 62

Broadcast 192.168.1.63/26

PRACTICAL NO : 2

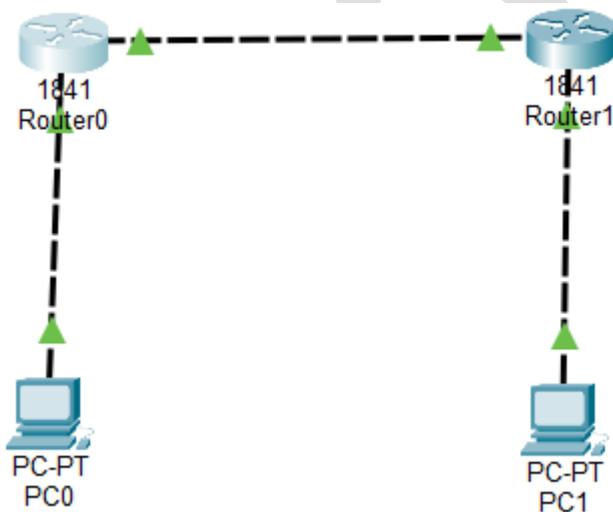
Q. Demonstrate the Static Routing in Packet Tracer.

Aim : To configure and demonstrate static routing between two networks using two routers in Packet Tracer.

Steps :

1. In packet tracer place 2 PCs and 2 Routers.
2. Connect Router0 with PC0 via FastEthernet0/0 using cross-copper cord and Router1 with PC1 via FastEthernet0/0 using cross-copper cord.
3. Connect both routers via FastEthernet0/1 using cross-copper cord.
4. Set the IP address and default gateway of both the PCs in IP configuration of both PCs respectively.

Topology :



Code

Router0 configuration

Router>enable

Router#configure terminal

Router(config)#interface FastEthernet0/0

```
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.2
Router(config)#exit
```

Router1 configuration

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 20.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 40.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
Router(config)#exit
```

PC 0 :

```
C:\>ipconfig  
C:\>ping 10.0.0.1  
C:\>ping 20.0.0.1  
C:\>ping 20.0.0.2  
C:\>ping 40.0.0.1  
C:\>ping 40.0.0.2
```

PC 1:

```
C:\>ipconfig  
C:\>ping 40.0.0.1  
C:\>ping 20.0.0.2  
C:\>ping 20.0.0.1  
C:\>ping 10.0.0.1  
C:\>ping 10.0.0.2
```

OUTPUT**PC 0:**

```
C:\>ping 40.0.0.2  
  
Pinging 40.0.0.2 with 32 bytes of data:  
  
Request timed out.  
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126  
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126  
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126  
  
Ping statistics for 40.0.0.2:  
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC 1:

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

CONCLUSION: The Above Network Topology Has Been Executed Successfully.

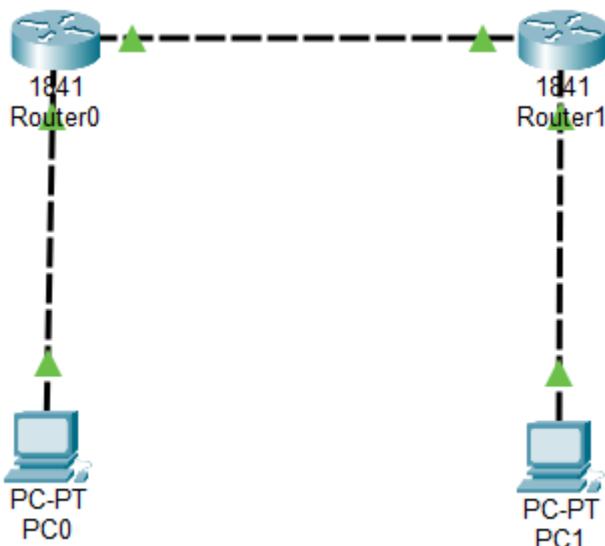
Q. Demonstrate the OSPF Routing in Packet Tracer.

Aim : To configure and demonstrate OSPF dynamic routing protocol between two networks using two routers in Packet Tracer.

Steps :

5. In packet tracer place 2 PCs and 2 Routers.
6. Connect Router0 with PC0 via FastEthernet0/0 using cross-copper cord and Router1 with PC1 via FastEthernet0/0 using cross-copper cord.
7. Connect both routers via FastEthernet0/1 using cross-copper cord.
8. Set the IP address and default gateway of both the PCs in IP configuration of both PCs respectively.
9. Configure OSPF routing protocol on both routers.

Topology :



Code :

Router0 configuration:

```

Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface FastEthernet0/0
  
```

```
Router0(config-if)#ip address 192.168.1.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface FastEthernet0/1
Router0(config-if)#ip address 10.0.0.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#router ospf 1
Router0(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router0(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router0(config-router)#exit
Router0(config)#exit
Router0#copy running-config startup-config
```

Router1 configuration:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface FastEthernet0/1
Router1(config-if)#ip address 10.0.0.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip address 172.16.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#router ospf 1
```

```
Router1(config-router)#network 10.0.0.0 0.0.0.255 area 0  
Router1(config-router)#network 172.16.1.0 0.0.0.255 area 0  
Router1(config-router)#exit  
Router1(config)#exit  
Router1#copy running-config startup-config
```

PC0 configuration :

- IP Address: 192.168.1.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

PC1 Configuration :

- IP Address: 172.16.1.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 172.16.1.1

PC0 Command Prompt :

```
C:\>ipconfig  
C:\>ping 192.168.1.1  
C:\>ping 10.0.0.1  
C:\>ping 10.0.0.2  
C:\>ping 172.16.1.1  
C:\>ping 172.16.1.2
```

PC1 Command Prompt :

```
C:\>ipconfig  
C:\>ping 172.16.1.1  
C:\>ping 10.0.0.2
```

C:\>ping 10.0.0.1
C:\>ping 192.168.1.1
C:\>ping 192.168.1.2

Router Verification Commands:

Router0#show ip route
Router0#show ip ospf neighbour
Router0#show ip ospf database
Router1#show ip route
Router1#show ip ospf neighbour

OUTPUT:

PC0 OUTPUT :

```
C:\>PING 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.2: bytes=32 time<1ms TTL=126
Reply from 172.16.1.2: bytes=32 time<1ms TTL=126
Reply from 172.16.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1 OUTPUT :

```
C:\>PING 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

OSPF Neighbour Output:

```
Router#show ip ospf neighbor

Neighbor ID      Pri   State            Dead Time     Address          Interface
172.16.1.1       1     FULL/BDR        00:00:34     10.0.0.2        FastEthernet0/1
```

IP Route Output:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
C        10.0.0.0 is directly connected, FastEthernet0/1
O        172.16.0.0/16 [110/2] via 10.0.0.2, 00:07:45, FastEthernet0/1
C        192.168.1.0/24 is directly connected, FastEthernet0/0
```

Conclusion : The Above Network Topology Has Been Executed Successfully.

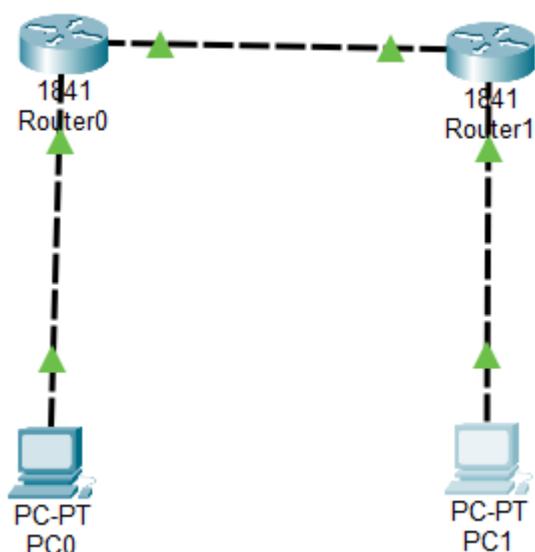
Q. Demonstrate the RIP Routing in Packet Tracer.

Aim: To configure and demonstrate RIP dynamic routing protocol between two networks using two routers in Packet Tracer.

Steps:

1. In packet tracer place 2 PCs and 2 Routers.
2. Connect Router0 with PC0 via FastEthernet0/0 using cross-copper cord and Router1 with PC1 via FastEthernet0/0 using cross-copper cord.
3. Connect both routers via FastEthernet0/1 using cross-copper cord.
4. Set the IP address and default gateway of both the PCs in IP configuration of both PCs respectively.
5. Configure RIP version 2 routing protocol on both routers.

Topology :



Code:**Router0 Configuration:**

```
Router>enable  
Router#configure terminal  
Router(config)#hostname Router0  
Router0(config)#interface FastEthernet0/0  
Router0(config-if)#ip address 192.168.10.1 255.255.255.0  
Router0(config-if)#no shutdown  
Router0(config-if)#exit  
Router0(config)#interface FastEthernet0/1  
Router0(config-if)#ip address 10.10.10.1 255.255.255.0  
Router0(config-if)#no shutdown  
Router0(config-if)#exit  
Router0(config)#router rip  
Router0(config-router)#version 2  
Router0(config-router)#network 192.168.10.0  
Router0(config-router)#network 10.10.10.0  
Router0(config-router)#no auto-summary  
Router0(config-router)#exit  
Router0(config)#exit  
Router0#copy running-config startup-config
```

Router1 configuration:

```
Router>enable  
Router#configure terminal  
Router(config)#hostname Router1  
Router1(config)#interface FastEthernet0/1
```

```
Router1(config-if)#ip address 10.10.10.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip address 172.16.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 10.10.10.0
Router1(config-router)#network 172.16.20.0
Router1(config-router)#no auto-summary
Router1(config-router)#exit
Router1(config)#exit
Router1#copy running-config startup-config
```

PC0 Configuration:

- IP Address: 192.168.10.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.1

PC1 Configuration:

- IP Address: 172.16.20.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 172.16.20.1

PC0 Command Prompt :

C:\>ipconfig

C:\>ping 192.168.10.1

```
C:\>ping 10.10.10.1  
C:\>ping 10.10.10.2  
C:\>ping 172.16.20.1  
C:\>ping 172.16.20.2
```

PC0 Command Prompt :

```
C:\>ipconfig  
C:\>ping 172.16.20.1  
C:\>ping 10.10.10.2  
C:\>ping 10.10.10.1  
C:\>ping 192.168.10.1  
C:\>ping 192.168.10.2
```

Router Verification Commands:

```
Router0#show ip route  
Router0#show ip protocols  
Router0#show ip rip database  
Router1#show ip route  
Router1#show ip protocols
```

OUTPUT :

PC0 OUTPUT :

```
C:\>ping 172.16.20.2

Pinging 172.16.20.2 with 32 bytes of data:

Reply from 172.16.20.2: bytes=32 time=1ms TTL=126
Reply from 172.16.20.2: bytes=32 time<1ms TTL=126
Reply from 172.16.20.2: bytes=32 time<1ms TTL=126
Reply from 172.16.20.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC1 OUTPUT :

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

IP ROUTE OUTPUT :

```

router0#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
C          10.10.10.0 is directly connected, FastEthernet0/1
      172.16.0.0/24 is subnetted, 1 subnets
R          172.16.20.0 [120/1] via 10.10.10.2, 00:00:13, FastEthernet0/1
C          192.168.10.0/24 is directly connected, FastEthernet0/0

```

RIP PROTOCOL OUTPUT :

```

router0#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 9 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
    Interface          Send   Recv   Triggered RIP   Key-chain
    FastEthernet0/0     22
    FastEthernet0/1     22
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.10.0
  Passive Interface(s):
  Routing Information Sources:
    Gateway          Distance      Last Update
    10.10.10.2        120          00:00:02
  Distance: (default is 120)

```

CONCLUSION : The above network topology has been executed successfully

PRACTICAL NO : 3

Q. Demonstrate DHCP Server in Cisco Packet Tracer.

Aim: To configure a router as DHCP server to automatically assign IP addresses to clients.

Devices Required:

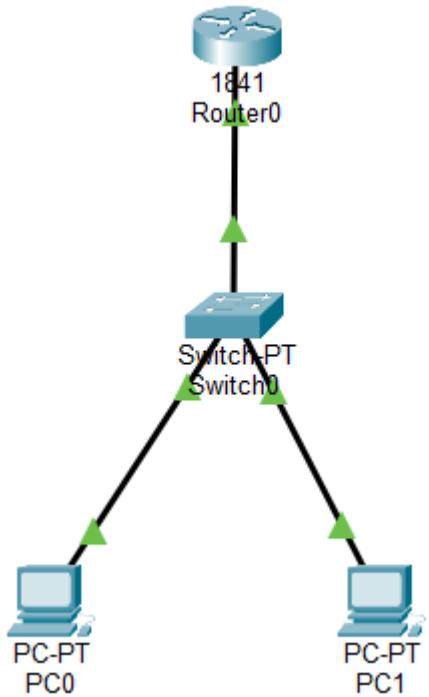
- 1 Router (1841 or any model)
- 1 Switch (2960 or any model)
- 2-4 PCs

Connections:

- Router FastEthernet0/0 to Switch FastEthernet0/1 (Straight-through cable)
- PC0 to Switch FastEthernet0/2 (Straight-through cable)

- PC1 to Switch FastEthernet0/3 (Straight-through cable)

Topology :



Router Configuration Commands:

Router>enable

Router#configure terminal

Router(config)#hostname DHCP-Router

DHCP-Router(config)#interface FastEthernet0/0

DHCP-Router(config-if)#ip address 10.0.0.1 255.255.255.0

DHCP-Router(config-if)#no shutdown

DHCP-Router(config-if)#exit

DHCP Pool Configuration:

DHCP-Router(config)#ip dhcp pool STUDENT_NETWORK

DHCP-Router(dhcp-config)#network 10.0.0.0 255.255.255.0

```
DHCP-Router(dhcp-config)#default-router 10.0.0.1  
DHCP-Router(dhcp-config)#dns-server 8.8.8.8  
DHCP-Router(dhcp-config)#exit
```

Exclude IP Addresses:

```
DHCP-Router(config)#ip dhcp excluded-address 10.0.0.1 10.0.0.10  
DHCP-Router(config)#exit  
DHCP-Router#copy running-config startup-config
```

PC Configuration:

- On each PC, go to **Desktop** tab → **IP Configuration**
- Select **DHCP** option

Verification command :

On Router:

```
DHCP-Router#show ip dhcp pool  
DHCP-Router#show ip dhcp binding  
DHCP-Router#show ip interface brief
```

On both PCs (Command Prompt):

```
C:\>ipconfig  
C:\>ipconfig /all  
C:\>ping 10.0.0.1
```

Output Results:

PC0 - ipconfig:

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: collegelab.local
Link-local IPv6 Address....: FE80::250:FFF:FEBC:55D2
IPv6 Address.....: ::
IPv4 Address.....: 10.0.0.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                           10.0.0.1
```

PC1 - ipconfig:

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: collegelab.local
Link-local IPv6 Address....: FE80::20C:85FF:FE14:5DE7
IPv6 Address.....: ::
IPv4 Address.....: 10.0.0.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                           10.0.0.1
```

Router - DHCP Bindings (WORKING COMMAND):

IP address	Client-ID/ Hardware address	Lease expiration	Type
10.0.0.11	0050.0FBC.55D2	--	Automatic
10.0.0.12	000C.8514.5DE7	--	Automatic

Router - DHCP Pool Status (WORKING COMMAND):

```
DHCP-router#show ip dhcp pool

Pool STUDENT_NETWORK :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                 : 254
Leased addresses                : 2
Excluded addresses              : 1
Pending event                   : none

1 subnet is currently in the pool
Current index          IP address range           Leased/Excluded/Total
10.0.0.1               10.0.0.1       - 10.0.0.254        2 / 1 / 254
```

Router - Interface Status:

```
DHCP-router#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    10.0.0.1       YES manual up        up
FastEthernet0/1    unassigned     YES unset administratively down down
Serial0/0/0        unassigned     YES unset administratively down down
Serial0/0/1        unassigned     YES unset administratively down down
Vlan1             unassigned     YES unset administratively down down
-----
```

Connectivity Test - PC0 to Router:

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Conclusion: The DHCP server has been successfully configured on the router using commands compatible with Cisco Packet Tracer.

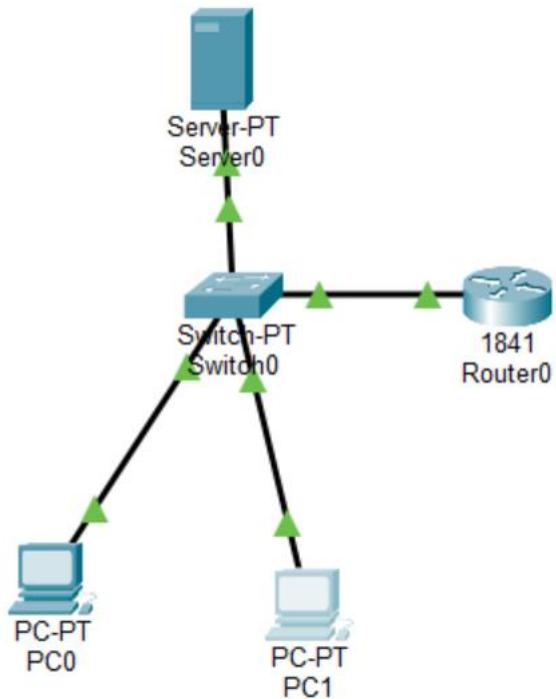
Q. Demonstrate DNS Server in Packet Tracer.

Aim: To configure a DNS server to resolve domain names to IP addresses and test name resolution in the network.

Devices Needed:

- 1 Server (DNS Server)
- 1 Router
- 1 Switch
- 2 PCs (Clients)

Topology:

**Code:****Configure DNS Records:**

Name: www.company.com

Type: A Record

Address: 192.168.1.5 # Points to Server itself

-> Add

Name: ftp.company.com

Type: A Record

Address: 192.168.1.5 # Points to Server itself

-> Add

Name: mail.company.com

Type: A Record

Address: 192.168.1.5 # Points to Server itself

-> Add

Server IP Configuration:

- IP Address: 192.168.1.5
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- DNS Server: 192.168.1.5

Router Configuration:

Router>enable

Router#configure terminal

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#exit

Router#copy running-config startup-config

PC0 Configuration:

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- DNS Server: 192.168.1.5

PC1 Configuration:

- IP Address: 192.168.1.11
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- DNS Server: 192.168.1.5

In PC Command Prompt**PC0:**

C:\>nslookup www.company.com

C:\>nslookup ftp.company.com

C:\>nslookup mail.company.com

C:\>ping www.company.com

C:\>ping ftp.company.com

PC1:

C:\>nslookup www.company.com

C:\>nslookup mail.company.com

C:\>ping www.company.com

C:\>ping mail.company.com

Output:

PC0 nslookup Results:

C:\>nslookup www.company.com

```
C:\>nslookup www.company.com
Server: [192.168.1.5]
Address: 192.168.1.5

Non-authoritative answer:
Name: www.company.com
Address: 192.168.1.5
```

C:\>nslookup ftp.company.com

```
C:\>nslookup ftp.company.com
Server: [192.168.1.5]
Address: 192.168.1.5

Non-authoritative answer:
Name: ftp.company.com
Address: 192.168.1.5
```

C:\>nslookup mail.company.com

```
C:\>nslookup mail.company.com

Server: [192.168.1.5]
Address: 192.168.1.5

Non-authoritative answer:
Name: mail.company.com
Address: 192.168.1.5
```

PC0 Ping Results:

C:\>ping www.company.com

```
C:\>ping www.company.com

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC1 nslookup Results:

C:\>nslookup mail.company.com

```
C:\>nslookup mail.company.com

Server: [192.168.1.5]
Address: 192.168.1.5

Non-authoritative answer:
Name: mail.company.com
Address: 192.168.1.5
```

C:\>nslookup www.company.com

```
C:\>nslookup www.company.com

Server: [192.168.1.5]
Address: 192.168.1.5

Non-authoritative answer:
Name: www.company.com
Address: 192.168.1.5
```

PC2 Ping Results:

C:\>ping mail.company.com

```
C:\>ping mail.company.com

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

CONCLUSION: The DNS server has been configured successfully.

Q. Demonstrate FTP Server in Packet Tracer.

Aim: To configure an FTP server and test file transfer between server and clients in the network.

Devices Needed:

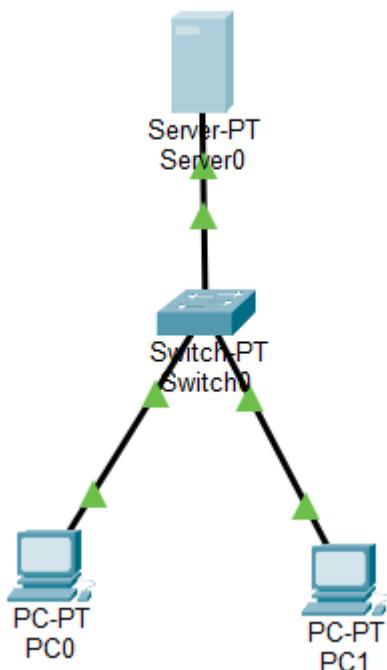
10. 1 Server (FTP Server)
11. 1 Switch

12. 2 PCs (FTP Clients)

Connection :

- Connect all devices to the switch using copper straight-through cables

Topology:



Code:

Server Configuration (FTP):

- Click on **Server** → **Services** tab → **FTP**
- **FTP Server Settings:**
 - FTP Service: **ON**
- **Add User Account:**
 - Username: **admin**
 - Password: **cisco**
 - Check all permissions: **Read/Write/List/Delete/Rename**
 - Click **Add**

Server IP Configuration:

- IP Address: 192.168.1.5

- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

PC1 Configuration:

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

PC2 Configuration:

- IP Address: 192.168.1.11
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

Create Test File on PC1

- Click on **PC1→Desktop tab →Text Editor**
- Type: This is a test file for FTP transfer
- Save as: upload_test.txt

Verification: In PC Command Prompt

PC1 FTP Commands:

```
C:\>ftp 192.168.1.5
```

```
Username: admin
```

```
Password: cisco
```

```
ftp> dir
```

```
ftp> put upload_test.txt
```

```
ftp> dir
```

```
ftp> get welcome.txt
```

```
ftp> delete notes.txt
```

```
ftp> quit
```

PC2 FTP Commands:

```
C:\>ftp 192.168.1.5
```

Username: admin

Password: cisco

```
ftp> dir
```

```
ftp> get upload_test.txt
```

```
ftp> rename upload_test.txt downloaded_file.txt
```

```
ftp> dir
```

```
ftp> quit
```

Ping Test (Both PCs):

```
C:\>ping 192.168.1.5
```

Output:

PC1 FTP Session:

```
C:\>ftp 192.168.1.5
Trying to connect...192.168.1.5
Connected to 192.168.1.5
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:*****
230- Logged in
(passive mode On)
ftp>dir
```

33	:	notes_text.txt	24
34	:	pt1000-i-mz.122-28.bin	5571584
35	:	pt3000-i6q4l2-mz.121-22.EA4.bin	3117390
36	:	upload_text.txt	37
37	:	welcome_text.txt	26

```
ftp>put upload_text.txt

Writing file upload_text.txt to 192.168.1.5:
File transfer in progress...

[Transfer complete - 36 bytes]

36 bytes copied in 0.021 secs (1714 bytes/sec)
ftp>put welcome.txt
```

```
ftp>dir

Listing /ftp directory from 192.168.1.5:
0   : asa842-k8.bin                               5571584
1   : asa923-k8.bin                               30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin    33591768
3   : c1841-ipbase-mz.123-14.T7.bin              13832032
4   : c1841-ipbasek9-mz.124-12.bin               16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin    33591768
6   : c2600-advipservicesk9-mz.124-15.T1.bin    33591768
7   : c2600-i-mz.122-28.bin                      5571584
8   : c2600-ipbasek9-mz.124-8.bin                13169700
9   : c2800nm-advipservicesk9-mz.124-15.T1.bin  50938004
10  : c2800nm-advipservicesk9-mz.151-4.M4.bin   33591768
11  : c2800nm-ipbase-mz.123-14.T7.bin          5571584
12  : c2800nm-ipbasek9-mz.124-8.bin            15522644
13  : c2900-universalk9-mz.SPA.155-3.M4a.bin   33591768
14  : c2950-i6q412-mz.121-22.EA4.bin           3058048
15  : c2950-i6q412-mz.121-22.EA8.bin           3117390
16  : c2960-lanbase-mz.122-25.FX.bin          4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin         4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin         4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin  8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin   10713279
21  : c800-universalk9-mz.SPA.152-4.M4.bin    33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin   83029236
23  : cat3k_caa-universalk9.16.03.02.SPA.bin  505532849
24  : cgr1000-universalk9-mz.SPA.154-2.CG     159487552
25  : cgr1000-universalk9-mz.SPA.156-3.CG     184530138
26  : ie9k_iosxe.17.09.04.SPA.bin             596133776
27  : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
28  : ir800-universalk9-mz.SPA.155-3.M        61750062
29  : ir800-universalk9-mz.SPA.156-3.M        63753767
30  : ir800_yocto-1.7.2.tar                  2877440
31  : ir800_yocto-1.7.2_python-2.7.3.tar    6912000
32  : ir8340-mono-universalk9_iot.17.08.01a.SPA.pkg 685645824
33  : notes_text.txt                         24
34  : pt1000-i-mz.122-28.bin                 5571584
35  : pt3000-i6q412-mz.121-22.EA4.bin       3117390
36  : upload_text.txt                       36
37  : welcome.txt                          25
38  : welcome_text.txt                     26
```

```
ftp>get welcome.txt

Reading file welcome.txt from 192.168.1.5:
File transfer in progress...

[Transfer complete - 25 bytes]

25 bytes copied in 0 secs
```

```
ftp>delete notes.txt
Deleting file notes.txt from 192.168.1.5: ftp>
[Deleted file notes.txt successfully ]
```

```
ftp>quit
221- Service closing control connection.
```

Ping Test Results:

```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC2 FTP Session:

```
C:\>ftp 192.168.1.5
Trying to connect...192.168.1.5
Connected to 192.168.1.5
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:*****
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.1.5:
```

31 : ir800_yocto-1.7.2_python-2.7.3.tar	6912000
32 : ir8340-mono-universalk9_iot.17.08.01a.SPA.pkg	685645824
33 : notes_text.txt	24
34 : pt1000-i-mz.122-28.bin	5571584
35 : pt3000-i6q4l2-mz.121-22.EA4.bin	3117390
36 : upload_text.txt	36
37 : welcome.txt	25
38 : welcome_	26

```

ftp>get upload_text.txt
Reading file upload_text.txt from 192.168.1.5:
File transfer in progress...
[Transfer complete - 37 bytes]
37 bytes copied in 0 secs

ftp>rename upload_text.txt downloaded_text.txt
Renaming upload_text.txt
ftp>
[OK Renamed file successfully from upload_text.txt to downloaded_text.txt]

ftp>dir
Listing /ftp directory from 192.168.1.5:
0   : asa842-k8.bin                         5571584
1   : asa923-k8.bin                         30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3   : c1841-ipbase-mz.123-14.T7.bin          13832032

25  : cgr1000-universalk9-mz.SPA.156-3.CG      184530138
26  : downloaded_text.txt                      37
27  : ie9k_iosxe.17.09.04.SPA.bin            596133776
28  : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
29  : ir800-universalk9-mz.SPA.155-3.M        61750062
30  : ir800-universalk9-mz.SPA.156-3.M        63753767
31  : ir800_yocto-1.7.2.tar                  2877440
32  : ir800_yocto-1.7.2_python-2.7.3.tar    6912000
33  : ir8340-mono-universalk9_iot.17.08.01a.SPA.pkg 685645824
34  : notes_text.txt                          24
35  : pt1000-i-mz.122-28.bin                5571584
36  : pt3000-i6q4l2-mz.121-22.EA4.bin       3117390
37  : welcome.txt                           25
38  : welcome_text.txt                     26

ftp>quit
221- Service closing control connection.

```

Ping Test Results:

```

C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

CONCLUSION: The FTP server has been configured successfully.

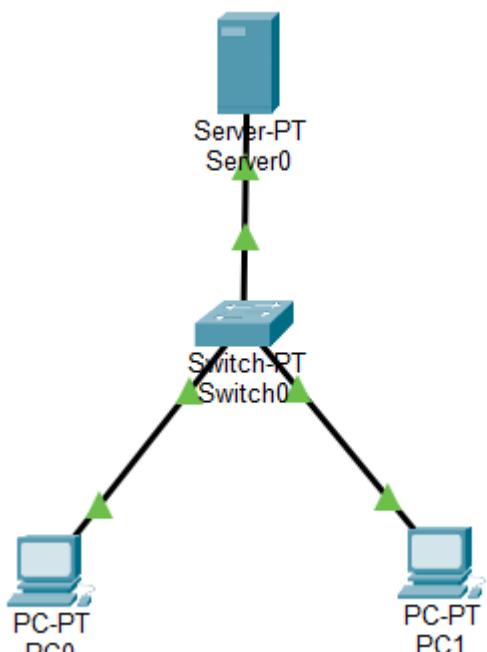
Q. Demonstrate HTTP Server in Packet Tracer.

Aim: To configure a web server and test web page access from clients using web browsers.

Steps:

- In packet tracer place 1 Server-PT and 2 PC-PT and 1 Switch.
- Connect Server-PT with Switch via FastEthernet0 using straight-through copper cord.
- Connect PC-PT0 and PC-PT1 with Switch via FastEthernet0 using straight-through cords.
- Set the IP address of Server-PT and both PCs in IP configuration.
- Configure HTTP service on Server-PT and create web pages.
- Test web access from both PCs.

Topology:



Code:

Server-PT Configuration:

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

HTTP Service Configuration:

- HTTP Service: ON
- Created web pages: index.html, about.html, courses.html

Web Page Code:**index.html:**

html

```
<!DOCTYPE html>

<html>
<head>
<title>My College Website</title>
</head>
<body>
<h1>Welcome to College Server</h1>
<p>This website is hosted on Server-PT in Packet Tracer.</p>
<a href="about.html">About College</a> |
<a href="courses.html">Courses</a>
</body>
</html>
```

about.html:

html

```
<!DOCTYPE html>

<html>
<head>
<title>About Our College</title>
</head>
<body>
```

```

<h1>About Our Institution</h1>
<p>Established in 1990, we provide quality technical education.</p>
<p><b>Departments:</b> Computer, IT, Electronics, Mechanical</p>
<a href="index.html">Home</a> |
<a href="courses.html">Our Courses</a>
</body>
</html>

```

courses.html:

```

<!DOCTYPE html>
<html>
<head>
<title>College Courses</title>
</head>
<body>
<h1>Available Courses</h1>
<ul>
<li>Computer Engineering</li>
<li>Information Technology</li>
<li>Electronics & Telecommunication</li>
<li>Mechanical Engineering</li>
</ul>
<a href="index.html">Home</a> |
<a href="about.html">About College</a>
</body></html>

```

PC-PT0 Configuration:

- IP Address: 192.168.1.20

- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

PC-PT1 Configuration:

- IP Address: 192.168.1.30
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

Verification: In Both PCs Web Browser

PC-PT0:

- Open Web Browser
- Enter URL: <http://192.168.1.10>
- Enter URL: <http://192.168.1.10/about.html>
- Enter URL: <http://192.168.1.10/courses.html>

PC-PT1:

- Open Web Browser
- Enter URL: <http://192.168.1.10>
- Enter URL: <http://192.168.1.10/about.html>
- Enter URL: <http://192.168.1.10/courses.html>

Connectivity Test:

C:\>ping 192.168.1.10

Output:

Ping Test Results:

PC 0 :

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=8ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

PC1 :

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

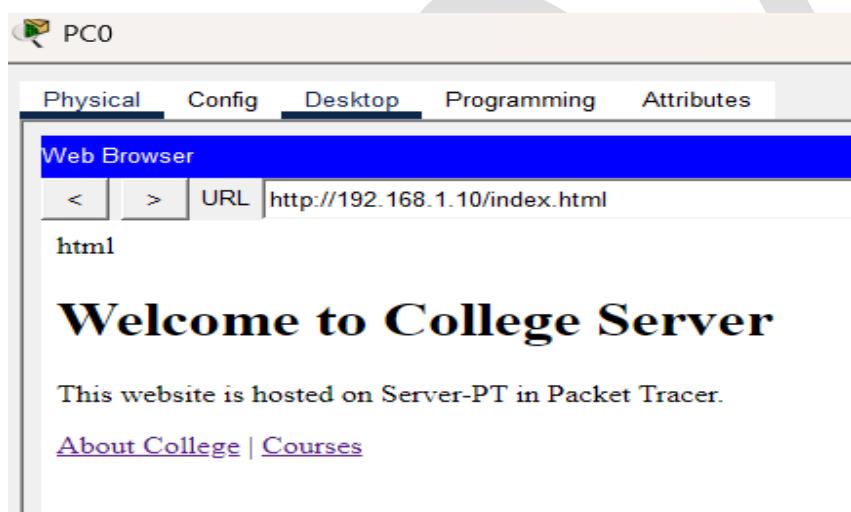
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Web Browser Output:

Homepage (<http://192.168.1.10>):

PC 0 :



PC 1: About Page (<http://192.168.1.10/about.html>):**PC0 :**

The screenshot shows a software interface for managing computer configurations. At the top, there's a toolbar with tabs: Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is currently selected, indicated by a blue background. Below the toolbar, a blue header bar displays the text 'Web Browser'. Underneath this, there's a URL input field containing the address 'http://192.168.1.10/about.html'. The main content area contains the following text:

About Our Institution

Established in 1990, we provide quality technical education.

Departments: Computer, IT, Electronics, Mechanical

[Home](#) | [Our Courses](#)

Pc1 :

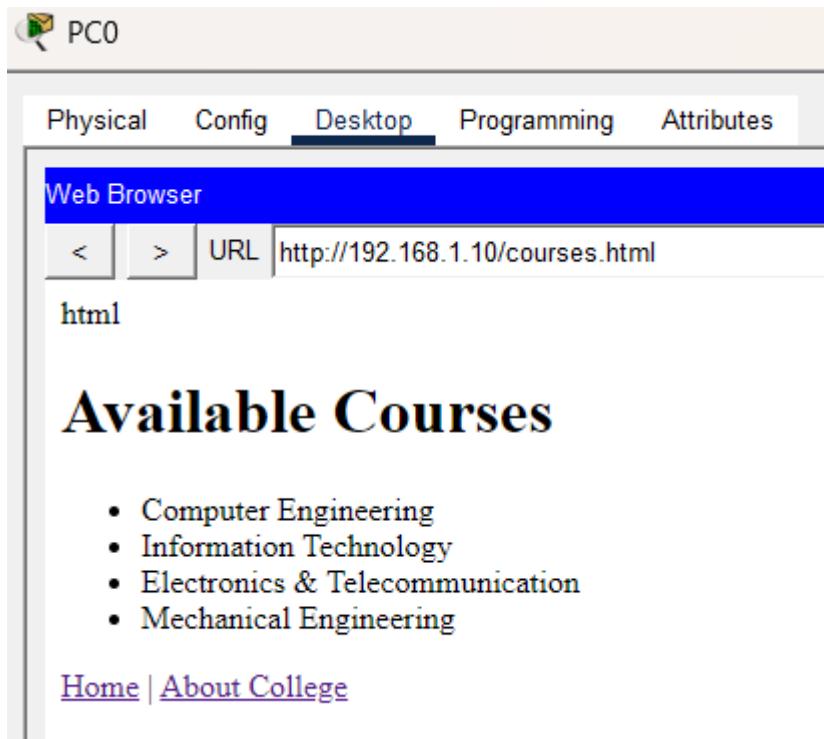
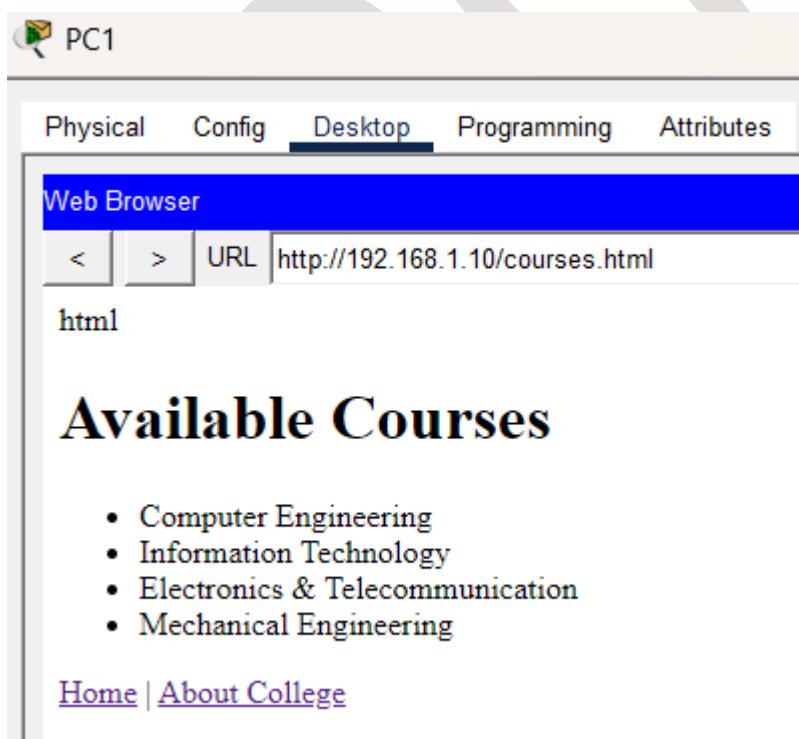
The screenshot shows a software interface for managing computer configurations, identical to PC0. The 'Desktop' tab is selected. A blue header bar displays 'Web Browser'. The URL input field shows 'http://192.168.1.10/about.html'. The main content area contains the following text:

About Our Institution

Established in 1990, we provide quality technical education.

Departments: Computer, IT, Electronics, Mechanical

[Home](#) | [Our Courses](#)

Courses Page (<http://192.168.1.10/courses.html>):**PC0 :****PC1 :**

CONCLUSION: The HTTP web server has been configured successfully.

Q. Demonstrate Telnet in Packet Tracer.

Aim: To configure Telnet on routers to enable remote administration and test remote connectivity between devices.

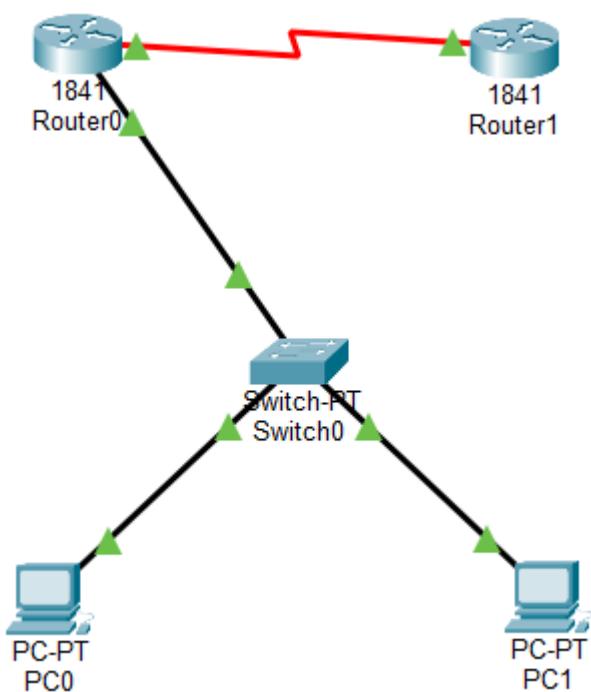
Devices Needed:

13. 2 Routers
14. 1 Switch
15. 2 PCs (Telnet Clients)

Connection Guide:

- Connect Router0 and Router1 via serial cable (Serial DCE)
- Connect Router0 to Switch via FastEthernet
- Connect PCs to Switch via copper straight-through cables

Topology:



Code:

Router1 Configuration:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface FastEthernet0/0
Router0(config-if)#ip address 192.168.1.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface Serial0/0/0
Router0(config-if)#ip address 10.0.0.1 255.255.255.252
Router0(config-if)#clock rate 64000
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#line vty 0 4
Router0(config-line)#password cisco
Router0(config-line)#login
Router0(config-line)#exit
Router0(config)#enable secret class
Router0(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
Router0(config)#exit
Router0#copy running-config startup-config
```

Router2 Configuration:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface Serial0/0/0
Router1(config-if)#ip address 10.0.0.2 255.255.255.252
Router1(config-if)#no shutdown
Router1(config-if)#exit
```

```
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip address 172.16.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#line vty 0 4
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#exit
Router1(config)#enable secret class
Router1(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
Router1(config)#exit
Router1#copy running-config startup-config
```

PC1 Configuration:

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

PC2 Configuration:

- IP Address: 192.168.1.11
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

Verification: In PC Command Prompt

PC1 Telnet Tests:

C:\>ping 192.168.1.1

C:\>ping 10.0.0.2

C:\>ping 172.16.1.1

C:\>telnet 192.168.1.1

C:\>telnet 10.0.0.2

PC2 Telnet Tests:

C:\>ping 192.168.1.1

C:\>ping 10.0.0.2

C:\>ping 172.16.1.1

C:\>telnet 192.168.1.1

C:\>telnet 172.16.1.1

Router Verification Commands:

Router#show users

Router#show line vty 0

Router#show running-config | include vty 0

Output:

PC1 Telnet to Router1: telnet 192.168.1.1

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Password:
router0>enable
Password:
router0#show users
  Line      User      Host(s)          Idle      Location
*196  vty 0            idle           00:00:00  192.168.1.10

  Interface    User          Mode          Idle      Peer Address
router0#exit

[Connection to 192.168.1.1 closed by foreign host]
```

PC1 Telnet to Router2:

C:\>telnet 10.0.0.2

```
C:\>telnet 10.0.0.2
Trying 10.0.0.2 ...Open

User Access Verification

Password:
router1>enable
Password:
router1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    172.16.1.1    YES manual down        down
FastEthernet0/1    unassigned     YES unset administratively down down
Serial0/0/0        10.0.0.2     YES manual up         up
Serial0/0/1        unassigned     YES unset administratively down down
Vlan1             unassigned     YES unset administratively down down
router1#
[Connection to 10.0.0.2 closed by foreign host]
```

PC2 Telnet to Router1:

C:\>telnet 192.168.1.1

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
router0>enable
Password:
router0#show running-config | include vty
line vty 0 4
router0#show running-config | include vty
line vty 0 4
router0#exit
[Connection to 192.168.1.1 closed by foreign host]
```

Ping Test Results:

```
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 10.0.0.2: Destination host unreachable.

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Router Show Users Output:

```
router0#show users
  Line      User      Host(s)          Idle      Location
*196 vty 0            idle           00:00:00 192.168.1.10

  Interface   User      Mode      Idle      Peer Address
router0#exit
```

Conclusion: Telnet has been configured successfully on both routers.

PRACTICAL NO : 4

STUDY OF CRYPTOGRAPHY SUBSTITUTION TECHNIQUES

AIM: To study and implement Substitution Techniques in Cryptography using Python to perform encryption and decryption of a message

PROGRAM:

```
def encrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            base = 'A' if char.isupper() else 'a'
            result += chr((ord(char) - ord(base) + shift) % 26 + ord(base))
        else:
            result += char
    return result

def decrypt(text, shift):
    return encrypt(text, -shift)

# input
text = input("Enter plain text: ")
shift = int(input("Enter shift value: "))

encrypted_text = encrypt(text, shift)
print("Encrypted Text:", encrypted_text)
```

```
decrypted_text = decrypt(encrypted_text, shift)
print("Decrypted Text:", decrypted_text)
```

OUTPUT:

```
... Enter plain text: HELLO
Enter shift value: 3
Encrypted Text: KHOOR
Decrypted Text: HELLO
```

CONCLUSION: The Above Program Has Been Executed Successfully.

PRACTICAL NO : 5
STUDY OF SYMMETRIC KEY

1. DES

AIM: To write a program in python to demonstrate DES

PROGRAM:

```
from Crypto.Cipher import DES  
from Crypto.Util.Padding import pad, unpad  
  
key = b'12345678'  
cipher = DES.new(key, DES.MODE_ECB)  
  
plaintext = input("Enter message: ")  
padded_text = pad(plaintext.encode(), DES.block_size)  
encrypted_text = cipher.encrypt(padded_text)  
print("Encrypted Text:", encrypted_text)  
decrypted_text = unpad(cipher.decrypt(encrypted_text), DES.block_size)  
print("Decrypted Text:", decrypted_text.decode())
```

OUTPUT:

```
Enter message: HELLO WORLD
Encrypted Text: b'\xf9\xd8\xc2\\xabtr\xf9K\xfe\x97\x93\x94~\xc9'
Decrypted Text: HELLO WORLD
```

2. AES

AIM: To write a program in python to demonstrate AES

PROGRAM:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
key = b'thisismysecretky'
cipher = AES.new(key, AES.MODE_ECB)

plaintext = input("Enter message: ")
padded_text = pad(plaintext.encode(), AES.block_size)
encrypted_text = cipher.encrypt(padded_text)
print("Encrypted Text:", encrypted_text)

decrypted_text = unpad(cipher.decrypt(encrypted_text), AES.block_size)
print("Decrypted Text:", decrypted_text.decode())
```

OUTPUT:

```
... Enter message: SECRET MESSAGE
Encrypted Text: b'o\xef\xaf4\x7f\x9fg\xb9\x84pQ\r\x9e&/m'
Decrypted Text: SECRET MESSAGE
```

CONCLUSION: The Above Program Has Been Executed Successfully.

PRACTICAL NO : 6
STUDY OF ASYMMETRIC KEY

1. DH

AIM: To write a python program to demonstrate DH.

PROGRAM:

```
P = 23 # prime number
G = 9 # primitive root
# Private keys
a = 4 # Alice's private key
b = 3 # Bob's private key
A = (G ** a) % P
B = (G ** b) % P
# Generate shared secret keys
key1 = (B ** a) % P # Alice's key
key2 = (A ** b) % P # Bob's key
print("Publicly Shared Values:")
print("P:", P, "G:", G)
print("Public Key of Alice (A):", A)
print("Public Key of Bob (B):", B)
```

```
print("\nSecret Keys:")
print("Alice's Secret Key:", key1)
print("Bob's Secret Key:", key2)
```

OUTPUT:

```
... Publicly Shared Values:
P: 23 G: 9
Public Key of Alice (A): 6
Public Key of Bob (B): 16

Secret Keys:
Alice's Secret Key: 9
Bob's Secret Key: 9
```

2. RSA

AIM: To write a python program to demonstrate RSA.

PROGRAM:

```
def gcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

```
p = 7
```

```
q = 17
```

```
n = p * q
```

```
phi = (p - 1) * (q - 1)
```

```
e = 5
```

```
while gcd(e, phi) != 1:  
    e += 1  
  
d = pow(e,1,phi) phi)  
print("Public Key (e, n):", (e, n))  
print("Private Key (d, n):", (d, n))  
msg = int(input("Enter message (as number): "))  
cipher = pow(msg, e, n)  
print("Encrypted Message:", cipher)  
decrypted = pow(cipher, d, n)  
print("Decrypted Message:", decrypted)
```

OUTPUT:

```
...  Public Key (e, n): (5, 119)  
     Private Key (d, n): (77, 119)  
     Enter message (as number): 12  
     Encrypted Message: 3  
     Decrypted Message: 12
```

CONCLUSION: The Above Program Has Been Executed Successfully.

PRACTICAL NO : 7
STUDY OF MD5 ALGORITHM

AIM: To Write A Python Program To Demonstrate MD5 Algorithm.

PROGRAM:

```
import hashlib  
str1 = "syit class"  
md5hash_value = hashlib.md5()  
md5hash_value.update(str1.encode('utf-8'))  
message_digest = md5hash_value.hexdigest()  
print("Message Digest:", message_digest)
```

OUTPUT:

Message Digest: def2fae3fe87648cd2f8fc69bb2074c

CONCLUSION: The Above Program Has Been Executed Successfully.

PRACTICAL NO : 8
STUDY OF HASH FUNCTION- RS HASH

AIM: To Write A Program To Demonstrate RSHash Function In Python.

PROGRAM:

```
def rs_hash_value(string):
    a = 63689
    b = 378551
    hash_value = 0
    for ch in string:
        hash_value = hash_value * a + ord(ch)
        a = a * b
    return hash_value & 0xFFFFFFFF

text = "syit class"
h1 = rs_hash_value(text)
print("RS Hash Value:", h1)
```

OUTPUT:

*** RS Hash Value: 4113426761

CONCLUSION: The Above Program Has Been Executed Successfully.

PRACTICAL NO : 9**CREATE, EXPORT AND VALIDATE A DIGITAL
CERTIFICATE.**

AIM: To write a code to Create, Export and Validate a digital Certificate.

STEPS:

1. Download and Install openssl
2. Add its bin path in environmental variable
3. Open command prompt

PROGRAM:

```
C:\User\Sherly\Desktop>openssl req -x509 -days 365 -  
newkey rsa:2048 -keyout private-key.pem -out  
certificate.pem
```

Enter PEM Pass: 123456

Country Name (2 letter code) []: IN

State or Province Name (full name) []: Maharashtra

Locality Name []: Mumbai

Organization Name []: SIWS

Organizational Unit Name []: IT

Common Name []: TMD

Email Address []: vaishnavithevar@gmail.com

```
C:\User\Vaishnavi\Desktop> openssl pkcs12 -export -in  
certificate.pem -inkey private-key.pem -out TMD.pfx -clcerts
```

Enter Export Password: 123456

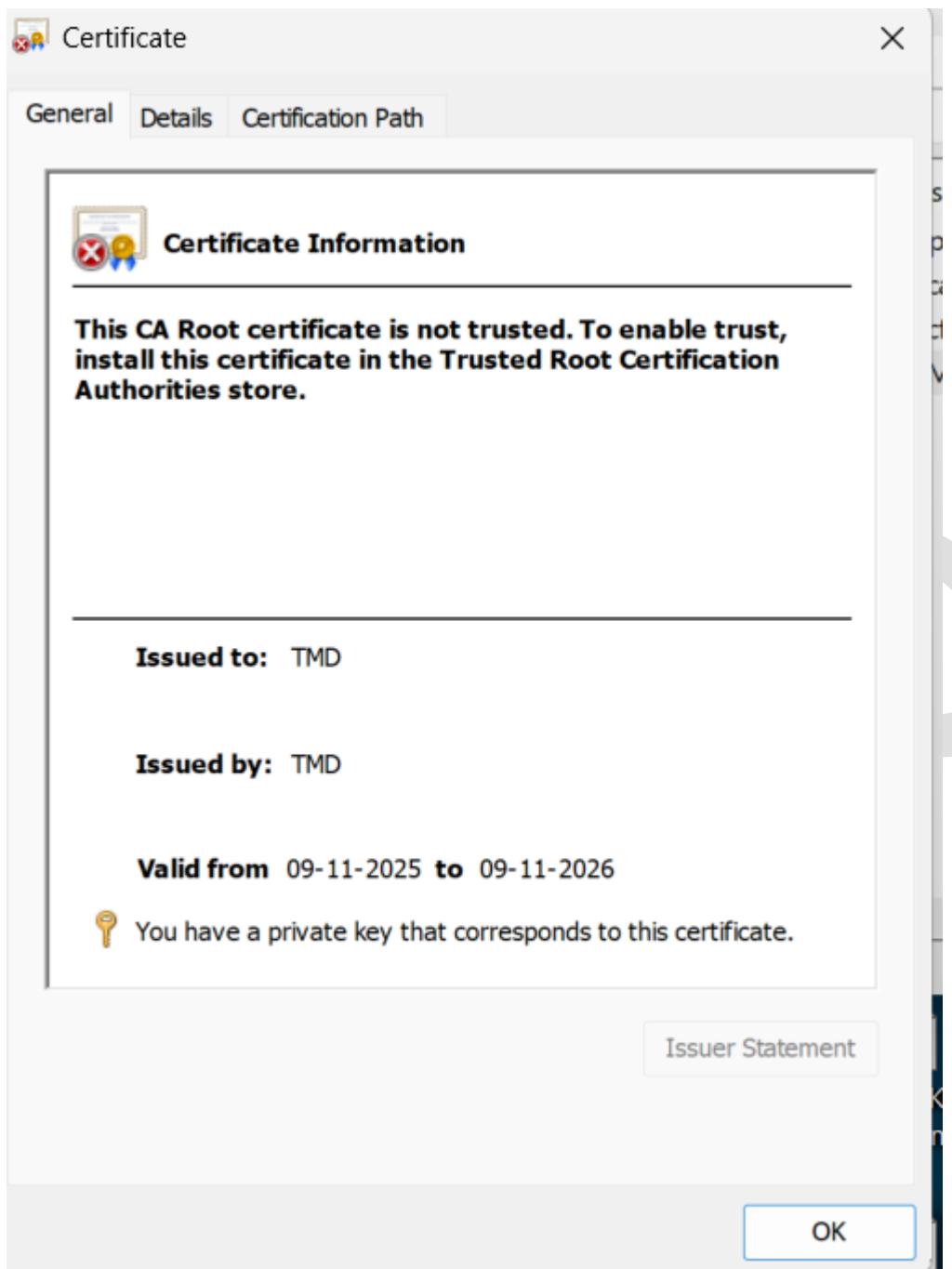
Verifying - Enter Export Password: 123456

```
C:\User\Vaishnavi\Desktop> openssl pkcs12 -in TMD.pfx -  
clcerts -nokeys -out public-key.pem
```

Enter Import Password: 123456

Import the certificate

OUTPUT:



CONCLUSION: The above creation is done successfully.