Course Code: CSE 360

Course Name: Computer Networks Laboratory

LAB REPORTS

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Submission: 19.03.23

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 01

Name of Experiment: Routing through Hub and Switch

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 29.09.22

Date of Submission: 13.10.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Introduction:

Hub: A hub is the simplest of these devices. Any data packet coming from one port is sent to all other ports. It is then up to the receiving computer to decide if the packet is for it or not. The biggest problem with hubs is their simplicity. Since every packet is sent out to every computer on the network, there is a lot of wasted transmission. This means that the network can easily become flooded. Hubs are typically used on small networks where the amount of data going across the network is never very high.

Switch: A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.

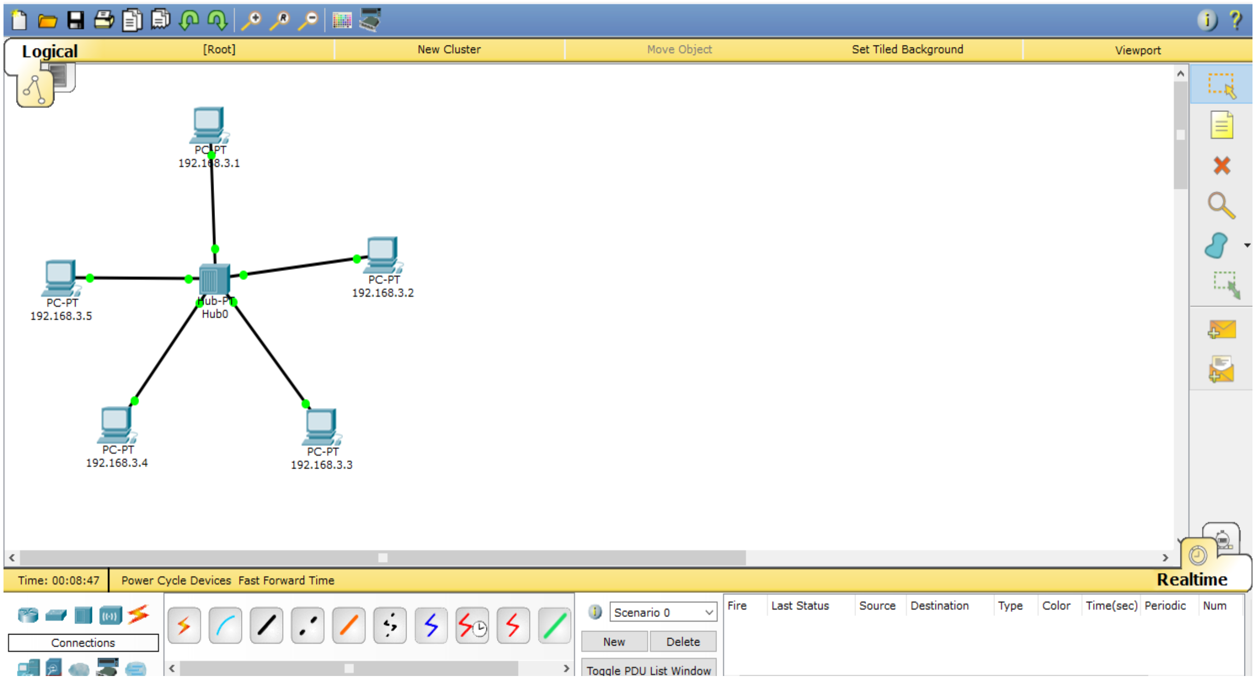
Objective:

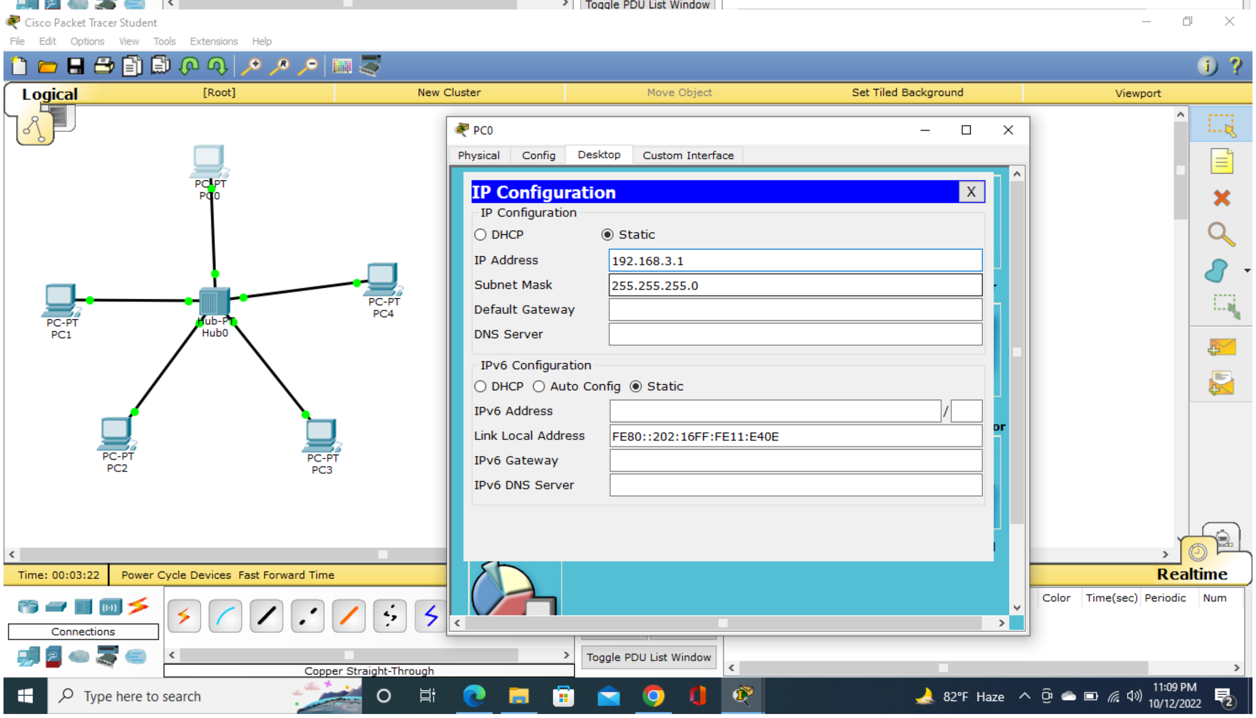
- To introduce network simulation tool “Cisco Packet Tracer” and learn how to use different components of it to build a network.
- To learn how to configure an IP address of a computer.
- To know how hub and switch behave in routing and difference between their routing procedure.
- To understand basic networking commands like tracert, ping.

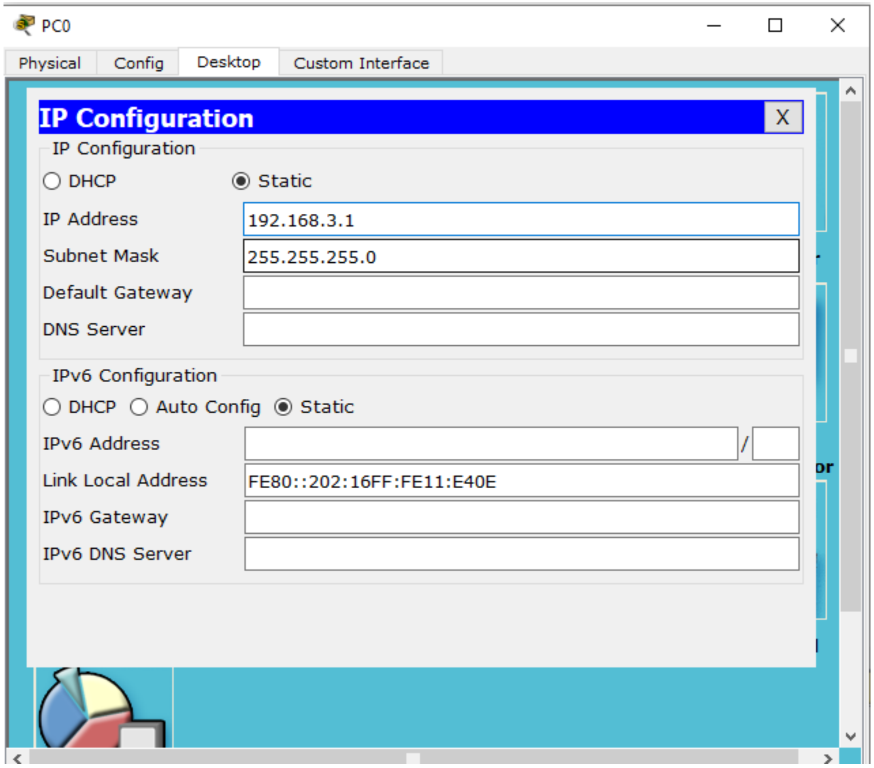
Apparatus:

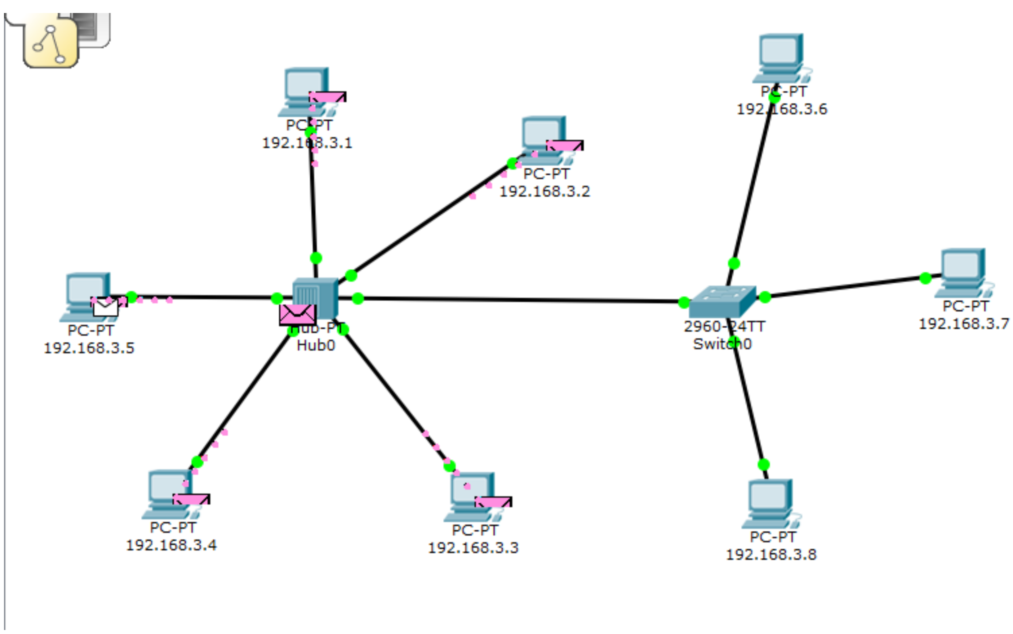
1. Computer
2. Software “Cisco Packet Tracer”

Network Diagram:

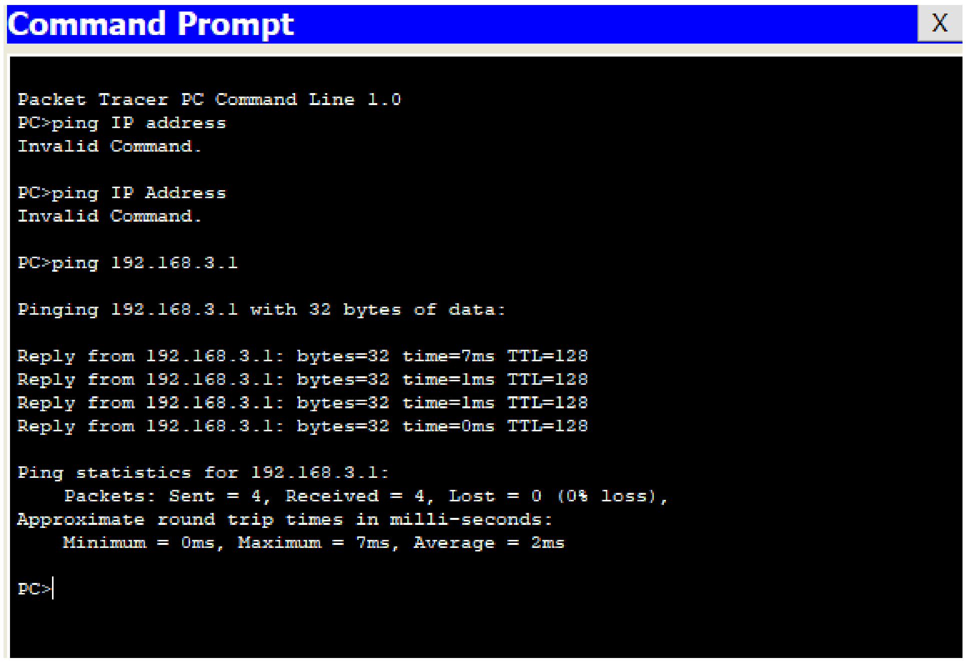





PC0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.3.1
Subnet Mask
255.255.255.0
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::202:16FF:FE11:E40E
IPv6 Gateway
IPv6 DNS Server


PC-PT
192.168.3.1
PC-PT
192.168.3.2
PC-PT
192.168.3.6
PC-PT
192.168.3.5
Hub-PT
Hub0
2960-24TT
Switch0
PC-PT
192.168.3.7
PC-PT
192.168.3.4
PC-PT
192.168.3.3
PC-PT
192.168.3.8

Result:



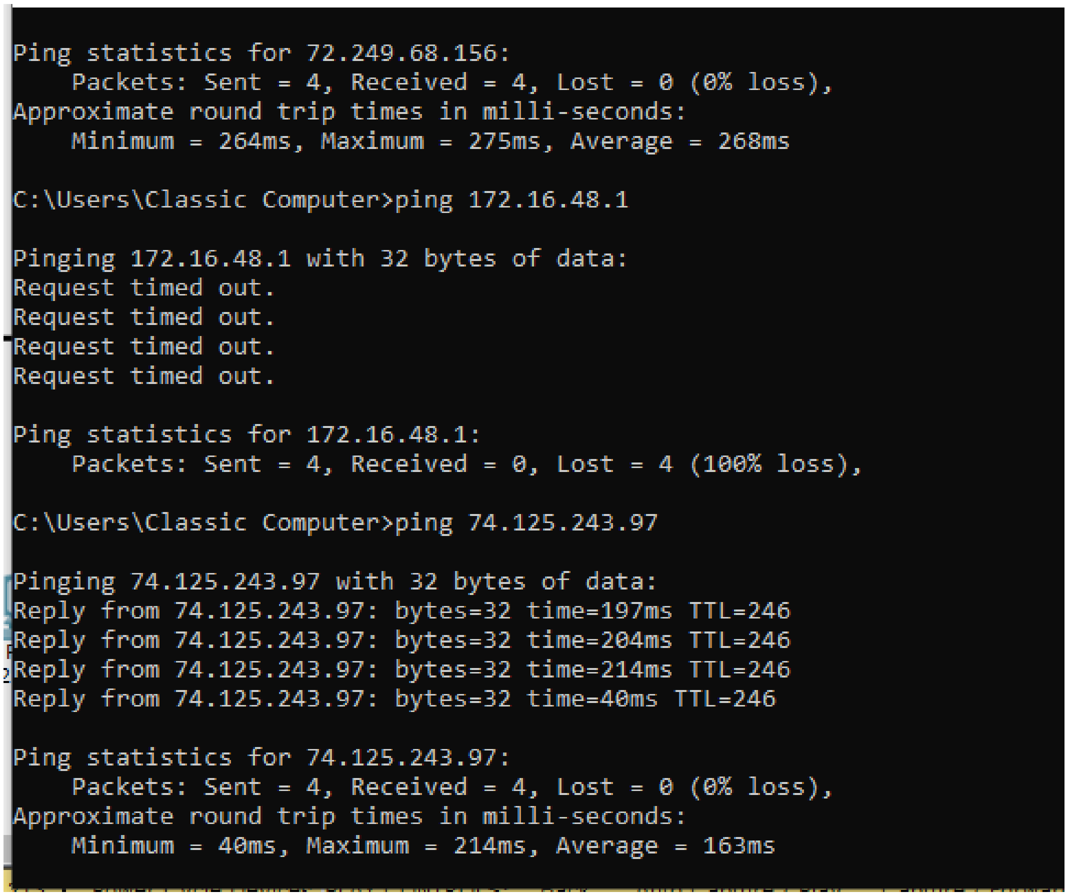
```
Command Prompt                                                    X

Packet Tracer PC Command Line 1.0
PC>ping IP address
Invalid Command.

PC>ping IP Address
Invalid Command.

PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=7ms TTL=128
Reply from 192.168.3.1: bytes=32 time=1ms TTL=128
Reply from 192.168.3.1: bytes=32 time=1ms TTL=128
Reply from 192.168.3.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

PC>
```

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=0ms TTL=128
Reply from 192.168.3.2: bytes=32 time=1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=18ms TTL=128
Reply from 192.168.3.2: bytes=32 time=19ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 9ms

PC>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=381ms TTL=128
Reply from 192.168.3.4: bytes=32 time=1ms TTL=128
Reply from 192.168.3.4: bytes=32 time=1ms TTL=128
Reply from 192.168.3.4: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 381ms, Average = 96ms

PC>
```

Command Prompt

```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Classic Computer>ping www.google.com

Pinging www.google.com [172.217.167.36] with 32 bytes of data:
Reply from 172.217.167.36: bytes=32 time=73ms TTL=116
Reply from 172.217.167.36: bytes=32 time=161ms TTL=116
Reply from 172.217.167.36: bytes=32 time=168ms TTL=116
Reply from 172.217.167.36: bytes=32 time=187ms TTL=116

Ping statistics for 172.217.167.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 73ms, Maximum = 187ms, Average = 147ms

C:\Users\Classic Computer>ping www.ju.com

Pinging ju-com-redirect-2013477519.ap-northeast-1.elb.amazonaws.com [54.92.27.157] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 54.92.27.157:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Classic Computer>
```



```
Ping statistics for 72.249.68.156:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 264ms, Maximum = 275ms, Average = 268ms

C:\Users\Classic Computer>ping 172.16.48.1

Pinging 172.16.48.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.48.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Classic Computer>ping 74.125.243.97

Pinging 74.125.243.97 with 32 bytes of data:
Reply from 74.125.243.97: bytes=32 time=197ms TTL=246
Reply from 74.125.243.97: bytes=32 time=204ms TTL=246
Reply from 74.125.243.97: bytes=32 time=214ms TTL=246
Reply from 74.125.243.97: bytes=32 time=40ms TTL=246

Ping statistics for 74.125.243.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 214ms, Average = 163ms
```

Discussion:

From this lab, we learn the routing procedure through hub and switch. Hub sends a packet not only the destination node but also the also all nodes that are connected with hub. Switch sends a packet only destination node.

We also know the purpose of using tracert and ping command. Tracert is used for checking the step by step route a packet takes to reach the destination. Ping is used for testing the connection between two nodes of a network.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 02

Name of Experiment: DSL Modem in WAN

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 13.10.22

Date of Submission: 20.10.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Introduction:

A common way to connect to an ISP is to use the phone line to your house using DSL (Digital Subscriber Line). The computer is connected to a DSL modem that converts between digital packets and analog signals that can pass unhindered over the telephone line.

At the other end, a device called a DSLAM (Digital Subscriber Line Access Multiplexer) converts between signals and packets.

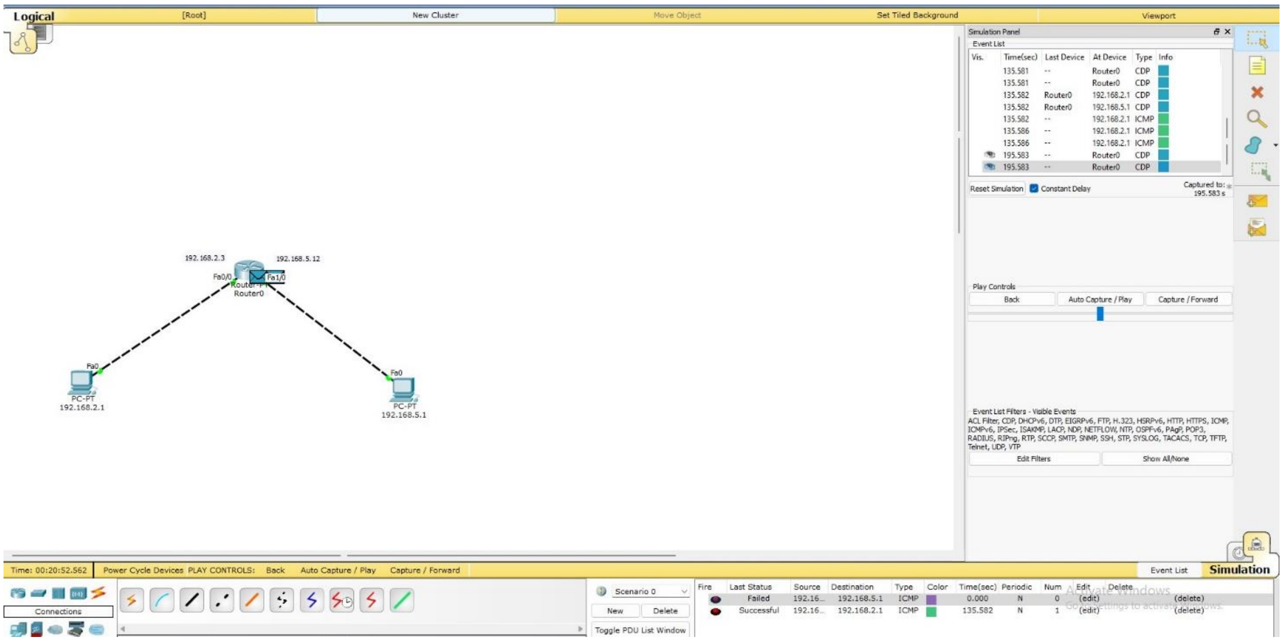
Objective:

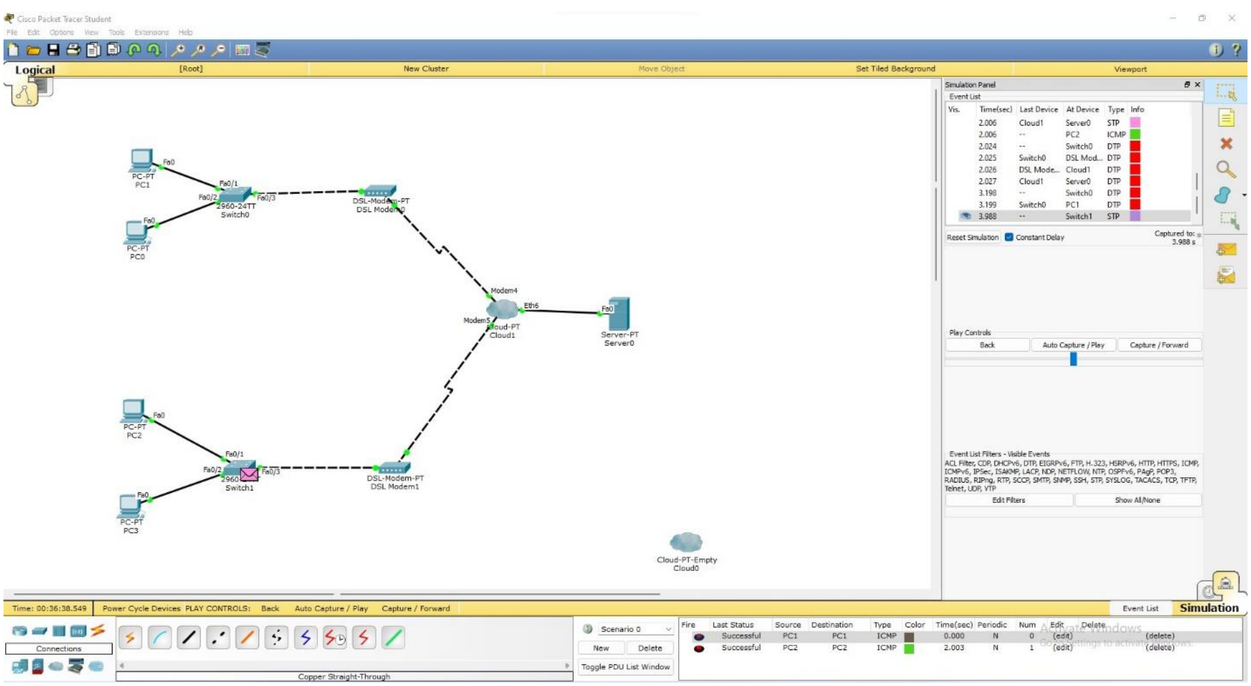
- To prove that Ethernet WAN allows to use as an DSL modem router or stand-alone wireless router
- To see Compatible with VDSL2, ADSL2/2+, ADSL, fiber and cable services for complete future-proofing
- To learn Fast Ethernet ports for the reliable internet performance
- To learn VDSL/ADSL WAN multi service for IPTV support

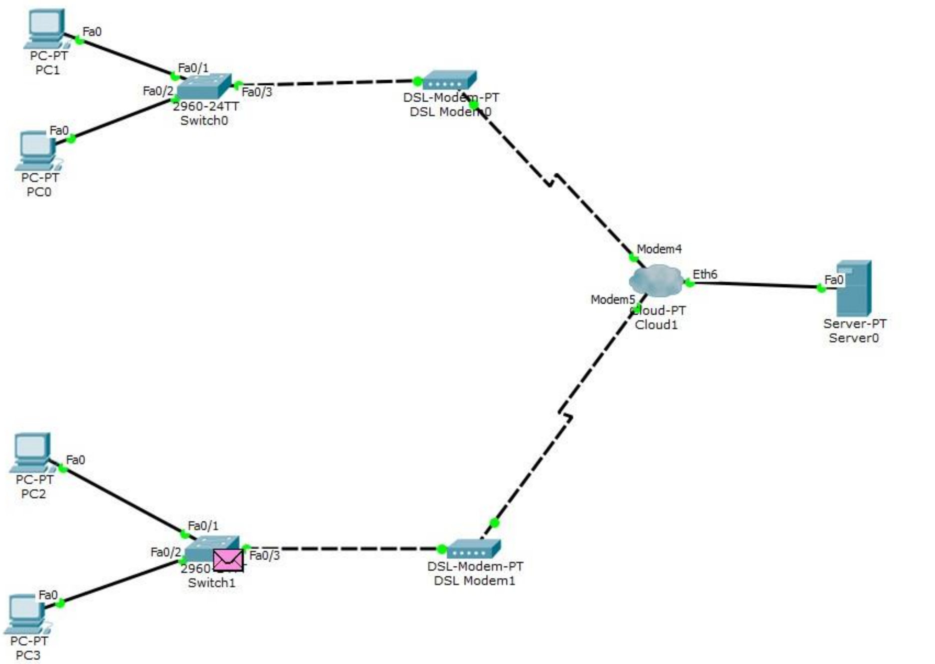
Apparatus:

3. Computer
4. Software “Cisco Packet Tracer”

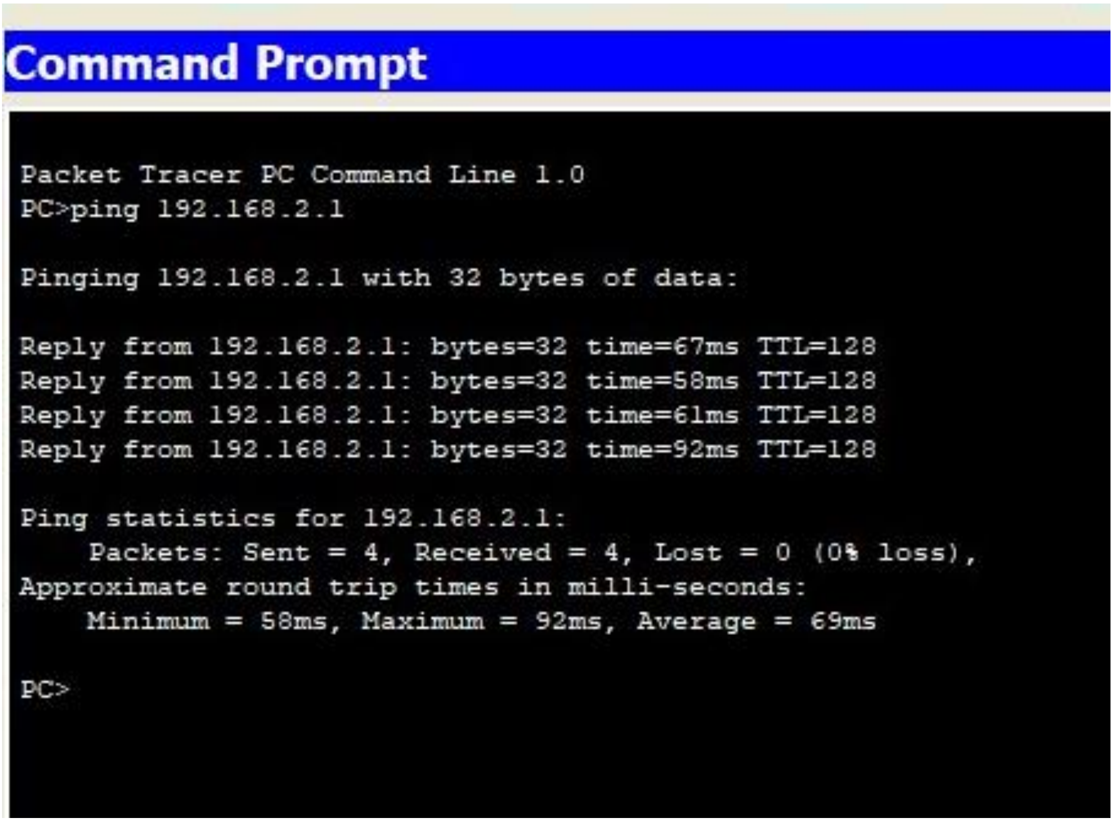
Network Diagram:






Fa0
PC-PT
PC1
Fa0/1
Fa0/2
Fa0/3
2960-24TT
Switch0
Fa0
PC-PT
PC0
DSL-Modem-PT
DSL Modem0
Modem4
Eth6
Modem5
Cloud-PT
Cloud1
Fa0
Server-PT
Server0
Fa0
PC-PT
PC2
Fa0/1
Fa0/2
Fa0/3
Switch1
Fa0
PC-PT
PC3
DSL-Modem-PT
DSL Modem1

Result:



Discussion:

Typically, a DSL modem router uses the phone line as the medium to connect directly to your ISP and provides internet to your other devices via wired or wireless connection. It also allows you to use the phone service while online. You just need a DSL Splitter to help connect both your modem router and your phone to the DSL port.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 03

Name of Experiment: Router Configuration Using CLI

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 20.10.22

Date of Submission: 27.10.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Introduction:

A router is similar in a switch in that it forwards packets based on address. But, instead of the MAC address that a switch uses, a router can use the IP address. This allows the network to send packet among different network ID.

Objective:

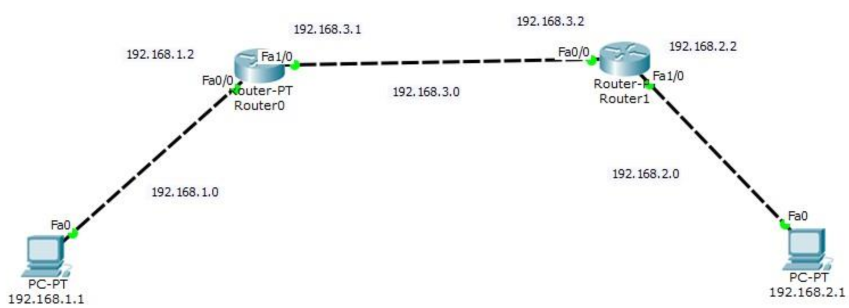
1. To learn how to create a network topology in PT

2. To learn how to configure a network topology using command mode

Apparatus:

1. Computer
2. Software "Cisco Packet Tracer"

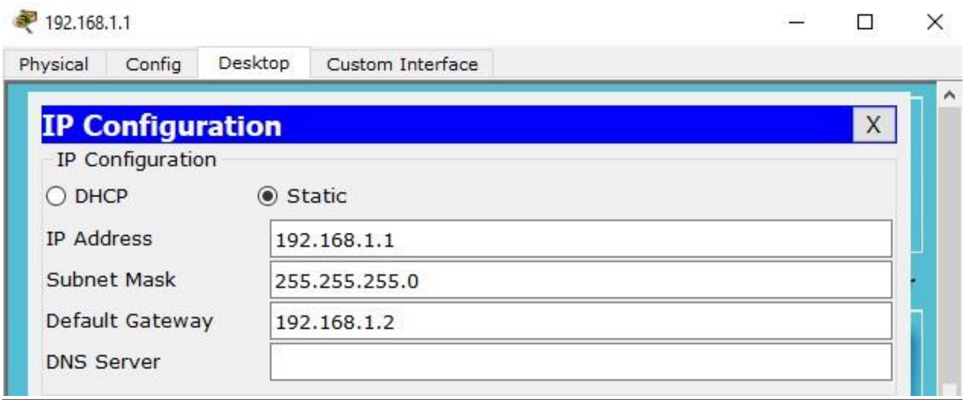
Network Diagram:

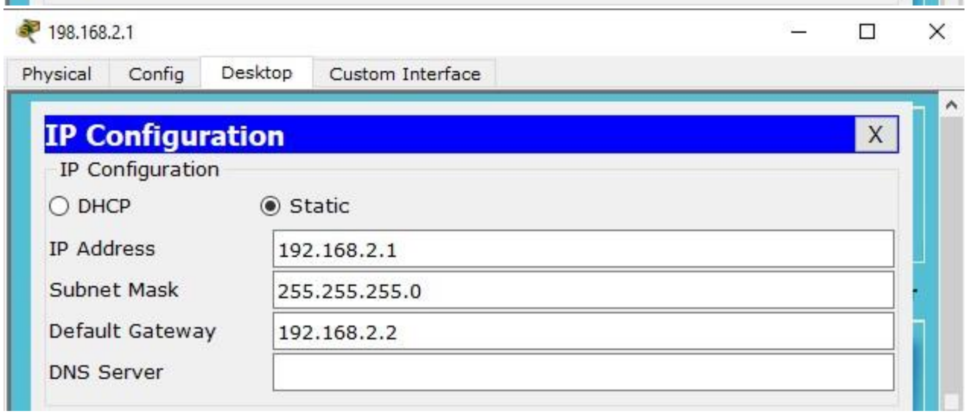


Methodology:

Step-1: Create the above local network using router and pc

Step-2: Configure each pc with router providing IC, and subnet musk





Step-3: Configure router using following command on CIF of ROUTER

Router>en %enable

Router#conf t %configure terminal

Router(config)#int fa0/0 %interface fa0/0

Router(config-if)#ip add 192.168.1.2 255.255.255.0

Router(config-if)#no shut %no shutdown i.e. make the port on

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa1/0

Router(config-if)#ip add 192.168.3.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#exit

Router#

Router#en

Router#conf t

Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

Router(config)#end

Router#

Router#sh ip route

C 192.168.1.0/24 is directly connected, FastEthernet0/0

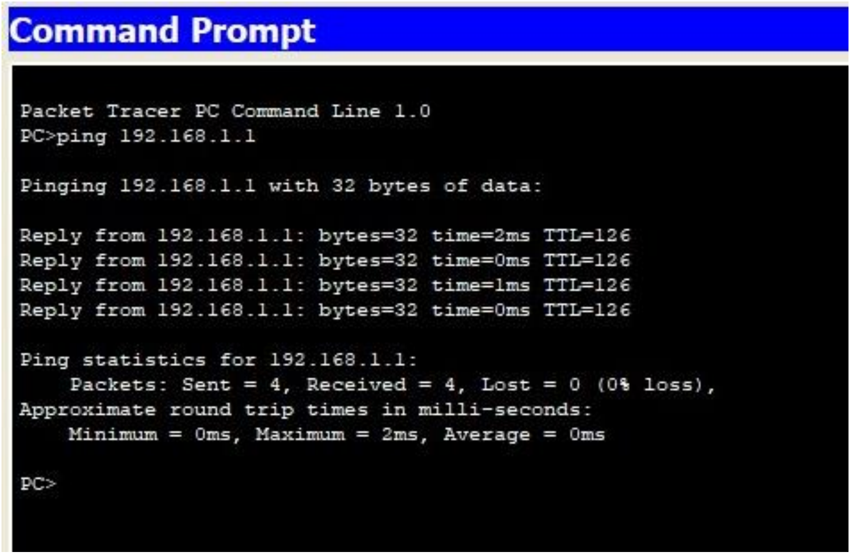
S 192.168.2.0/24 [1/0] via 192.168.3.2

C 192.168.3.0/24 is directly connected, FastEthernet1/0

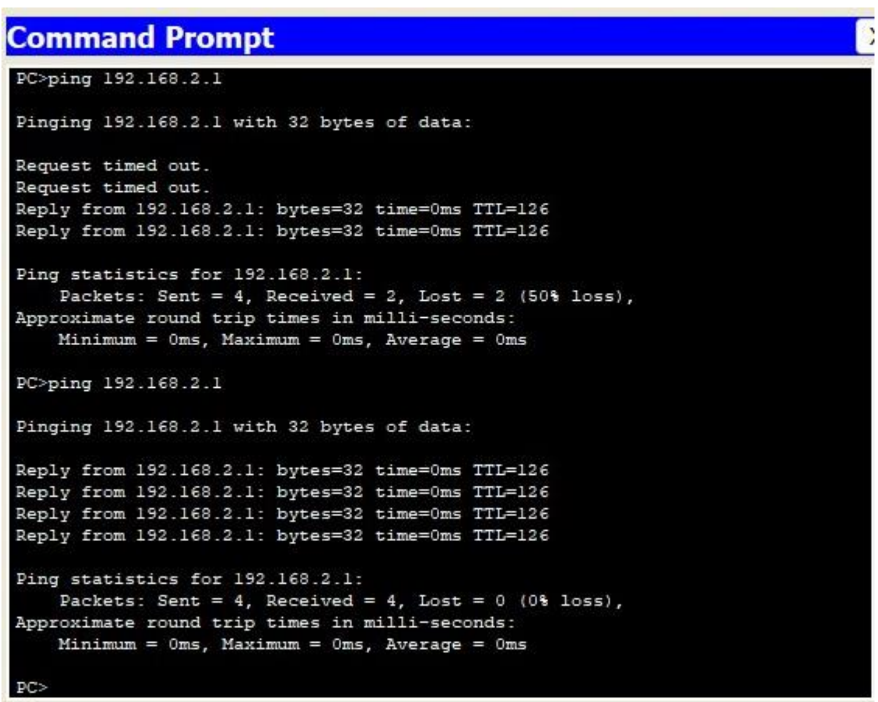
Router#

Step-4: Perform the same steps for router-1

Result:



```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```



```
Command Prompt
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

Discussion: We can see that the Routers sends the packet the required path mentioned in the rout table.

Comment: Using a table to determine hops is efficient.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 04

Name of Experiment: VLAN Configuration with Switch and Router

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 27.10.22

Date of Submission: 04.11.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Experiment Name: VLAN Configuration with Switch and Router.

Introduction:

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

Objective:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Apparatus:

1. Packet Tracer software
2. Generic Router (1)
3. Generic PC (6)
4. Switch (1)

Network Diagram:

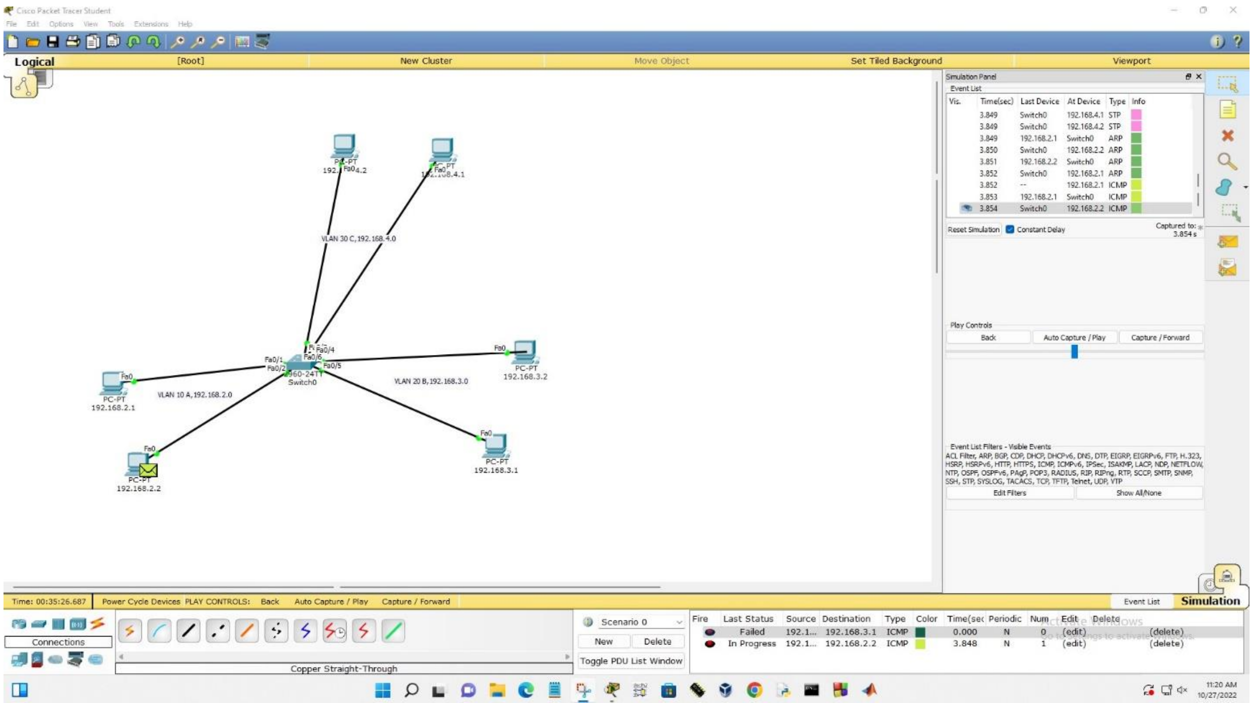


Fig. Network diagram of Van configuration

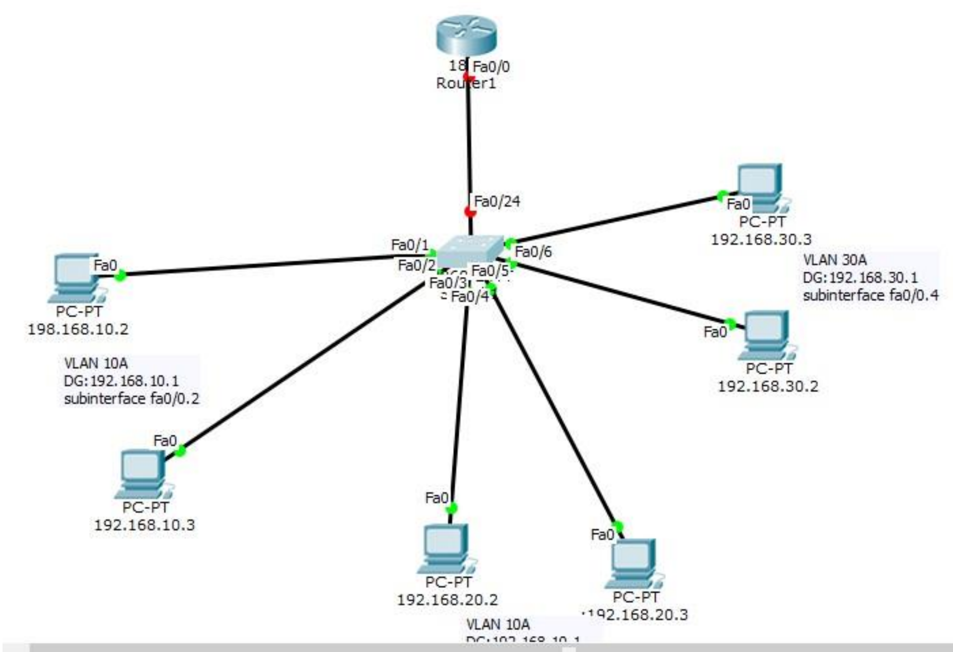
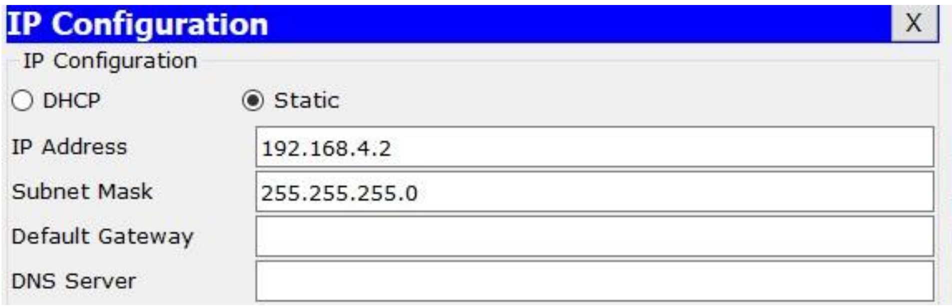
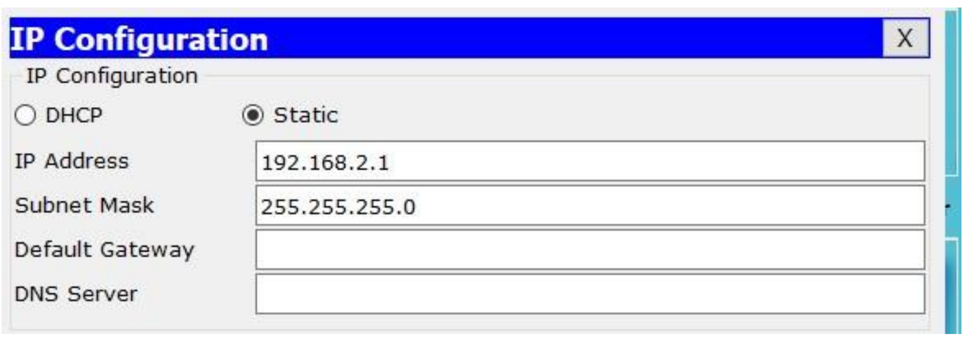


Fig. VLAN under sub-interface

Methodology:

Step-1: Provide IP and subnet must to each PC. For example,





Step-2: Configure the switches and Re-enable the user ports.

Switch>en

Switch# vlan database

Switch(vlan)# vlan 10 name A

Switch(vlan)# vlan 20 name B

Switch(vlan)# vlan 30 name C

Switch(vlan)# exit

Switch#

Switch# conf t

Switch(config)# int fa0/1

Switch(config-if)# switchport mode access

```
Switch(config-if)# switchport access vlan 10
Switch(config-if)# int fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# int fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# int fa0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# int fa0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 30
Switch(config-if)# int fa0/6
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 30
Switch(config-if)#end
Switch#
```

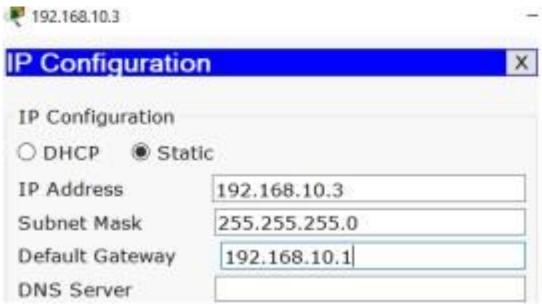
Step 3: Verify that the VLANs have been created on S1. Use the show vlan brief command to verify that the VLANs have been created.

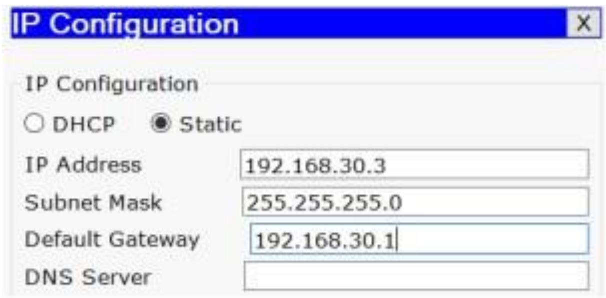
```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   faculty/staff                    active
20   students                         active
30   guest                            active
99   management                       active
```

Step-5: Now apply ping on PC of IP 192.168.2.2 to PC 192.168.2.2 of same VLAN 10 will be success. But to the PC 192.168.4.2 of different VLAN, the ping will be fail as shown below. Similarly you can verify the ICMP packet under simulation mode.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Step-6: Create VLAN under sub-interface and configure the PC





Step-7: Configure the Switch again using command prompt

Switch>en

Switch#

Switch#vlan database

Switch(vlan)#vlan 10 name A

Switch(vlan)#vlan 20 name B

Switch(vlan)#vlan 30 name C

Switch(vlan)#exit

Switch#conf t

Switch(config)#int range fa0/1-6

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

Switch(config-if-range)#int range fa0/7-14

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 20

Switch(config-if-range)#int range fa0/15-23

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#int fa0/24

Switch(config-if)#switchport mode trunk

Switch(config-if)#end

Switch#sh vlan brief

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/24, Gig1/1, Gig1/2
10   A                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
20   B                                active    Fa0/7, Fa0/8, Fa0/9, Fa0/10 ,Fa0/11, Fa0/12, Fa0/13, fa0/14
30   C                                active    Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Step-8: Configure the router using cmd

Router#conf t

Router(config)#int fa0/0

Router(config-if)#no shut

Router(config-if)#int fa0/0.1

Router(config-subif)#encapsulation dot1q 1

Router(config-subif)#ip add 192.168.1.1 255.255.255.0

Router(config-subif)#int fa0/0.2

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip add 192.168.10.1 255.255.255.0

Router(config-subif)#int fa0/0.3

Router(config-subif)#encapsulation dot1q 20

Router(config-subif)#ip add 192.168.20.1 255.255.255.0

Router(config-subif)#int fa0/0.4

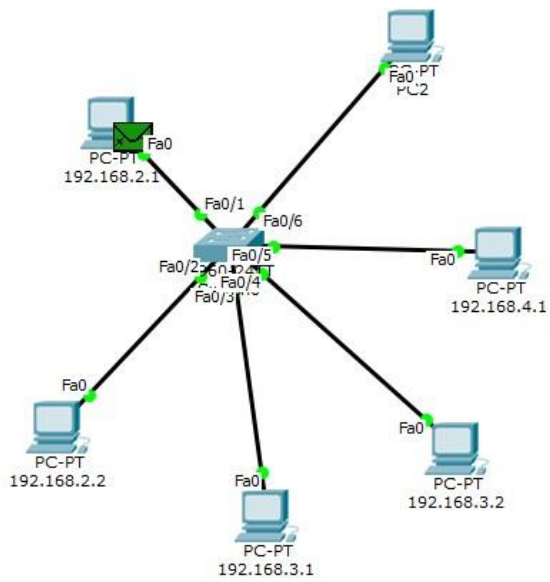
Router(config-subif)#encapsulation dot1q 30

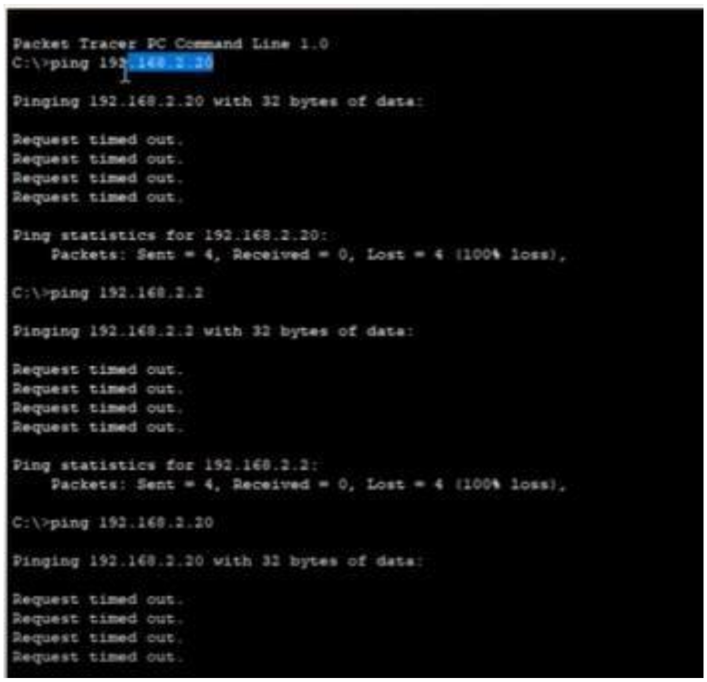
Router(config-subif)#ip add 192.168.30.1 255.255.255.0

Router(config-subif)#end

Result:

Verify the network using ping and ICMP





Discussion:

There are three different options for Routing between VLANs. In each case, the hosts in communication behave exactly the same. In fact, the hosts have no visibility into how and what they are connected to.Each strategy above has its own benefits and limitations. Hopefully at this point you have a good idea of the options available to enable communication between hosts on different VLANs.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 05

Name of Experiment: Implementation of Wireless LAN (Wi-Fi)

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 10.11.22

Date of Submission: 22.11.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Introduction:

A wireless local area network (WLAN) is a wireless distribution method for two or more devices. WLANs use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

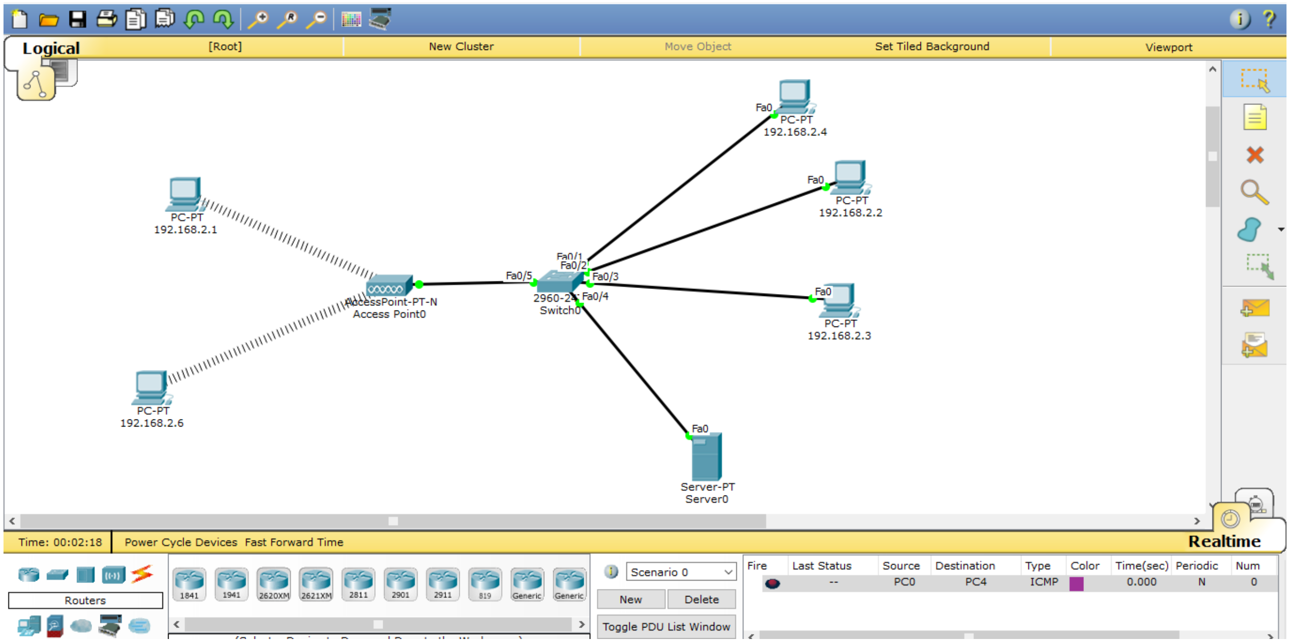
Objective:

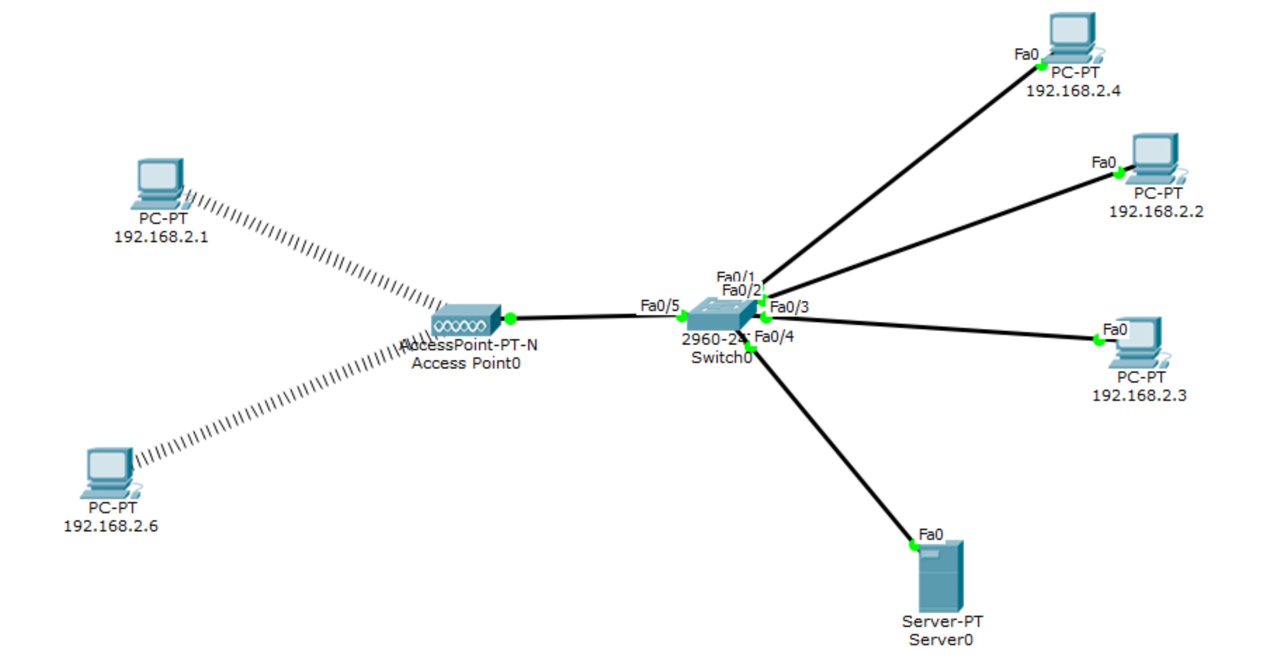
- Introduction to Wireless Local Area Network
- Advantages of WLAN
- Describe the components and operations of basic wireless LAN topologies.
- Describe the components and operations of basic wireless LAN security.
- Configure and verify basic wireless LAN access.
- Configure and troubleshoot wireless client access

Apparatus:

5. Packet Tracer software
6. Generic Router (1)
7. Generic PC (6)
8. Switch (1)

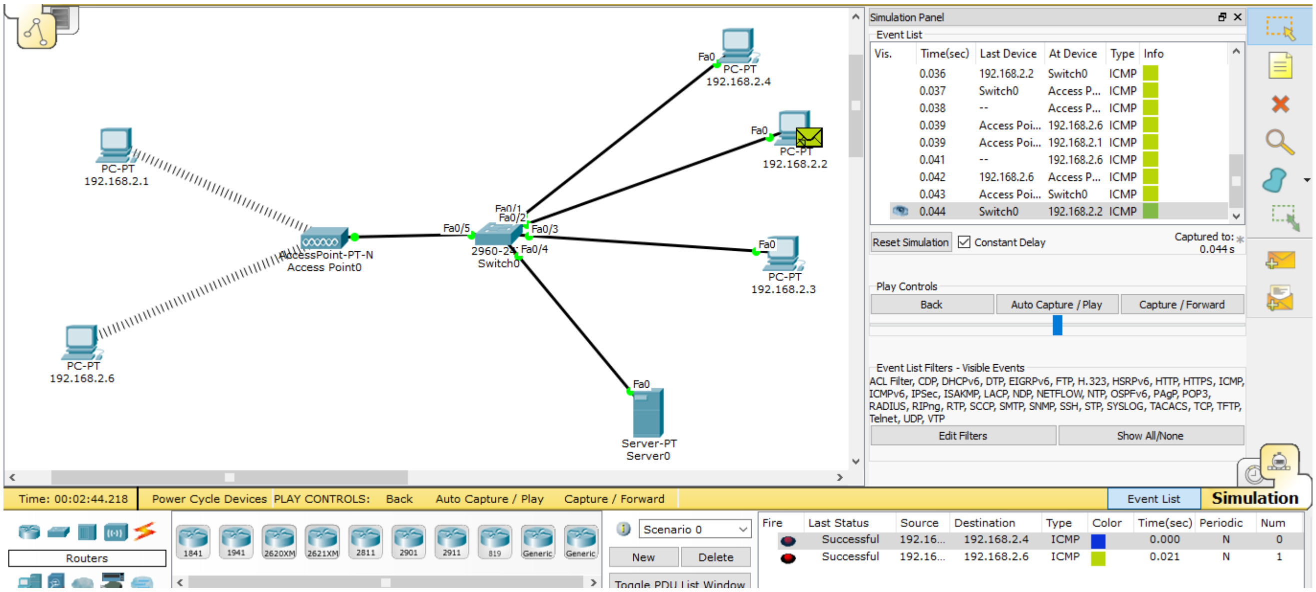
Network Diagram:

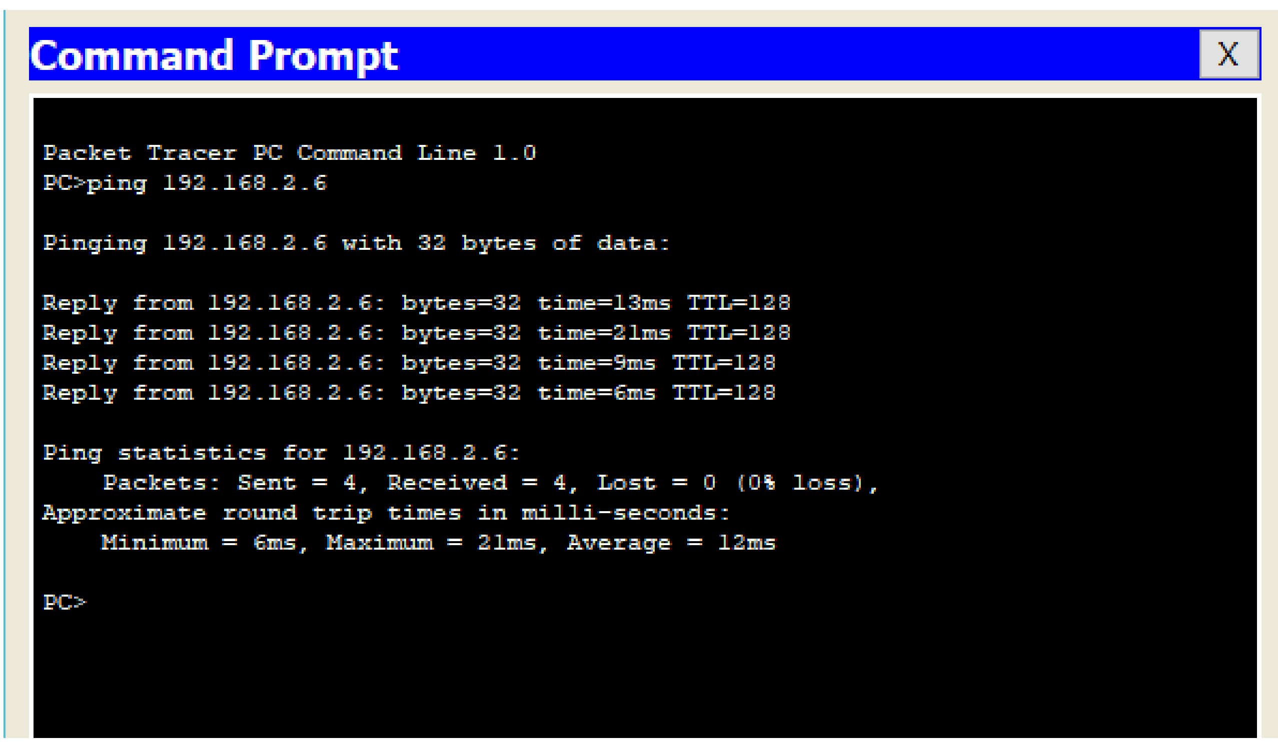




Result:

Verify the network using ping and ICMP





Discussion:

Wireless LANs have many advantages over wired LANS as in providing support for mobility, robustness, cost of installations, increased capacity, scalability, expansion and above all license free . Infrared and radio waves are commonly used for WLANs. IrDA is simple , cheap can be easily integrated but requires line-of-sight and has shorter range whereas radio based networks have large range, can penetrate through walls and buildings but suffers from interference from nearby devices.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 06

Name of Experiment: IP Telephony

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 22.11.22

Date of Submission: 01.12.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Experiment Name: Internet protocol telephony

Introduction: IP telephony (Internet Protocol telephony) is a general term for the technologies that use the Internet Protocol's packet-switched connections to exchange voice, fax, and other forms of information that have traditionally been carried over the dedicated circuit-switched connections of the public switched telephone network (PSTN).

Objective:

Objective of this experiment is to implement a small network of IP telephony. Each telephone will be verified with its content of IP address and corresponding telephone number. Finally, the network will be tested by dialing to each other IP phone.

Apparatus:

1. Packet Tracer software
2. Generic Router (3)
3. Generic PC (3)

Network Diagram:

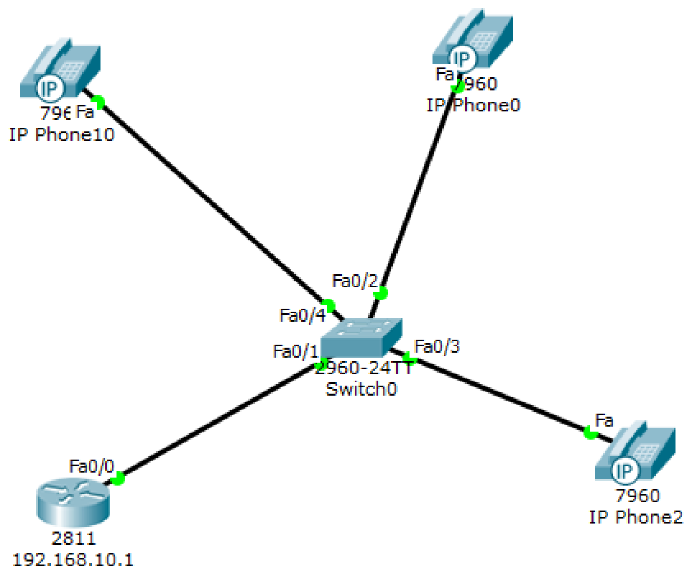
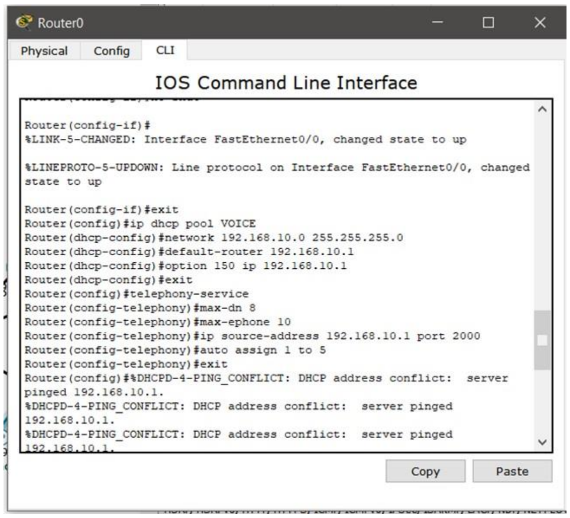


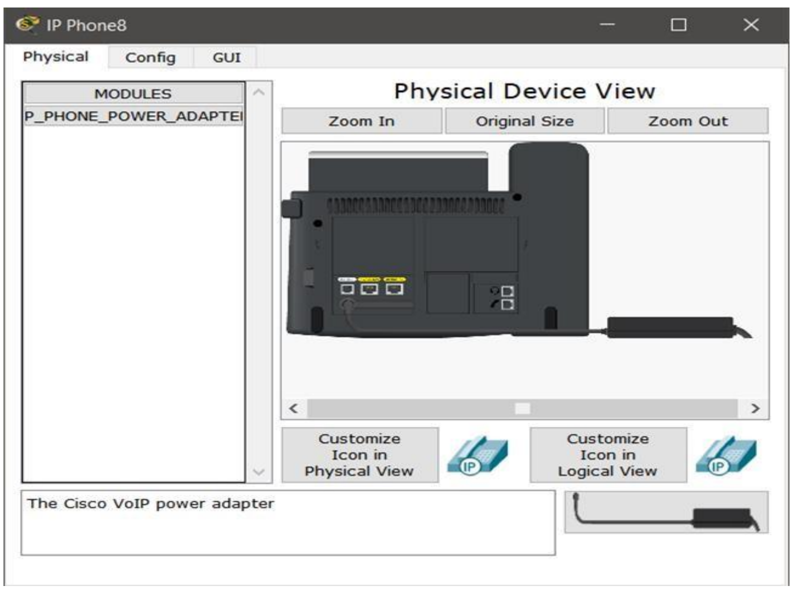
Fig. Network Diagram for IP telephone

Methodology:

Step-1: Implement the IP telephony circuit likes above. During connection to the IP phone the option PC should be selected. Configure router though command line interface using below command.

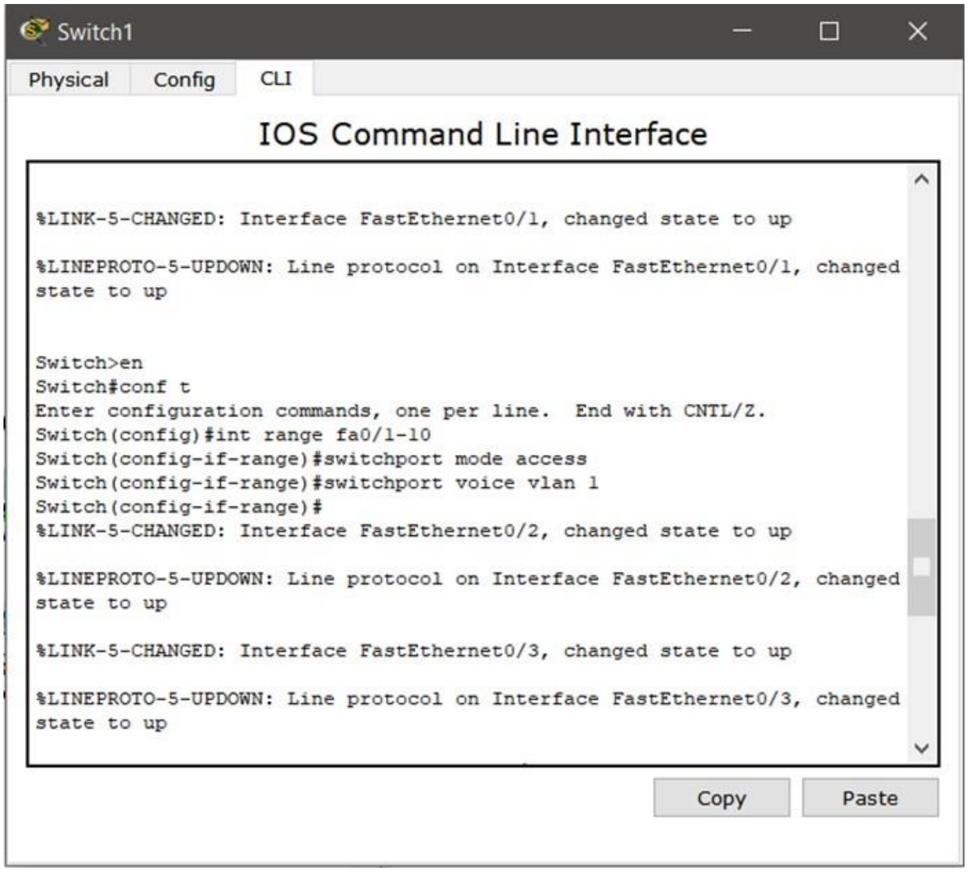


Step-2: Plug in both the telephones.

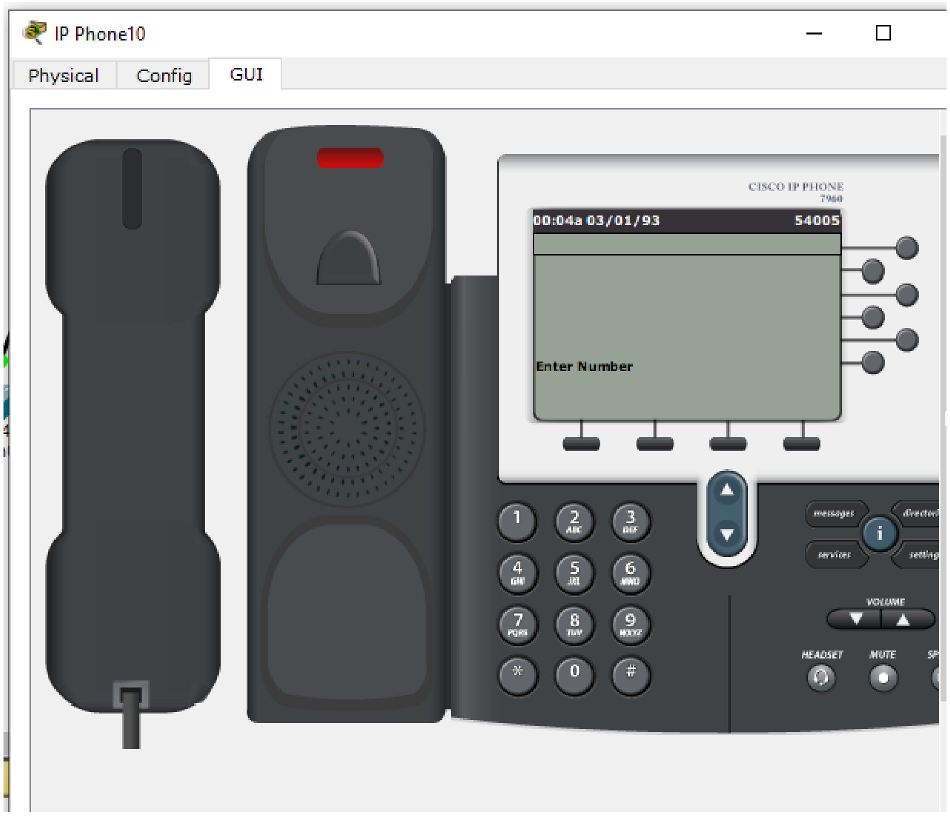


Step3:

Configure the switch using CLI like



Result: Dailing number 54002 from 54005 and it ring out.


IP Phone10
Physical
Config
GUI
CISCO IP PHONE
7960
00:04a 03/01/93
54005
Enter Number
messages
services
VOLUME
HEADSET
MUTE


00:04a 03/01/93
54005
To: 54002
Ring Out


The phone is ringing
00:04a 03/01/93
54002
From: 54005

Fig. Connected to the call

Discussion: We can clearly observe that providing different IP to the telephones it is possible to transfer packet among them and construct a communication among them. So the experiment is valid.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 07

Name of Experiment: Implementation of OSPF (Open Shortest Path First) Algorithm

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 01.12.22

Date of Submission: 08.12.22

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Experiment Name: Implementation of OSPF (open shortest path first) Algorithm

Introduction:

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4.The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPF supports the Classless Inter-Domain Routing (CIDR) addressing model.

Objective:

- Simulate a network with 3 routers with one pc connected with 3 router network and implement OSPF algorithm among these routers.
- Add wic-2t after switching off router. Then turn on again

Apparatus:

1. Packet Tracer software
2. Generic Router (3)
3. Generic PC (3)

Network Diagram:

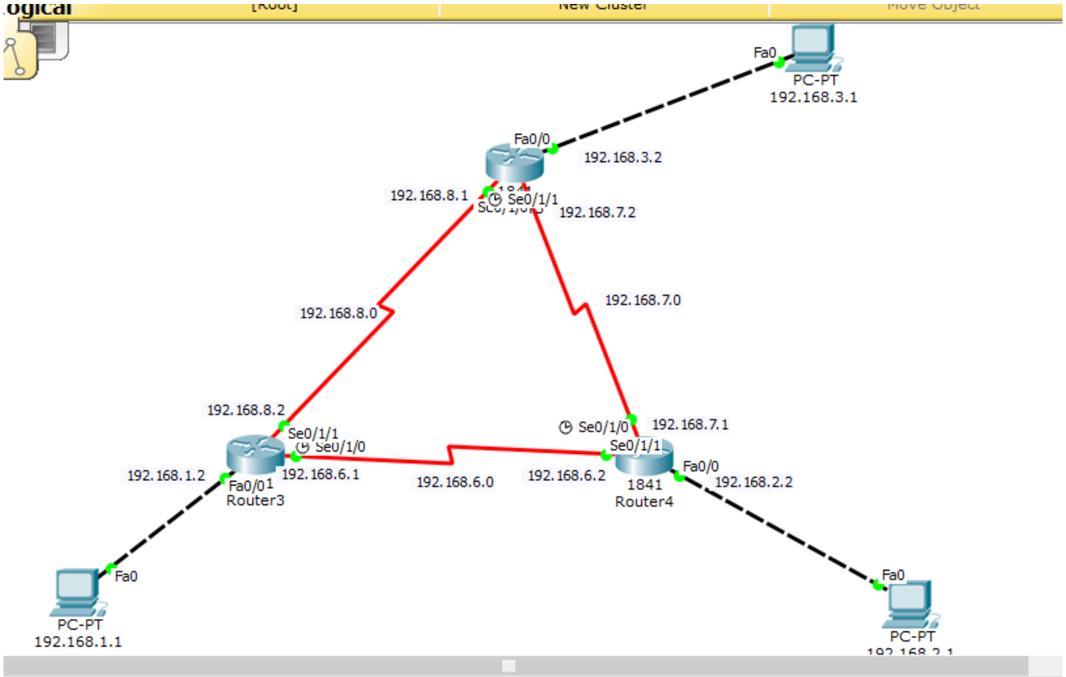
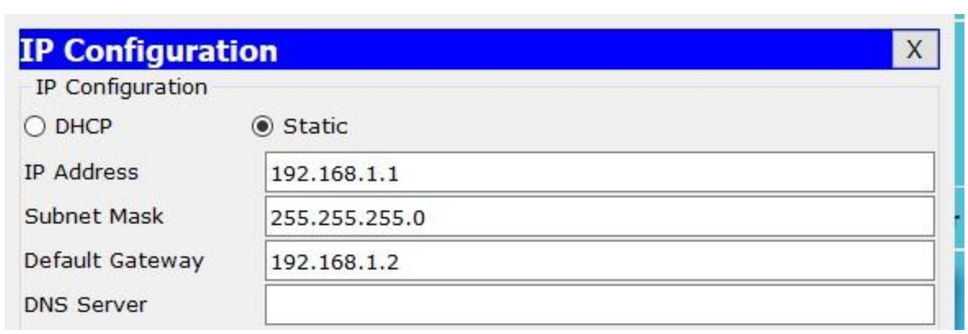
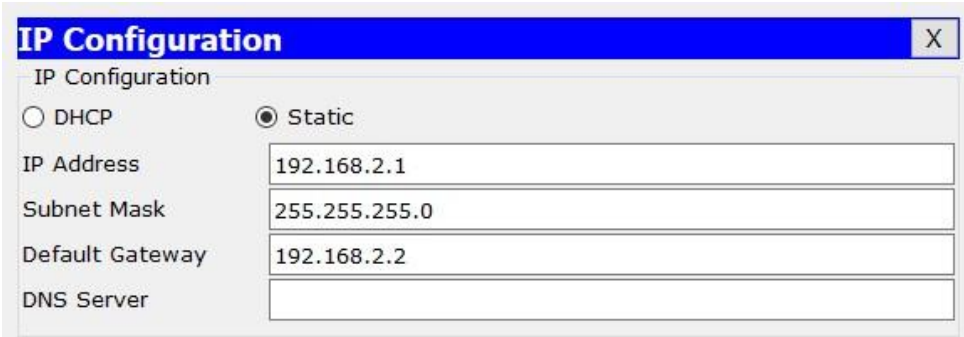


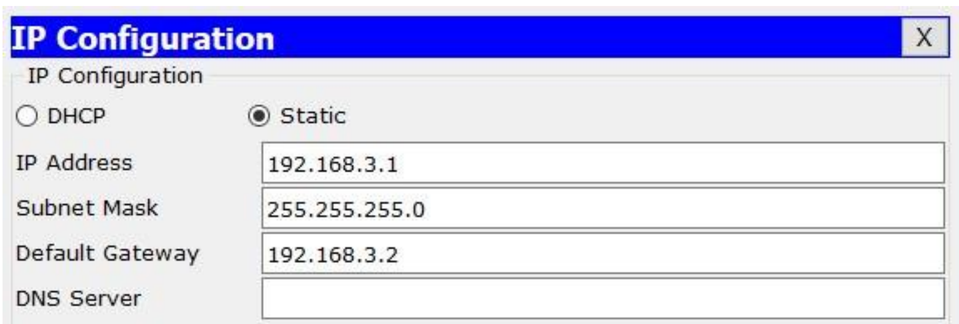
Fig. Network diagram for OSPF algorithm implementation

Methodology:

Step-1: As the above network topology, for each Router, set IP for the default gateway, then set IP for the PC statically (one click on PC > Desktop > IP configuration).

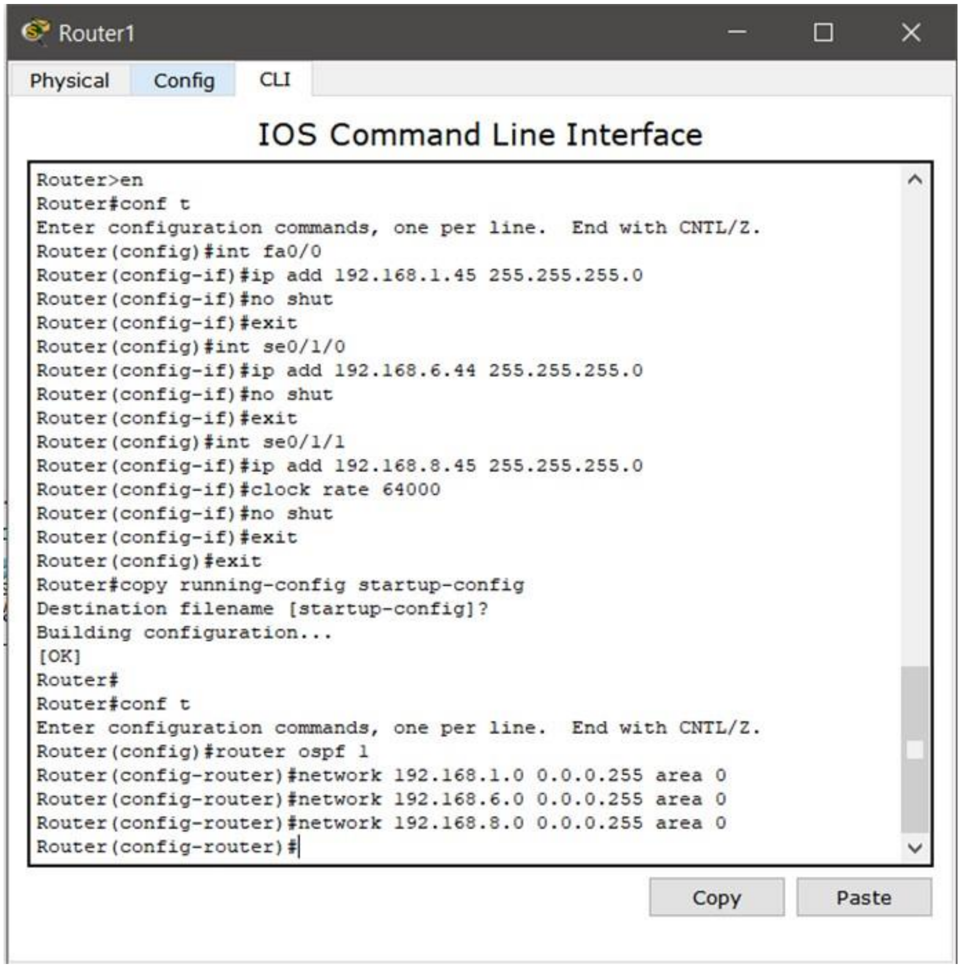




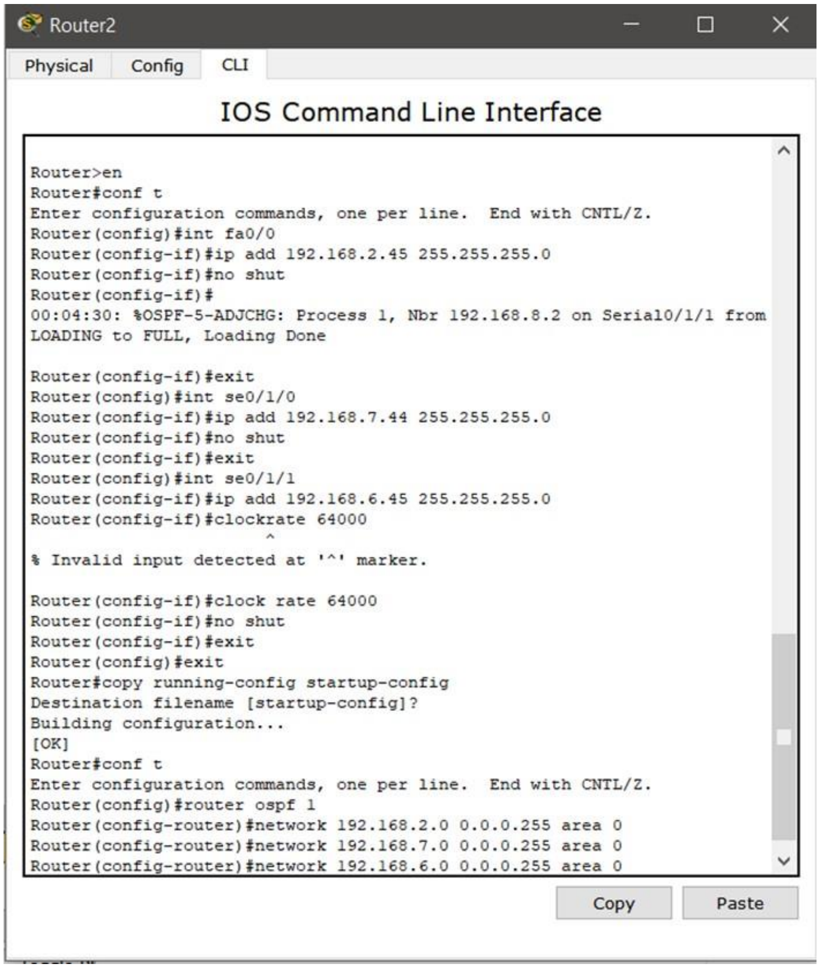


Step-2: Setup each router (one click on router> CLI)and write command to configure each fast ethernet cable and configure ospf network for each router.

Router-1:

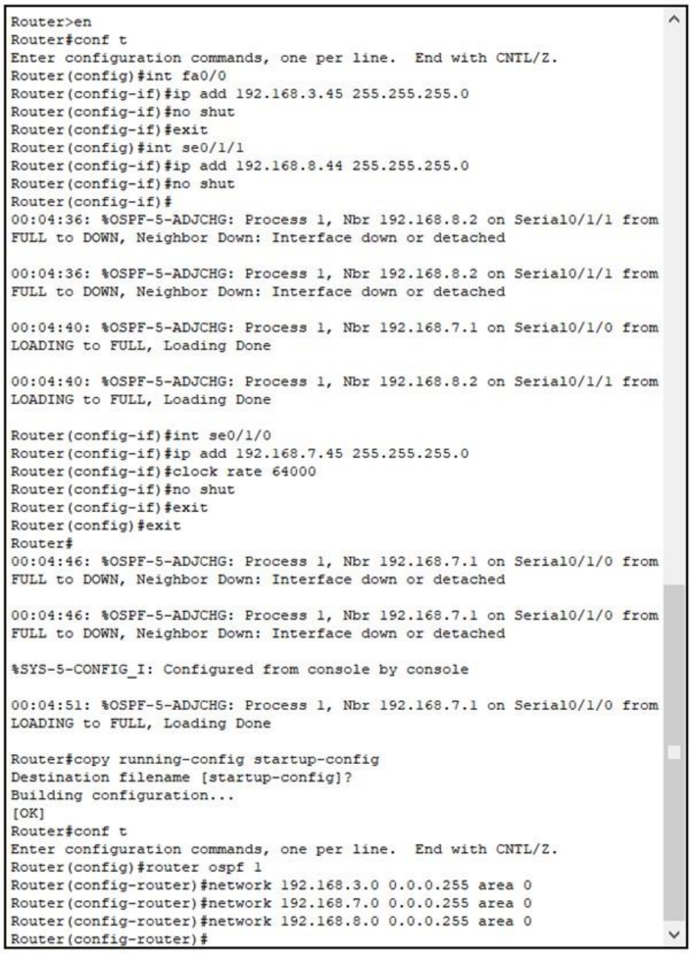

Router1
Physical
Config
CLI
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.1.45 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int se0/1/0
Router(config-if)#ip add 192.168.6.44 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int se0/1/1
Router(config-if)#ip add 192.168.8.45 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.6.0 0.0.0.255 area 0
Router(config-router)#network 192.168.8.0 0.0.0.255 area 0
Router(config-router)#
Copy
Paste

Router-2:




```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.2.45 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
00:04:30: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.8.2 on Serial0/1/1 from
LOADING to FULL, Loading Done

Router(config-if)#exit
Router(config)#int se0/1/0
Router(config-if)#ip add 192.168.7.44 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int se0/1/1
Router(config-if)#ip add 192.168.6.45 255.255.255.0
Router(config-if)#clockrate 64000
                        ^
% Invalid input detected at '^' marker.

Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 192.168.7.0 0.0.0.255 area 0
Router(config-router)#network 192.168.6.0 0.0.0.255 area 0
```

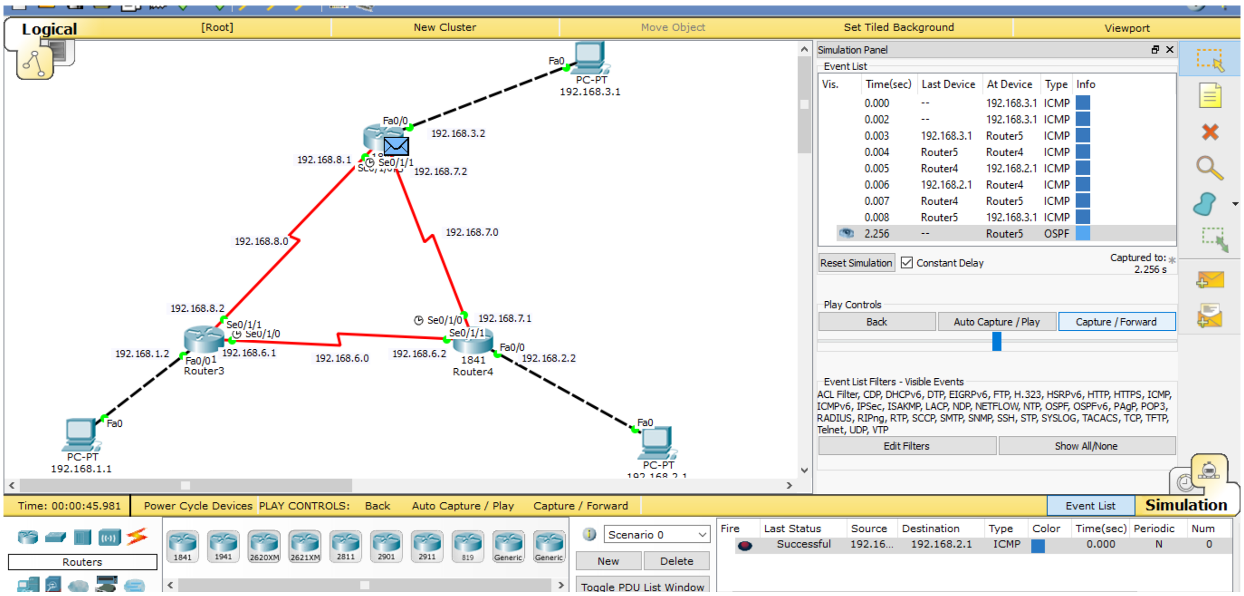
Router-3:



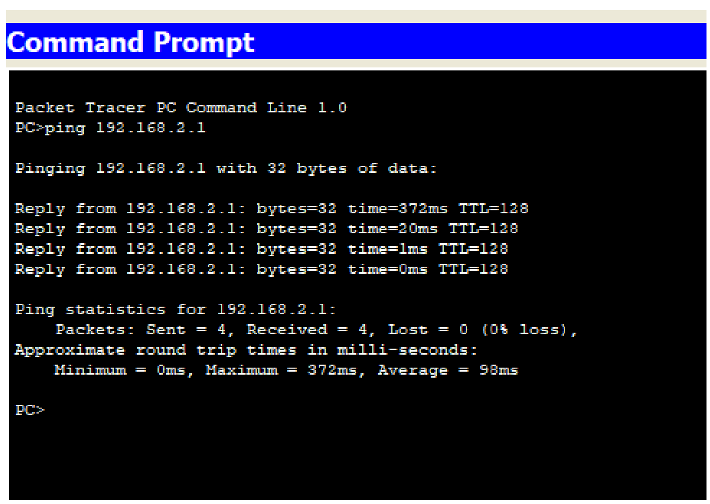
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.3.45 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int se0/1/1
Router(config-if)#ip add 192.168.8.44 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
00:04:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.8.2 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached

00:04:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.8.2 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached

00:04:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.7.1 on Serial0/1/0 from
LOADING to FULL, Loading Done

00:04:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.8.2 on Serial0/1/1 from
LOADING to FULL, Loading Done

Router(config-if)#int se0/1/0
Router(config-if)#ip add 192.168.7.45 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#exit
Router#
00:04:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.7.1 on Serial0/1/0 from
FULL to DOWN, Neighbor Down: Interface down or detached

00:04:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.7.1 on Serial0/1/0 from
FULL to DOWN, Neighbor Down: Interface down or detached

%SYS-5-CONFIG_I: Configured from console by console

00:04:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.7.1 on Serial0/1/0 from
LOADING to FULL, Loading Done

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.7.0 0.0.0.255 area 0
Router(config-router)#network 192.168.8.0 0.0.0.255 area 0
Router(config-router)#
```

Results:

Verify the network in simulation mode:



Ping command from pc0 to pc3



Discussion: The OSPF is used for the area where more routers are used and also large network usage. It mainly use is that it has unlimited hop count and Irrespective of other techniques it uses a concept of area to ease management and traffic control. We can clearly observe that providing different IP to the pc and different network to the router it is possible to transfer packet among them and construct a communication among them using OSPF algorithm. So, the experiment is valid.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 08

Name of Experiment: RSA algorithm in text and image encryption/decryption

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 08.12.22

Date of Submission: 05.01.23

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Introduction:

RSA encryption and decryption algorithms talk about the secrecy of messages between two users. It involves a public key and a private key generation. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The private key is not publicly known, it is only known to the receiver so that she/he can decrypt the encrypted message. These keys “public and private keys" for the RSA algorithm are generated using some mathematical operations.

Objective:

1. Confidentiality: Hiding information from unauthorized access
2. Integrity: Preventing information from Unauthorized modification
3. Availability: Should be easily available to authorized users

Apparatus:

1. Matlab Software
2. Computer

RSA Algorithm:

Description of the encryption and decryption procedures of RSA)

1. Find two large primes p and q and define n by n= p q
2. Find a large random integer d that is relatively prime to the integer (p-1)(q-1)
3. Compute the unique integer e in the range 1<e<(p-1)(q-1) from the formula ed = 1mod(p-1)(q-1)
4. Make known the public key, which consists of the pair of integers (e, n)
5. Represent M, the message to be transmitted, as an integer in the range {1,…,n};break M into blocks if it is too big.
6. Encrypt M into a cryptogram C by the rule c = Me (mod N)
7. Decrypt by using the private key d and the formula D = Cd(mod N)

Methodology:

Step 1: RSA In Text Encryption and Decryption using Matlab

```
>> e = 3; n = 33; d = 7; %RSA parameters
>> y='JAHANGIRNAGAR'; %input string
z = double(y); %ASCII values
S=z-60; %to reduce size of the integer
>> for i=1:length(z)
Encrypt(i)=mod(S(i)^e, n);
end
char(Encrypt) % encrypted string
Encrypt=double(Encrypt);
for j=1:length(z)
Decrypt(j)=mod(Encrypt(j)^d, n);
end
Recover=char(Decrypt+60) %increase the decoded value by 60

ans =

    '▯▯▯▯▯▯▯▯▯▯▯▯▯'


Recover =

    'JAHANGIRNAGAR'

>> |
```

Step 2: RSA In Image Encryption and Decryption using Matlab

```
Command Window
>> e = 3; n = 33; d = 7; N=256;
>> I=imread('peppers.png');
>> I=rgb2gray(I);
>> I=imresize(I,[N, N]);
>> subplot(2,2,1)
>> imshow(I)
title('Original Image')
>> I=double(I);
R=mod(I,16);
%Remainder of the image
for i=1:N
for j=1:N
Q(i,j)=uint8((I(i,j)/16)-0.5);
% Quiescent of the image
end
end

>> Q=double(Q);
for i =1:N
for j = 1:N
Qe(i, j)=mod(Q(i,j)^e, n);
Re(i, j)=mod(R(i,j)^e, n);
%Decryption of image
Qd(i, j)=mod((Qe(i,j))^d, n);
Rd(i, j)=mod((Re(i,j))^d, n);
end
end
```

```
>> Rec=Qd*16+Rd;
subplot(2,2,2)
imshow(uint8(Qe))
title('Encrypted Quiescent Image')
subplot(2,2,3)
imshow(uint8(Re))
title('Encrypted Remainder Image')
subplot(2,2,4)
imshow(uint8(Rec))
title('Decrypted Image')
```

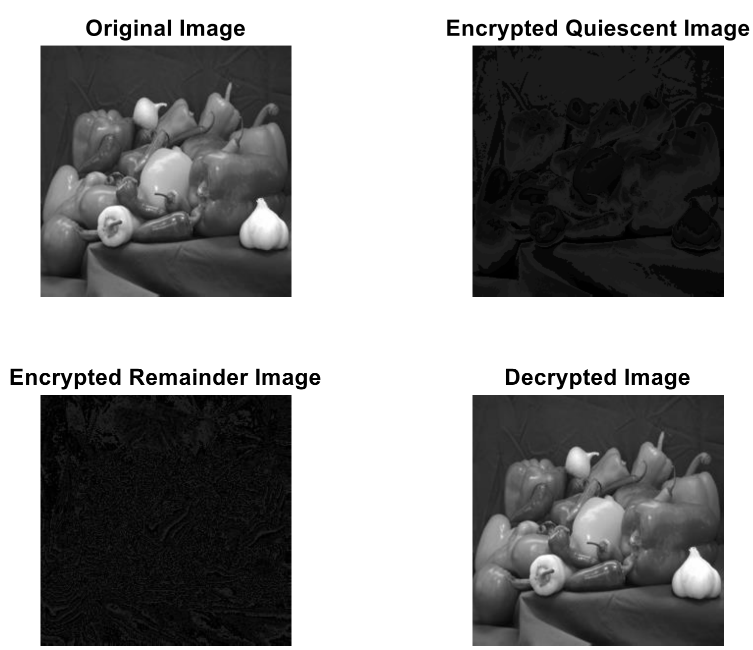
Step 2: RSA In RGB Image Encryption and Decryption using Matlab

Cn_lab9.m

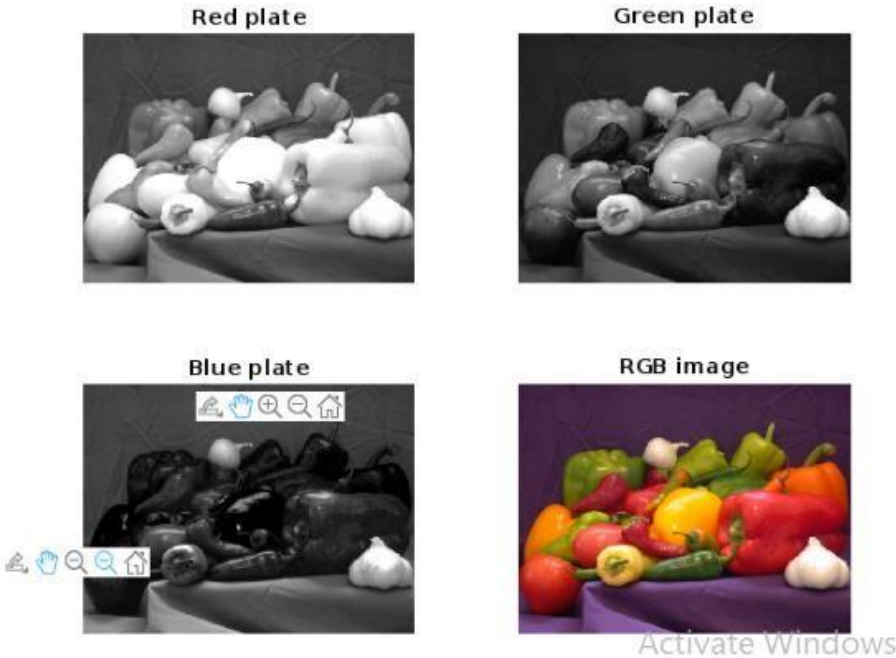
```
I=imread('peppers.png');
I1=I(:,:,1); %red plate
I2=I(:,:,2); %green plate
I3=I(:,:,3); %blue plate
subplot(2,2,1)
imshow(I1)
title('Red plate')
subplot(2,2,2)
imshow(I2)
title('Green plate')
subplot(2,2,3)
imshow(I3)
title('Blue plate')
Y=cat(3,I1,I2,I3);
subplot(2,2,4)
imshow(Y)
title('RGB image')
```

Results:

Output of Image Encryption and Decryption:



Output of RGB Image plane



Discussion:

The cryptography mechanism is using the RSA algorithm with the public key encryption to increase the security levels of the encrypted. Here one key is needed to encrypt, and another key is needed to decrypt the image. Finally, the image cryptography experiment provides the feasibility of security to the image in network security. The data is not viewed by anyone without knowledge of cryptography. The image consists of secrets, and it is going to be encrypted it is called an original image that may contain the data. The Original image is encrypted by the key which is generated by the RSA algorithm. It is converting the image into the cipher text. Finally, the ciphers text is decrypted by another one decrypt key which so generated by the RSA algorithm. And it converts the cipher text into the resultant image.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 09

Name of Experiment: DNS Server Configuration

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 05.01.23

Date of Submission: 19.01.23

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Experiment Name: DNS Server Configuration

Objective: The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names meaningful for users to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. Main objective of this experiment is to become familiar with DNS configuration using packet tracer.

Apparatus:

1. Packet Tracer software
2. Server-PT (2)
3. 1841 Router (1)
4. Switch (2)
5. Generic PC (4)

Network Diagram:

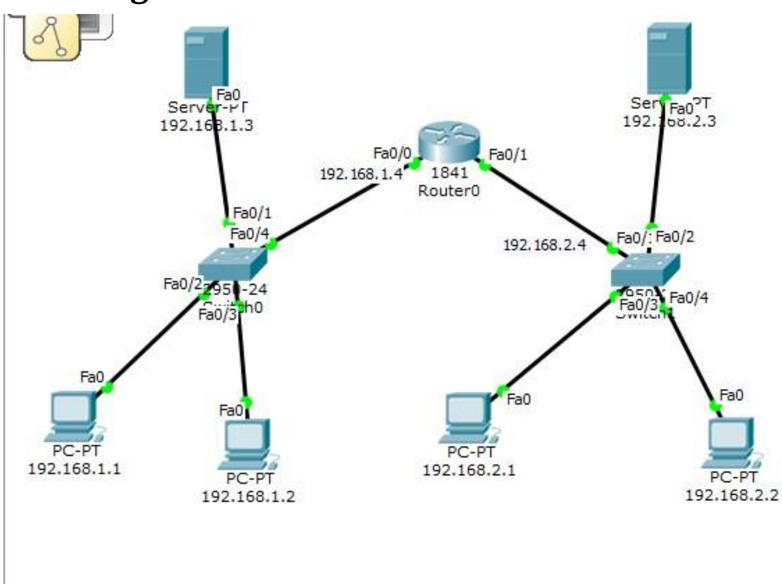


Fig. Network Diagram of DNS server configuration

Methodology:

Step 1: As the above network topology, for fast ethernet port (Fa0/0) of Router-0, set 192.168.1.4 IP for the default gateway, then set IP for the DNS server statically (one click on DNS server > Desktop > IP configuration).

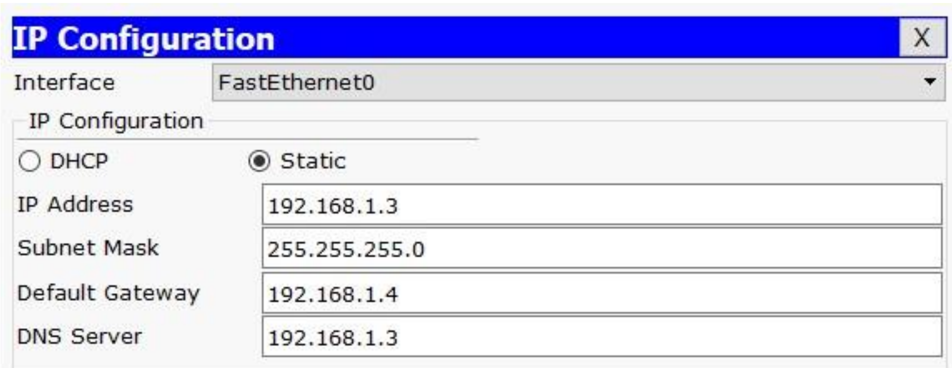


Fig-IP configuration of JU server

for fast ethernet port (Fa0/1) of Router-0, set 192.168.2.4 IP for the default gateway, then set IP for the DNS server statically (one click on DNS server > Desktop > IP configuration).

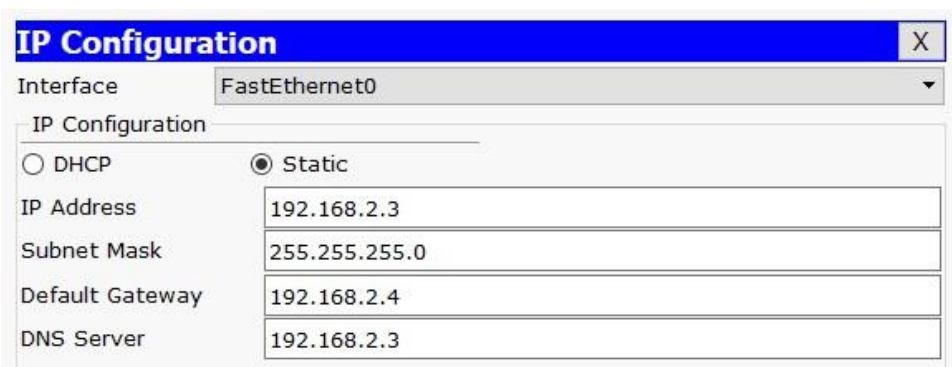


Fig-IP configuration of DU server

Step-2: Set IP for PC statically, with 198.168.1.1 and 198.168.1.2 for JU DNS server field.

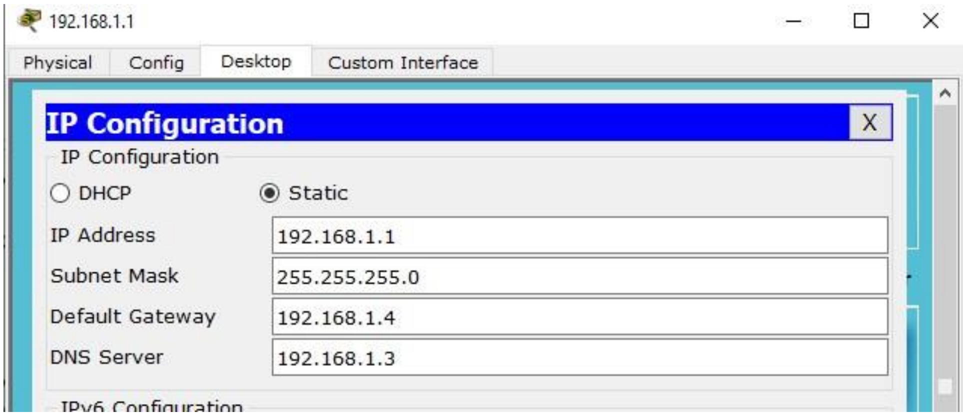


Fig-IP configuration of PC-1

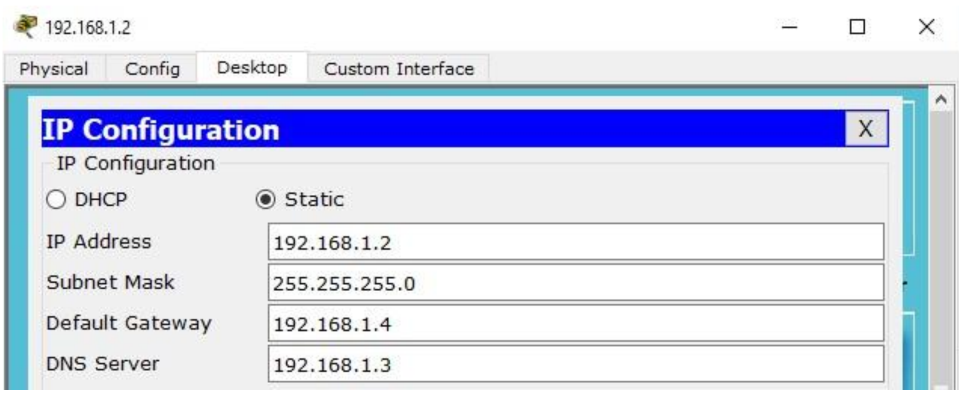


Fig-IP configuration of PC-2

Step-2: Set IP for PC statically, with 198.168.2.1 and 198.168.2.2 for DU DNS server field.

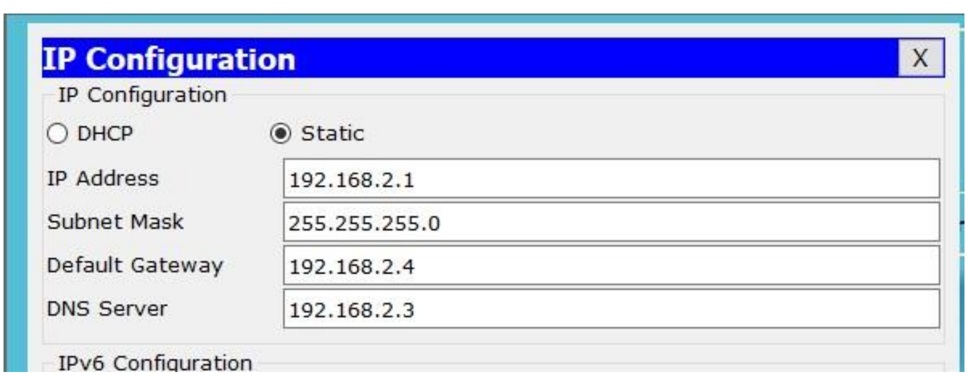


Fig-IP configuration of PC-1

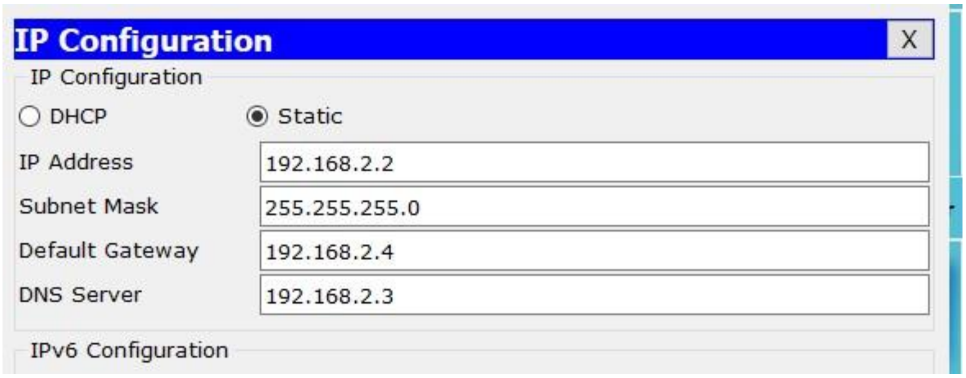
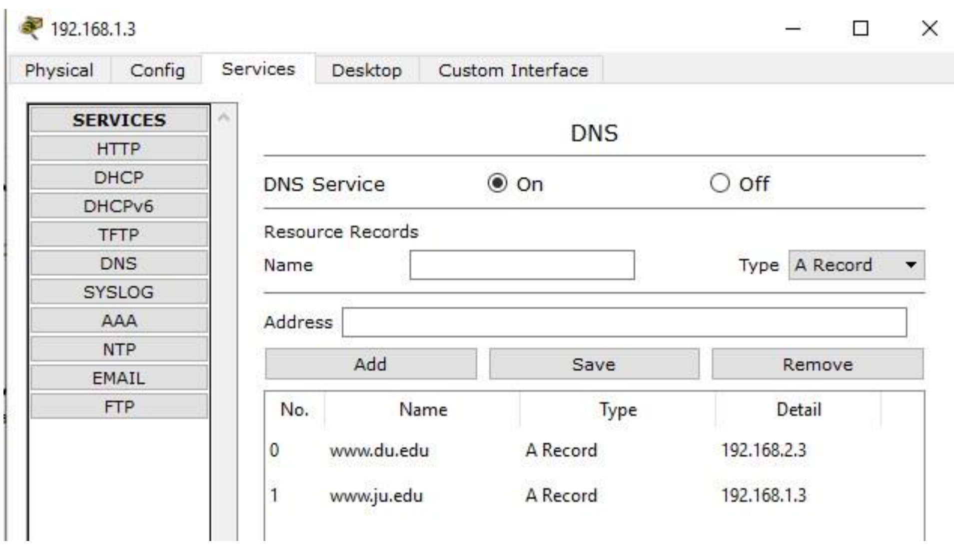
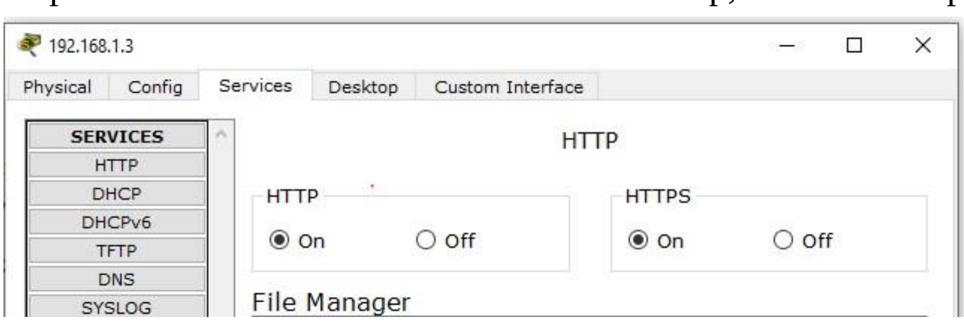


Fig-IP configuration of PC-2

Step 4: one click on DNS server > services > DNS, enable the DNS service, in the name field we should put the name of the website which the user can open it from, type field should be A Record which means that IP address for the website have one name, address field should be the web server IP address



Step 5: one click on web server > services > http, enable the http and https services.



Now in the file manager table, in the index row, click edit and write the html code for your website (here it is www.JU.edu) Then click save, yes to replace the file.

File Name: ju.html

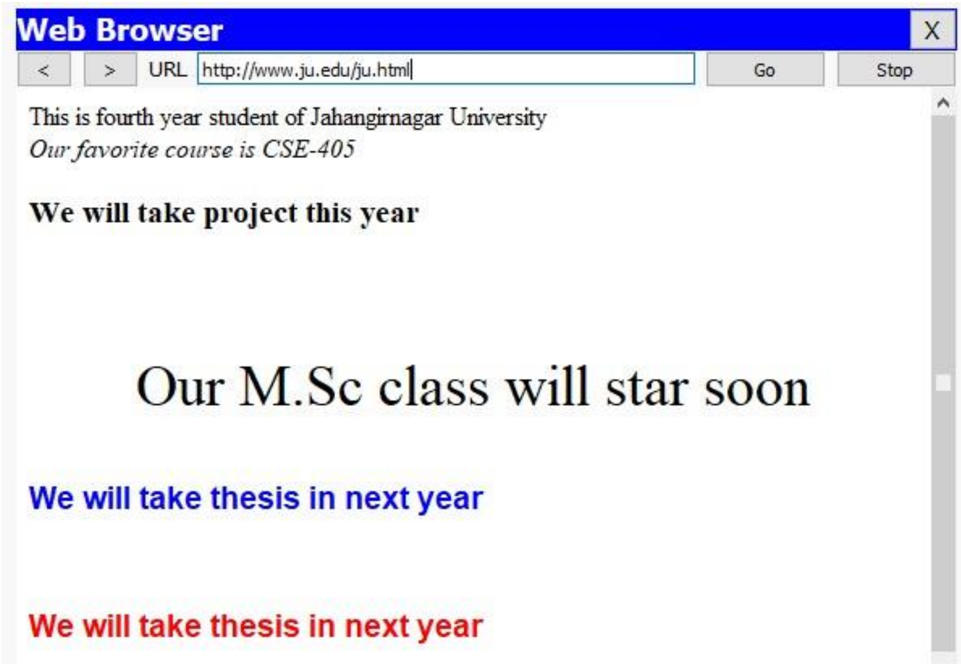
```
<html>
<head>
<title>
<h1>This is CSE of Jahangirnagar University<h1>
</title>
</head>
<body>
This is fourth year student of Jahangirnagar University<br/>
<i> Our favorite course is CSE-405 </i> <br/>
<h3> We will take project this year </h3> <br/>
<p style="font-size:36px; text-align:center;">
Our M.Sc class will star soon </p>
<h3 style="font-family:arial;color:blue;"> We will take thesis in
next year </h3> <br/>
<h3 style="font-family:arial;color:red;"> We will take thesis in
next year </h3> <br/>
</body>
</html>
```

Step-6: Follow the same procedure for DU server to http and https server and load the html code for du.html on DU server.

```
<html>
<head>
<title>
<h1>This is CSE of Dhaka University<h1>
</title>
</head>
<body>
This is fourth year student of Dhaka University<br/>
<i> Our favourite course is CSE-206 </i> <br/>
<h3> We will take project this year </h3> <br/>
<p style="font-size:36px; text-align:center;">
Our M.Sc class will star soon </p>
<h3 style="font-family:arial;color:blue;"> We will take thesis in
next year </h3> <br/>
<h3 style="font-family:arial;color:red;"> We will take thesis in
next year </h3> <br/>
</body>
</html>
```

Results

- one click on any PC > Desktop > Web Browser, enter the name that we set in DNS which is (www.du.edu or www.ju.edu), the result will be as shown below.



- Verify ping, tracert and ipconfig commands on the command prompt of the client.

```
Packet Tracer PC Command Line 1.0
PC>ping www.ju.edu

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms
```

```
PC>tracert www.ju.edu

Tracing route to 192.168.1.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.3

Trace complete.
```

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::207:ECFF:FEE4:503
   IP Address......................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.1.4
```

Using the website address is faster than using the website name, because the request from a PC will go directly to the web server. But using the website name, the request will go first to the DNS server where the name-IP table is, DNS server find the IP address for the name asked and resend it to the web server that have that IP address.

Discussion:

The Domain Name System (DNS) is a standard technology for managing public names of Web sites and other Internet domains. DNS technology allows you to type names into your Web browser like google.com and your computer to automatically find that address on the Internet.

Course Code: CSE 360

Course Name: Computer Networks Laboratory

Experiment No: 10

Name of Experiment: Socket programming

Submitted By

Name: Md. Ashraful Morsalin

Class Roll: 377

Exam Roll: 191356

Date of Performance: 19.01.23

Date of Submission: 19.03.23

Department of Computer Science & Engineering

Jahangirnagar University, Savar, Dhaka.

Experiment Name: Socket programming

Objective:

- To create sockets using Python
- Connect to web i.e Google using socket
- To establish client server communications
- To converse with the server and the client

Apparatus:

- Python IDLE
- PCs

Methodology:

Step 1: First of all, create sockets and connect to Google using Python programming language in Python IDLE using following code:

```
import socket

s = socket.socket(socket.AF_INET,

socket.SOCK_STREAM) print("Socket successfully

created") port = 80

host_ip = socket.gethostbyname('www.google.com')

s.connect((host_ip,port))

print('IP of www.google.com', host_ip)
```

Step 2: Create server side and client side communication methods using following code segment:

Server Side:

```
import socket

LOCALHOST = '127.0.0.1'
PORT = 8080

server = socket.socket(socket.AF_INET,socket.SOCK_STREAM)

server.bind((LOCALHOST, PORT))

server.listen(1) print("Server started")

print("Writing for client request..")

clientConnection, clientAddress = server.accept()

print("Connected client:", clientAddress)

msg='' while True:

in_data = clientConnection.recv(1024)

msg = in_data.decode()

if msg == 'bye':

    break

print("From Client:", msg)

out_data = input()

clientConnection.send(bytes(out_data,'UTF-8'))

print("Client disconnected....")

clientConnection.close()
```

Client Side:

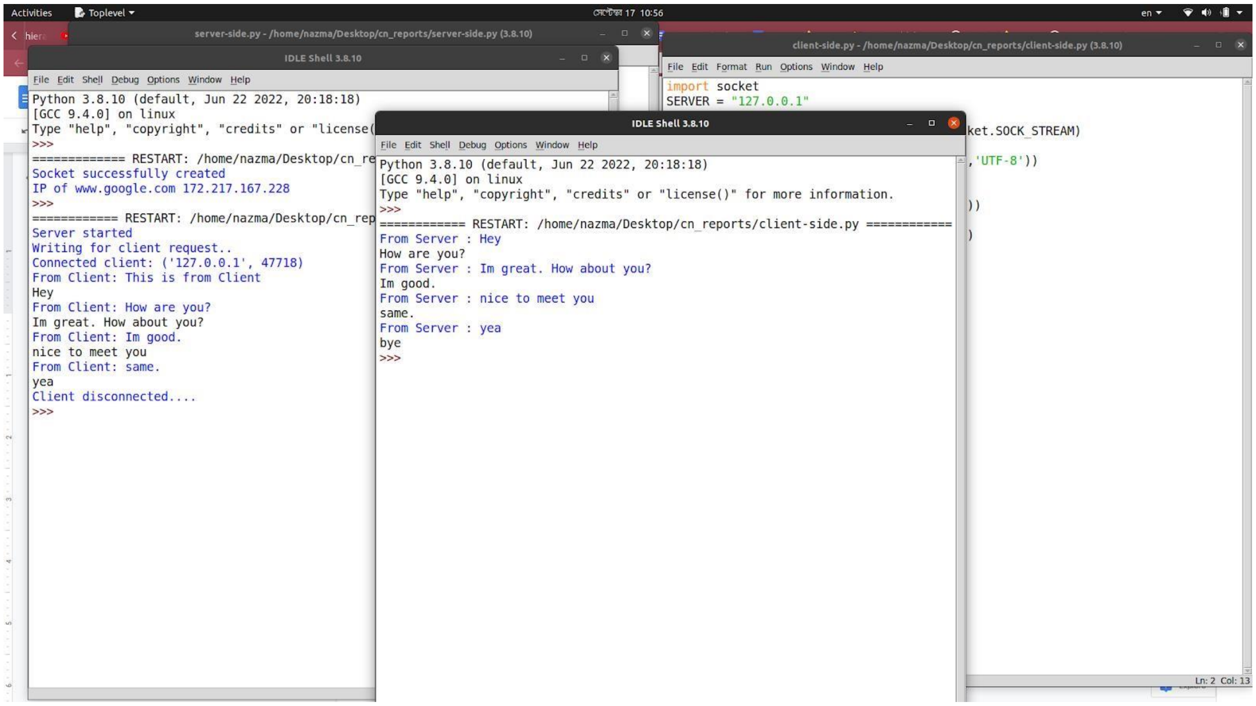
```
import socket
```

```
SERVER = "127.0.0.1"
PORT = 8080
client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client.connect((SERVER, PORT))
client.sendall(bytes("This is from Client",'UTF-8'))
while True:
in_data = client.recv(1024)
print("From Server :" ,in_data.decode())
out_data = input()
client.sendall(bytes(out_data,'UTF-8'))
if out_data=='bye':
    break client.close()
```

Step 3: Communicate from both ends of server and client side.

Result and Discussion:

The socket is successfully created and connected to Google.



Communication between both server side and client side: