NETAJI SUBHAS UNIVERSITY OF TECHNOLOGY

PRACTICAL FILE

Name : Arsh Poddar

Roll Number : 2021UEC2518

Branch : Electronics and Communication Engineering - 1

Course Name : Computer Networks

Course Code : ECECC19

INDEX

Experiment : 1

Aim : To Generate an Exponentially distributed random number from a Uniformly distributed random number.

Software Used : MATLAB

Theory :

A uniform distribution, sometimes also known as a rectangular distribution, is a distribution that has constant probability. The probability density function of the continuous uniform distribution is

$$f(x) = \begin{cases} \frac{1}{b-a} & \text{for } a \leq x \leq b, \\ 0 & \text{for } x < a \text{ or } x > b \end{cases}$$

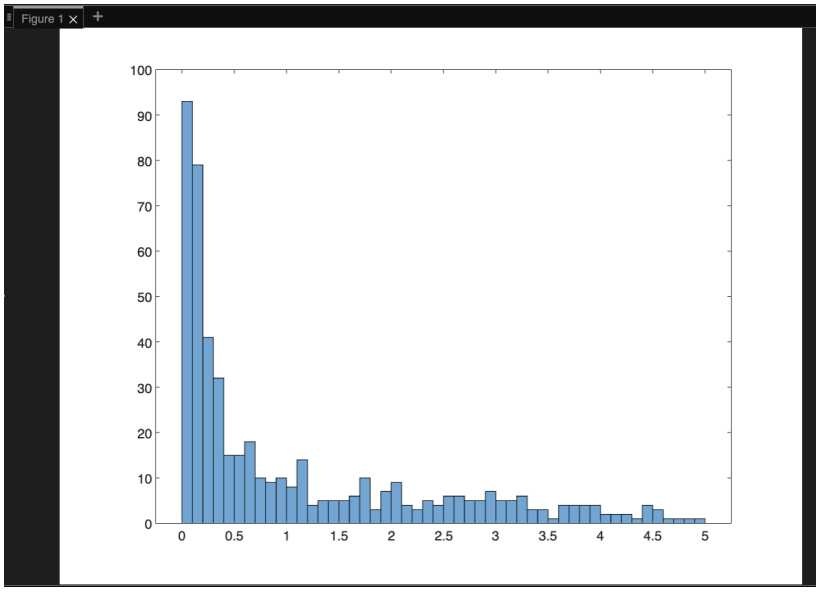
The probability density function of an exponential distribution is

$$f(x) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

Code :

```
% AIM : To Generate an Exponentially distributed random number from a Uniformly distributed random number.
% Name : Arsh Poddar
% Roll Number : 2021UEC2518
% Branch and section : ECE-1
% Subject : Computer Networks

clc;
clear all;
close all;
n=500;
a=zeros(n,1);
lamb=5;
x = rand(n,1); %generate uniformly distributed random number
for i=1:n
a(i)=lamb*exp(-lamb*x(i)); %exponential distribution
end
histogram(a,(n/10))
```

Output :



Result : An exponentially distributed random number is generated from a uniformly distributed random number.

Experiment : 2

Aim : Configure and analyze bus, ring, star, mesh, and hybrid network topology with wired vs wireless networks.

Software Used : Cisco Packet Tracer

Theory :

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required=N*(N-1).

Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2.

Advantages of mesh topology

- Communication is very fast between the nodes.
- It is robust. The fault is diagnosed easily.
- Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Problems with mesh topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

Bus Topology

Alternatively called line topology, bus topology is a network setup where each computer and network device is connected to a single cable or backbone. Depending on the type of computer network card, a coaxial cable or an RJ-45 network cable is used to connect them together. The following sections contain both the advantages and disadvantages of using a bus topology with your devices.

Advantages of bus topology

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

Problems with bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

Star Topology

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD (Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

Advantages of star topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.

· It is Robust. If one link fails only that link will affect and not other than that.

· Easy to fault identification and fault isolation.

· Star topology is cost-effective as it uses inexpensive coaxial cable.

Problems with star topology

· If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.

· The cost of installation is high. Performance is based on the single concentrator i.e. hub.

Ring Topology

In this topology, it forms a ring connecting devices with exactly two neighbouring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e.., it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

Advantages of ring topology

· The data transmission is high-speed.

· The possibility of collision is minimum in this type of topology.

· Cheap to install and expand. It is less costly than a star topology.

Problems with ring topology

· The failure of a single node in the network can cause the entire network to fail.

· Troubleshooting is difficult in this topology.

· The addition of stations in between or the removal of stations can disturb the whole topology.

· Less secure.

Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. It is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above.

Advantages of hybrid topology

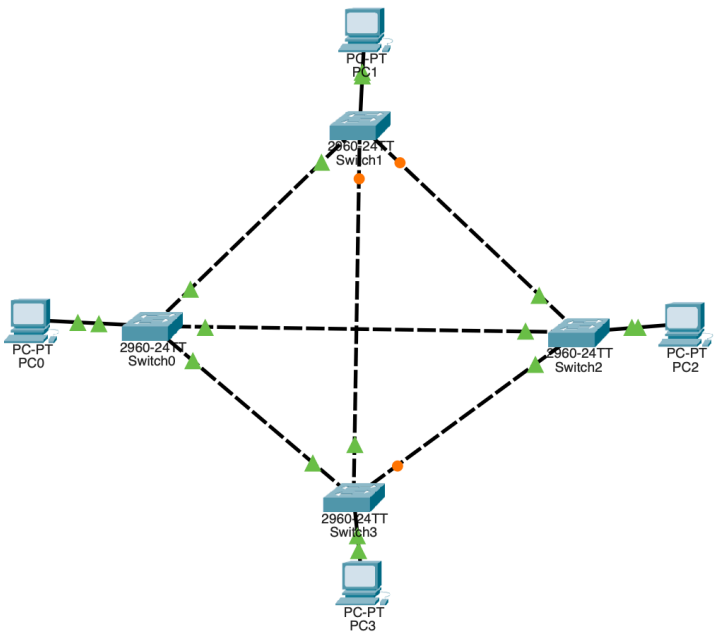
- This topology is very flexible.
- The size of the network can be easily expanded by adding new devices.

Problems with hybrid topology

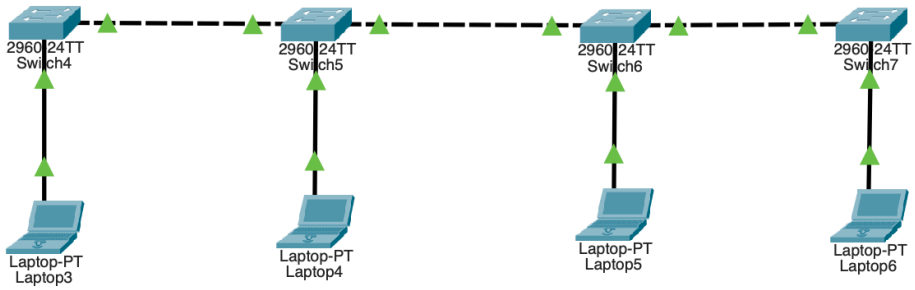
- It is challenging to design the architecture of the Hybrid Network.
- Hubs used in this topology are very expensive.
- The infrastructure cost is very high as a hybrid network requires a lot of cabling and network devices.

Simulations :

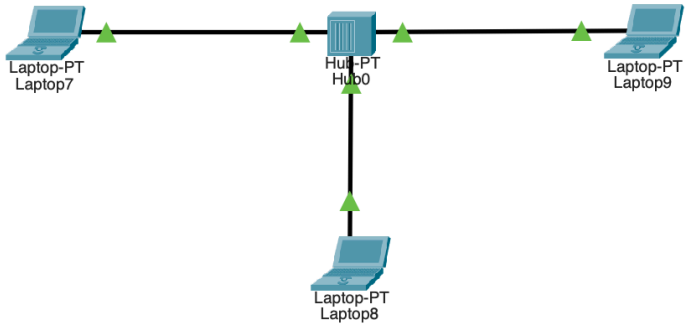
Mesh Topology



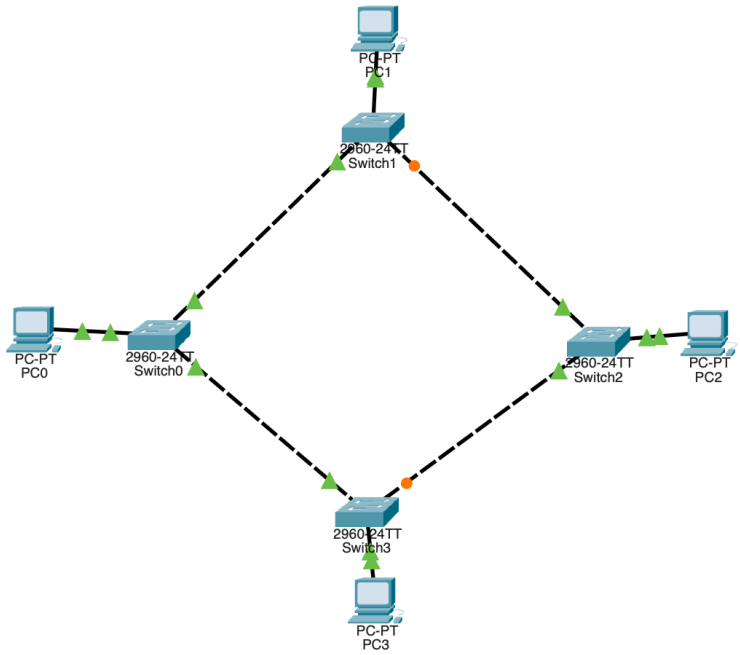
Bus Topology



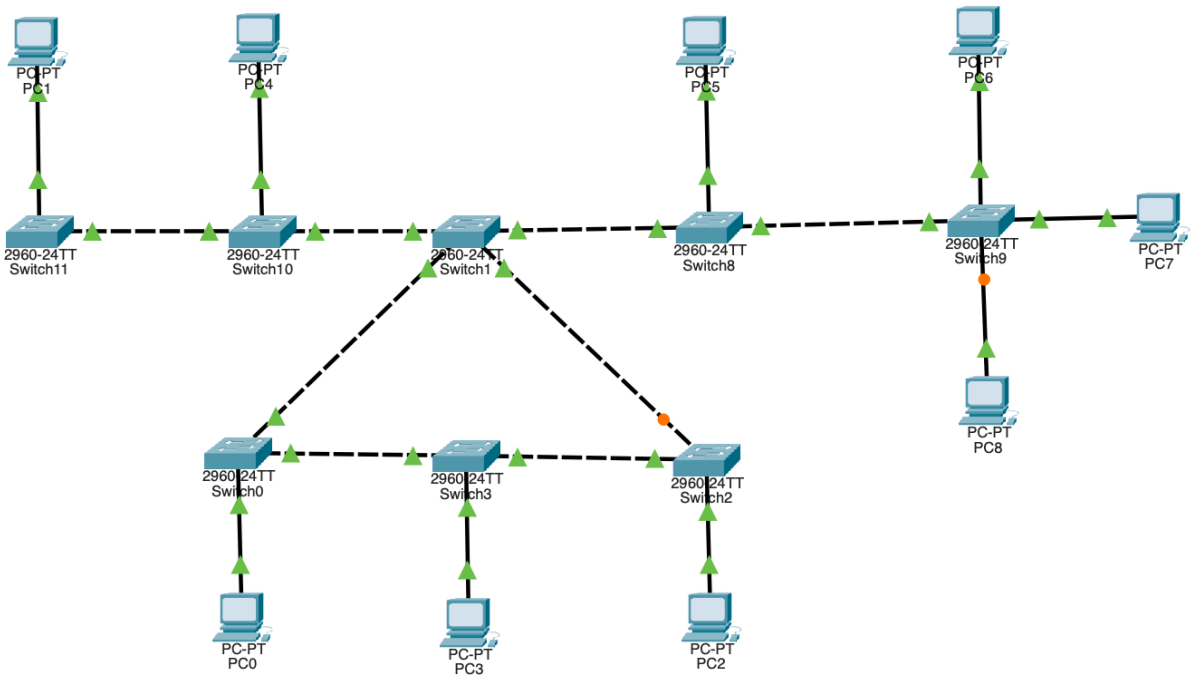
Star Topology



Ring Topology



Hybrid Topology



Result : Bus, ring, star, mesh, hybrid topologies were configured and analyzed.

Experiment : 3

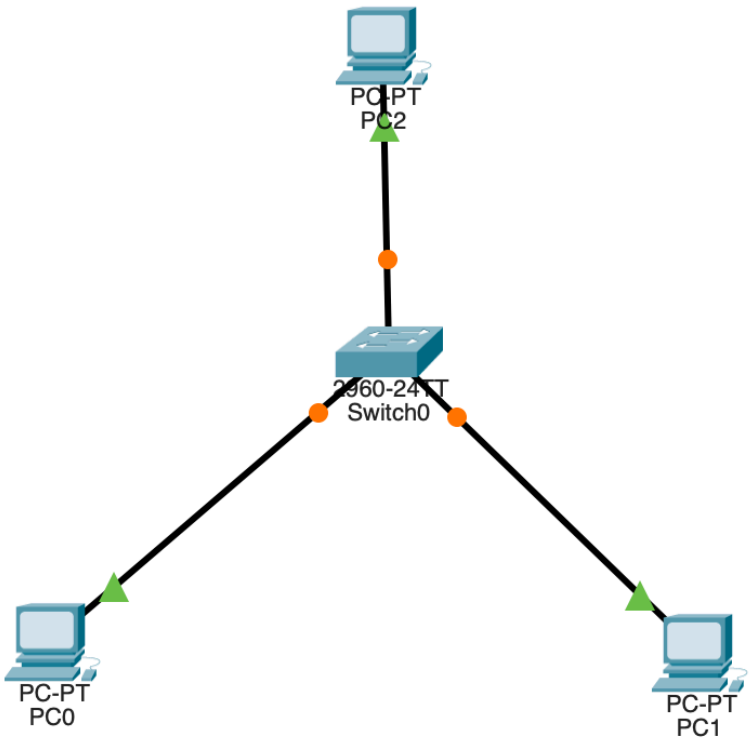
Aim : Connect the computers in Local Area Network, and Study of basic network commands and network configuration commands.

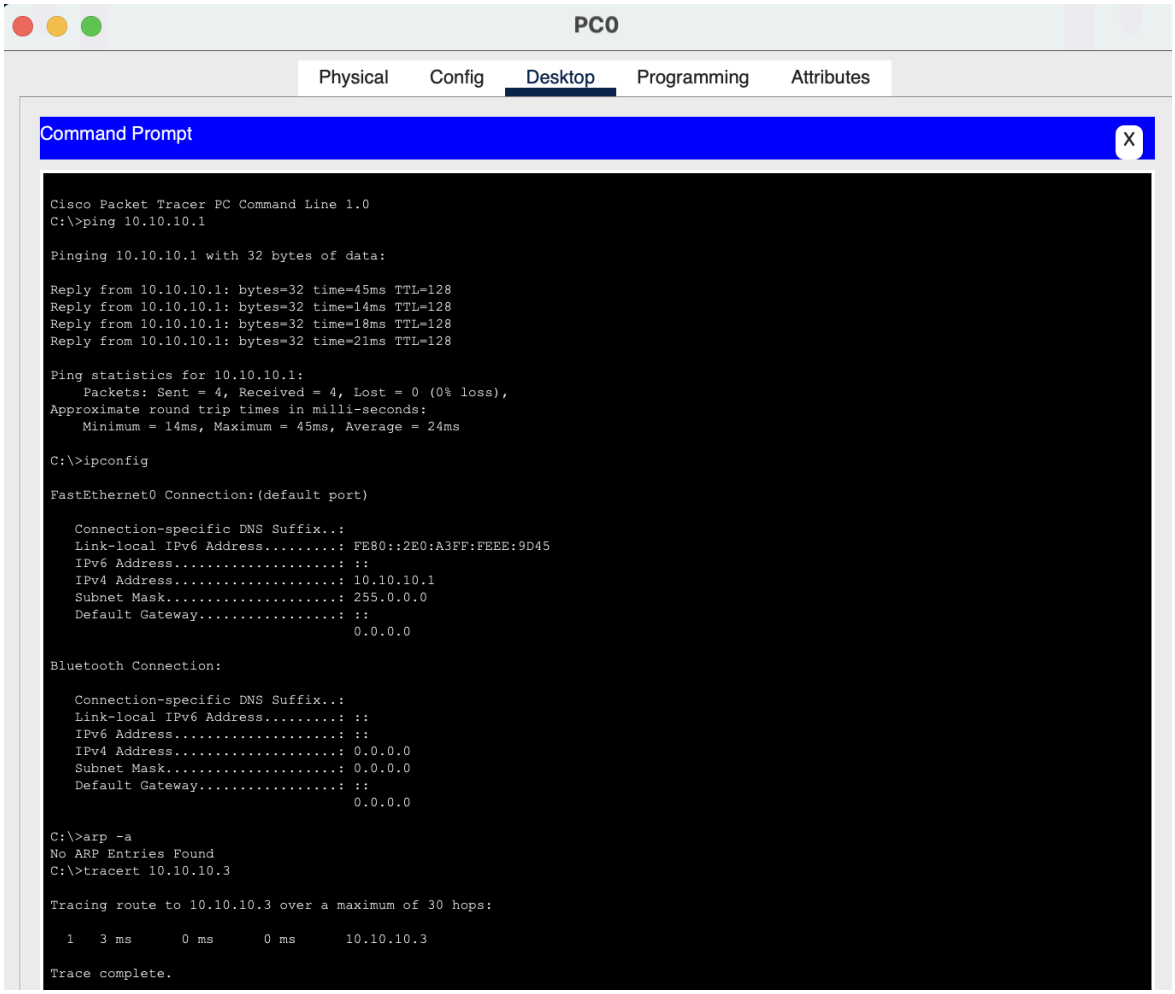
Software Used : Cisco Packet Tracer

Theory : Basic Commands:

1. ping – Check the connection between source and destination nodes
2. ipconfig – Check the IP configuration of the end device
3. tracert – Trace the route from source to destination
4. arp –a – ARP is used by a computer system to find another computer's MAC address based on its IP address

Simulations :





IP configurations - PC0 - 10.10.10.1 , PC1 - 10.10.10.2 , PC2 - 10.10.10.3

Result : Computers in Local Area Network were connected and study of basic network command and network configuration commands was carried out.

Experiment : 4

Aim : Study of the following Network Devices in Detail: Repeater, Hub, Switch, Bridge, Router, Gate way.

Software Used : Cisco Packet Tracer

Theory :

1. Repeater -

It is a 2-port device that operates in the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

2. Hub -

It is a multiport device which operates in the physical layer of the OSI model. A hub is used to primarily broadcast data. It cannot filter the data, i.e., it is a non-intelligent device that sends messages to all the ports.

3. Switch -

It is a multiport device that works in the data link layer. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device. It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.

4. Bridge -

It is a 2-port device which operates in the data link layer. Bridges are used to connect two subnetworks. It is a repeater, which adds on the functionality of filtering content by reading the MAC addresses of the source and destination.

5. Router -

It is a multiport device which operates in the network layer of the OSI model. It connects different networks together and sends data packets from one network to another. Switches are also responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, and consults its routing tables to decide the optimal route.

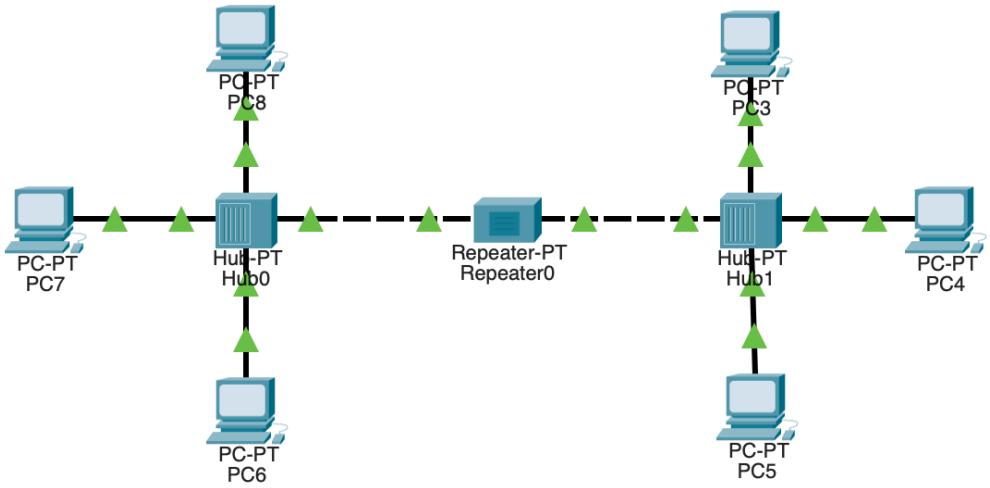
6. Gateway –

Gateway is the connecting point of any network that helps it to connect with different networks. The gateway monitors and controls all the incoming and outgoing traffic of the network. Gateways are also known as protocol converters because they help to convert protocols

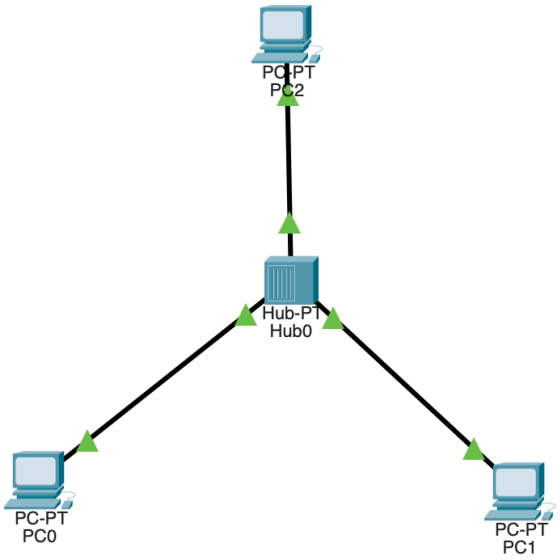
supported by traffic of the different networks into those that are supported by this network. Because of that, it makes smooth communication between two different networks.

Simulations :

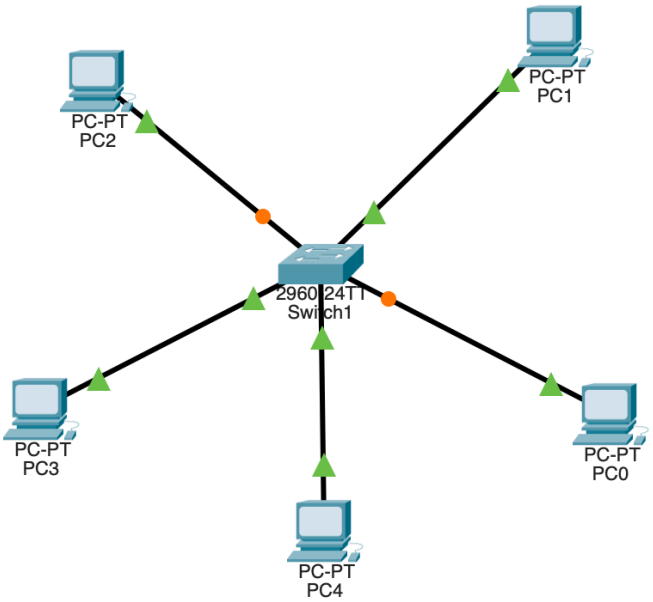
Repeater



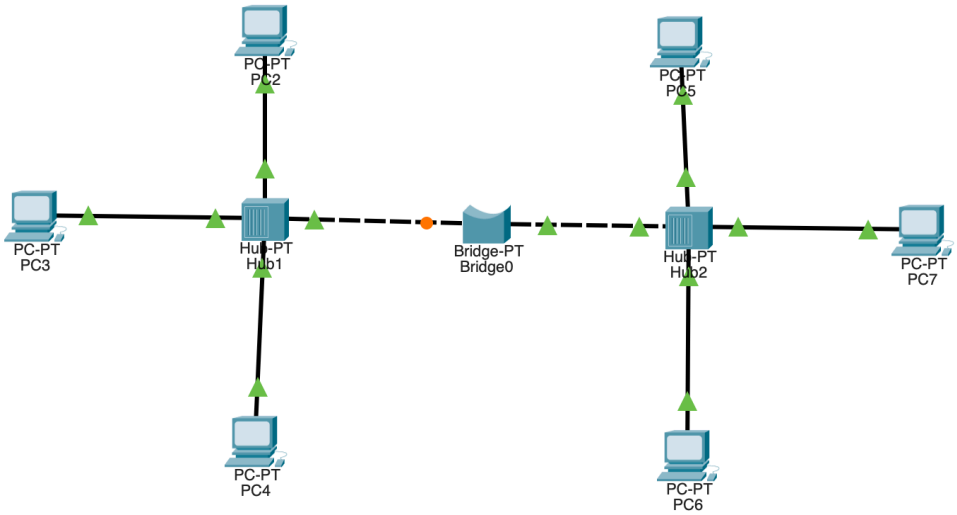
Hub



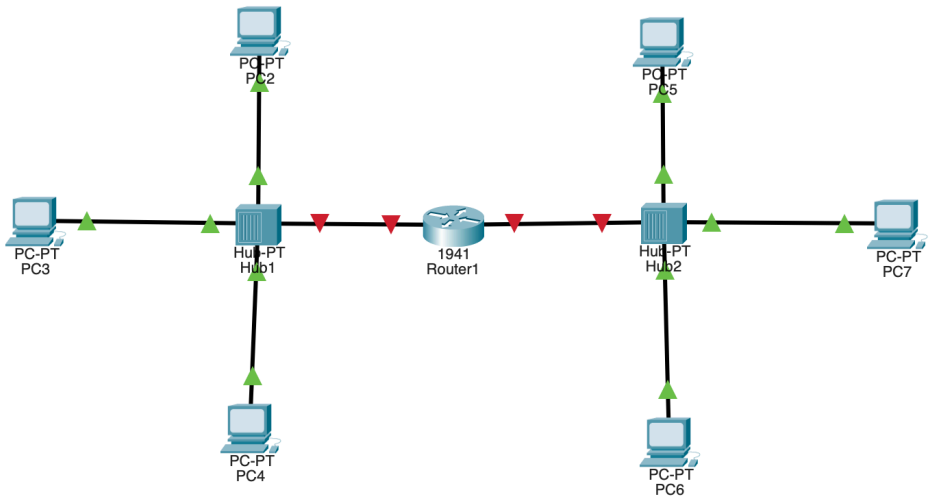
Switch



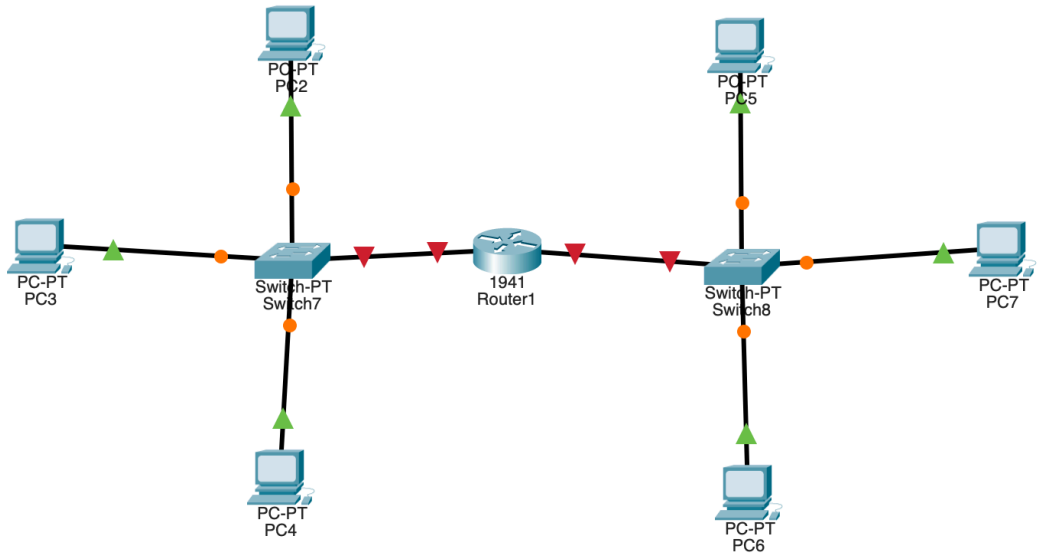
Bridge



Router



Gate way



Result : Successfully studied and simulated various network devices.

Experiment : 5

Aim : To evaluate STOP and WAIT protocol and evaluate its performance.

Software Used : MATLAB

Theory :

Stop and Wait is a reliable transmission flow control protocol. This protocol works only in Connection Oriented (Point to Point) Transmission. The Source node has a window size of ONE. After transmission of a frame the transmitting (Source) node waits for an acknowledgement from the destination node. If the transmitted frame reaches the destination without error, the destination transmits a positive acknowledgement. If the transmitted frame reaches the Destination with error, the receiver destination does not transmit an acknowledgement. If the transmitter receives a positive acknowledgement it transmits the next frame if any. Else if its acknowledgement receive timer expires, it retransmits the same frame.

1. Start with the window size of 1 from the transmitting (Source) node.

2. After transmission of a frame the transmitting (Source) node waits for a reply (Acknowledgement) from the receiving (Destination) node.

3. If the transmitted frame reaches the receiver (Destination) without error, the receiver (Destination) transmits a Positive Acknowledgement.

4. If the transmitted frame reaches the receiver (Destination) with error, the receiver (Destination) does not transmit acknowledgement.

5. If the transmitter receives a positive acknowledgement it transmits the next frame if any. Else if the transmission timer expires, it retransmits the same frame again.

6. If the transmitted acknowledgment reaches the Transmitter (Destination) without error, the Transmitter (Destination) transmits the next frame if any.

7. If the transmitted frame reaches the Transmitter (Destination) with error, the Transmitter (Destination) transmits the same frame.

8. This concept of the Transmitting (Source) node waiting after transmission for a reply from the receiver is known as STOP and WAIT.

Code :

```
% AIM : To evaluate STOP and WAIT protocol and evaluate its performance
% Name : Arsh Poddar
% Roll Number : 2021UEC2518
% Branch and section : ECE-1
% Subject : Computer Networks

close all;
clear all;
clc;
n = 8;%number of frames
i = 1;
while i<n
fprintf('Transmitting frame %d\n',i);
s = randi(10,1,1);
if s<=3
fprintf('Time out \n %d\n',i);
else
fprintf('Received frame %d\n',i);
i = i+1;
end
end
```

Output :

Command Window

```
Transmitting frame 1
Received frame 1
Transmitting frame 2
Received frame 2
Transmitting frame 3
Time out
 3
Transmitting frame 3
Received frame 3
Transmitting frame 4
Received frame 4
Transmitting frame 5
Received frame 5
Transmitting frame 6
Received frame 6
Transmitting frame 7
Received frame 7
>>
```

Result : Stop and Wait protocol is evaluated using MATLAB.

Experiment : 6

Aim : To simulate SLIDING WINDOW protocol and evaluate its performance with variation of window size.

Software Used : MATLAB

Theory :

A sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the Data Link Layer (OSI model) as well as in the Transmission Control Protocol (TCP). Conceptually, each portion of the transmission (packets in most data link layers, but bytes in TCP) is assigned a unique consecutive sequence number, and the receiver uses the numbers To place received packets in the correct order, discarding duplicate packets and identifying missing ones.

The problem with this is that there is no limit on the size of the sequence number that can be required. By placing limits on the number of packets that can be transmitted or received at any given time, a sliding window protocol allows an unlimited number of packets to be communicated using fixed-size sequence numbers. The term "window" on the transmitter side represents the logical boundary of the total number of packets yet to be acknowledged by the receiver. The receiver informs the transmitter in each acknowledgment packet the current maximum receiver buffer size (window boundary).

The TCP header uses a 16 bit field to report the received window size to the sender. Therefore, the largest window that can be used is 216 = 64 kilobytes. In slow-start mode, the transmitter starts with low packet count and increases the number of packets in each transmission after receiving acknowledgment packets from the receiver. For every ack packet received, the window slides by one packet (logically) to transmit one new packet. When the window threshold is reached, the transmitter sends one packet for one packet received.

In this simulation we have used the Go Back-N sliding window protocol. In Go-Back-N ARQ, N is the sender's window size. Suppose we say that Go-Back3, which means that the three frames can be sent at a time before expecting the acknowledgment from the receiver. It uses the principle of protocol pipelining in which multiple frames can be sent before receiving the acknowledgment of the first frame. If we have five frames and the concept is Go-Back-3, which means that the three frames can be sent, i.e., frame no 1, frame no 2, frame no 3 can be sent before expecting the acknowledgment of frame no 1. In Go-Back-N ARQ, the frames are numbered sequentially as Go-Back-N ARQ sends the multiple frames at a time that requires the numbering approach to distinguish the frame from another frame, and these numbers are known as the sequential numbers. 00:00/07:31. The number of frames that can be sent at a time totally depends on the size of the sender's window.

So, we can say that 'N' is the number of frames that can be sent at a time before receiving the acknowledgment from the receiver. If the acknowledgment of a frame is not received within an agreed-upon time period, then all the frames available in the current window will be retransmitted.

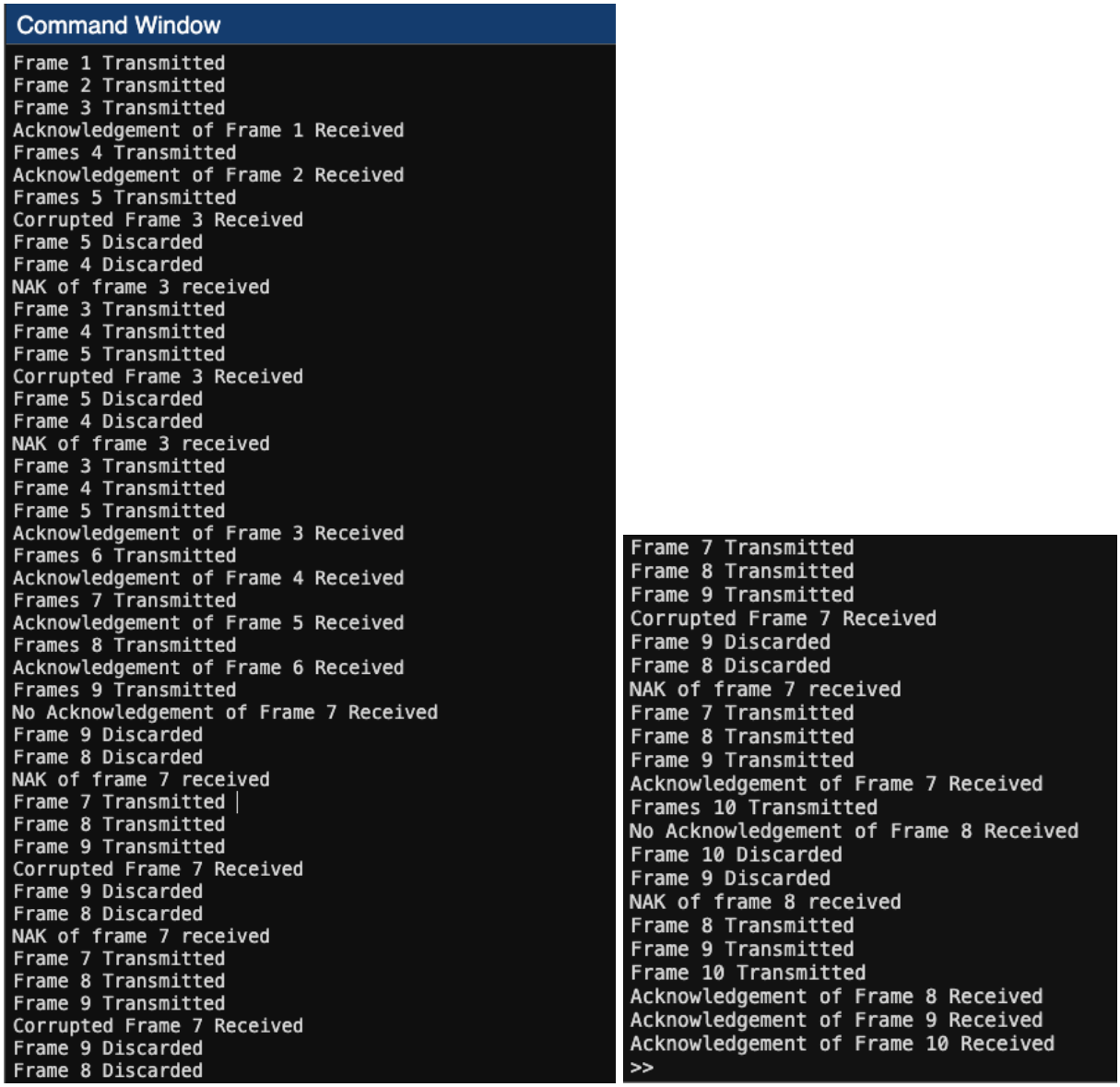
Code :

```
% AIM : To simulate SLIDING WINDOW protocol and evaluate its performance with variation of window size.
% Name : Arsh Poddar
% Roll Number : 2021UEC2518
% Branch and section : ECE-1
% Subject : Computer Networks

clc;
n = 10;
w = 3;

while w >= n
    w = input('Invalid Window size - Cannot be bigger than or equal to the number of frames. \n Re-enter Window size:');
end

sentframes = 0;
windowframes = 0;
unsentframes = n;
pt = 1;
flag = 0;
flag2 = 0;
a = 1:n;
threshold = 32;
dropcount = 0;

pause(1.0);

while flag == 0 && pt <= n
    if flag2 == 0
        for i = 1:w
            fprintf('Frame %d Transmitted \n', a(pt));
            unsentframes = unsentframes - 1;
            windowframes = windowframes + 1;
            pt = pt + 1;
        end
        pause(2.0);
        flag2 = 1;
    end

    noise = randi(100, 1, 1);
    pause(2.0);
```

```
    if noise > threshold
        fprintf('Acknowledgement of Frame %d Received\n', a(pt - w));
        sentframes = sentframes + 1;

        if pt == n + 1
            fprintf('Frames %d Transmitted \n', a(pt - 1));
        else
            fprintf('Frames %d Transmitted \n', a(pt));
        end

        windowframes = windowframes + 1;
        unsentframes = unsentframes - 1;

        if pt == n + 1 || a(pt) == n
            flag = 1;
        end

        pt = pt + 1;
    else
        dropcount = dropcount + 1;
        err = randi(10, 1, 1);

        if err > 5
            fprintf('Corrupted Frame %d Received \n', a(pt - w));
        else
            pause(1.0);
            fprintf('No Acknowledgement of Frame %d Received \n', a(pt - w));
        end

        for j = w - 1:-1:1
            fprintf('Frame %d Discarded \n', a(pt - w + j));
            windowframes = windowframes - 1;
            unsentframes = unsentframes + 1;
        end
```

```
        fprintf('NAK of frame %d received \n', a(pt - w));
        windowframes = windowframes - 1;
        unsentframes = unsentframes + 1;
        pt = pt - w;
        flag2 = 0;
    end
end

i = n - w + 1;

while i <= n
    noise = randi(100, 1, 1);
    pause(2.0);

    if noise > threshold
        fprintf('Acknowledgement of Frame %d Received\n', a(i));
        sentframes = sentframes + 1;
        i = i + 1;
    else
        dropcount = dropcount + 1;
        err = randi(10, 1, 1);

        if err > 5
            fprintf('Corrupted Frame %d Received\n', a(i));
        else
            pause(1.0);
            fprintf('No Acknowledgement of Frame %d Received\n', a(i));
        end

        for j = n:-1:i + 1
            fprintf('Frame %d Discarded \n', a(j));
            windowframes = windowframes - 1;
            unsentframes = unsentframes + 1;
        end

        fprintf('NAK of frame %d received\n', a(i));
        windowframes = windowframes - 1;
        unsentframes = unsentframes + 1;

        pause(2.0);

        for k = i:n
            fprintf('Frame %d Transmitted\n', a(k));
            windowframes = windowframes + 1;
            unsentframes = unsentframes - 1;
        end
    end
end
```

Output :



Result : Sliding window protocol is evaluated using MATLAB.

Experiment : 7

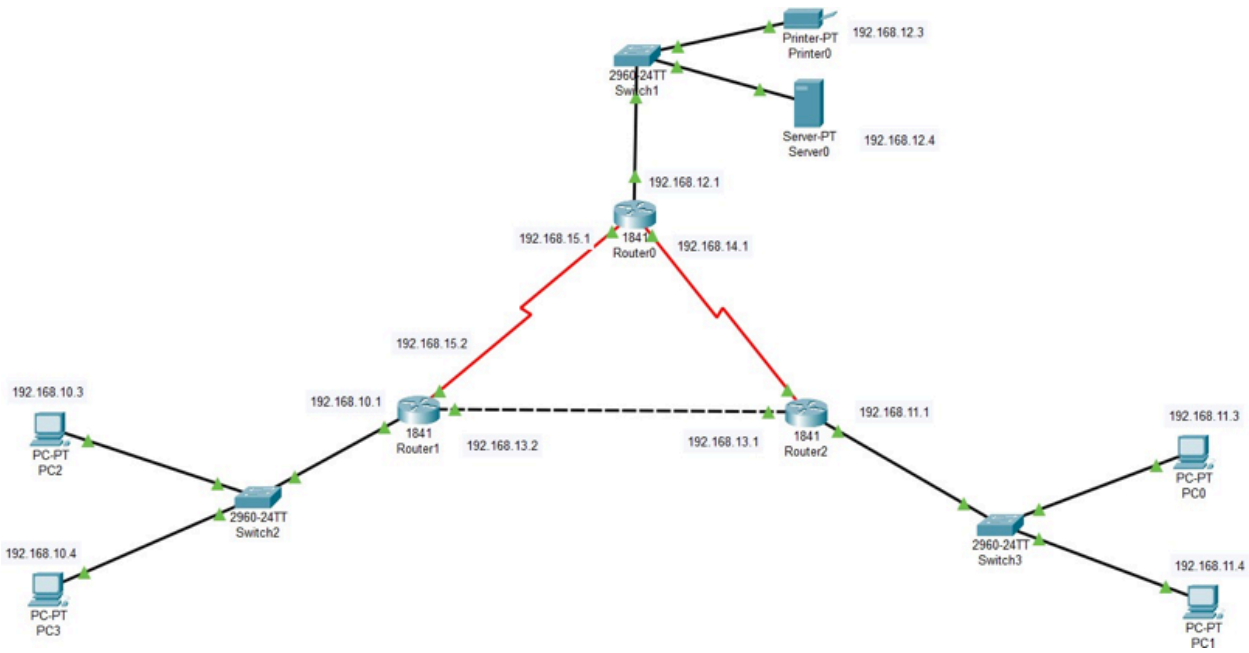
Aim : Analyze Distance Vector Routing Protocol using Routing Information Protocol to configure a computer network.

Software Used : Cisco Packet Tracer

Theory :

A distance-vector routing protocol in data networks determines the best route for data packets based on distance. Distance-vector routing protocols measure the distance by the number of routers a packet has to pass; one router counts as one hop. Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route. To determine the best route across a network, routers using a distance-vector protocol exchange information with one another, usually routing tables plus hop counts for destination networks and possibly other traffic information. Distance-vector routing protocols also require that a router inform its neighbors of network topology changes periodically.

Topology :



Routes known to router 0 :

```
R0#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 17 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 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  GigabitEthernet0/0/1  12 1
  Serial0/1/0           12 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          192.168.11.0
          192.168.12.0
          192.168.13.0
          192.168.14.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
          192.168.13.2         120      00:00:04
          192.168.14.2         120      00:00:16
Distance: (default is 120)
```

Routes known to router 1 :

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 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 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  GigabitEthernet0/0/1  12 1
  Serial0/1/0           12 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          192.168.10.0
          192.168.11.0
          192.168.13.0
          192.168.15.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
          192.168.13.1         120      00:00:01
          192.168.15.2         120      00:00:29
Distance: (default is 120)
```

Routes known to router 2 :

```
R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 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 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/1/0           12 1
  Serial0/1/1           12 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          192.168.10.0
          192.168.12.0
          192.168.14.0
          192.168.15.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
          192.168.14.1         120      00:00:26
          192.168.15.1         120      00:00:21
Distance: (default is 120)
```

Result : An exponentially distributed random number is generated from a uniformly distributed random number.

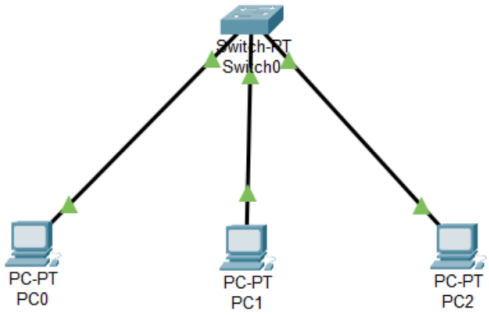
Experiment : 8

Aim : Performing an Initial Switch Configuration, and Initial Router Configuration using packet tracer.

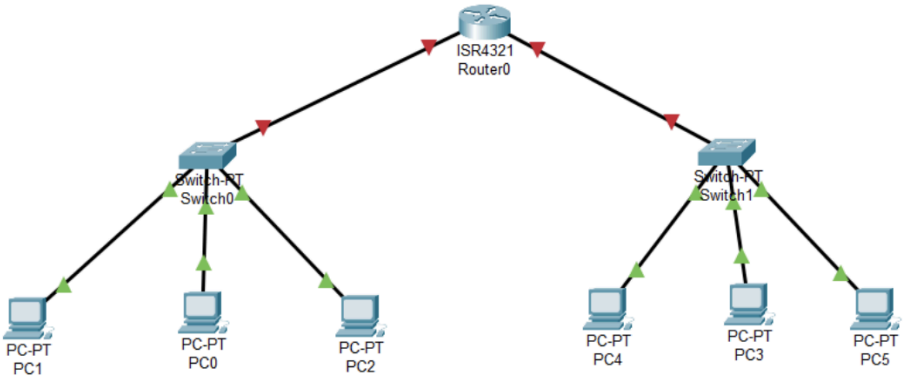
Software Used : Cisco Packet Tracer

Theory :

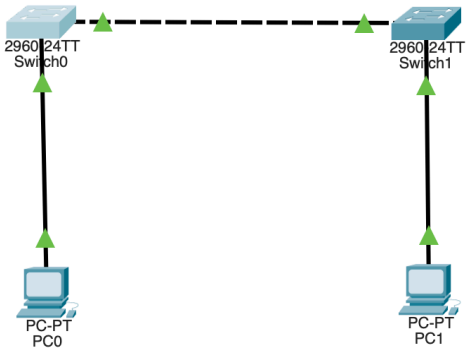
Switch: A Switch operates at the data link layer of the OSI model of a network. It uses the MAC address to forward the data packets. The advantage of using a switch is that it leads to less network traffic as it transmits using the MAC address and thus leading to less net conjunction.



Router: A Router is a networking device that forwards data packets between computer networks. It operates in the network layer of the OSI model. It connects different networks together and sends data packets from one network to another.



Switch Configuration :



1. Configuring initial switch settings topology

   Step 1 : Verifying default switch settings

```
Switch>enable
Switch#show running-config
Building configuration...

Current configuration : 1080 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Step 2 : Creating a basic switch configuration

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname s2
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#console 0
           ^
% Invalid input detected at '^' marker.

s2(config)#line console 0
s2(config-line)#password helloworld
s2(config-line)#login
s2(config-line)#exit
s2(config)#
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#exit









s2 con0 is now available




Press RETURN to get started.


User Access Verification

Password:
Password:

s2>enable
s2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#enable password cisco
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#ext
Translating "ext"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

s2#exit









s2 con0 is now available




Press RETURN to get started.
```

```
User Access Verification

Password:

s2>enable
Password:
s2#show running-config
Building configuration...

Current configuration : 1128 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname s2
!
enable password cisco
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 password helloworld
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

```
s2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#enable secret notasecret
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#show running-config
Building configuration...

Current configuration : 1175 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname s2
!
enable secret 5 $1$mERr$ZPwSEYLtngoDIQttAK34V/
enable password cisco
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/1
!
interface FastEthernet0/
!
interface FastEthernet
!
interface FastEtherne
!
interface FastEtherr
!
interface FastEthe
!
interface FastEth
!
interface Gigab
!
interface Giga
!
interface Vla
 no ip addre
 shutdown
!
!
!
!
line con
 passwo
 login
!
line
 logi
line
 lo
!
!
!
!
```

```
s2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#service password-encryption
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#show run
Building configuration...

Current configuration : 1195 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname s2
!
enable secret 5 $1$mERr$ZPwSEYLtngoDIQttAK34V/
enable password 7 0822455D0A16
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 password 7 0829494205161218000708
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Step 3 : Configure a MOTD banner

```
User Access Verification

Password:

s2>enable
Password:
s2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#banner motd "This is a secure system. Authorized Access Only"
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#exit









s2 con0 is now available




Press RETURN to get started.









This is a secure system. Authorized Access Only

User Access Verification

Password:
```

Step 4 : Save configuration files to NVRAM

```
s2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2. Router configuration

Step 1 : Verify the default router settings

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up









Router con0 is now available




Press RETURN to get started.









Press RETURN to get started!


Router>enable
Router#show running-config
Building configuration...

Current configuration : 618 bytes
!
```

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017D0IL-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


Router#
```

Step 2 : Configure and verify initial router configuration

```
Router#show startup-config
startup-config is not present
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

User Access Verification

Password:

R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable password cisco
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit


User Access Verification

Password:

R1>enable
Password:
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret notasecret
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner motd "Unauthorized access is strictly prohibited"
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Unauthorized access is strictly prohibited

User Access Verification

Password:

R1>enable
Password:
R1#show run
Building configuration...

Current configuration : 784 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$ZPwSEYLtngoDIQttAK34V/
enable password 7 0822455D0A16
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017D0IL-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized access is strictly prohibited^C
!
!
!
!
!
line con 0
 password 7 082D495A041C0C19
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Step 3 : Save the running file configuration

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show flash

System flash directory:
File  Length   Name/status
  3   33591768 2800nm-advipservicesk9-mz.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


R1#copy startup-config flash
Destination filename [startup-config]?

784 bytes copied in 0.416 secs (1884 bytes/sec)
R1#show flash

System flash directory:
File  Length   Name/status
  3   33591768 2800nm-advipservicesk9-mz.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
  4   784      startup-config
[33848371 bytes used, 221895629 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

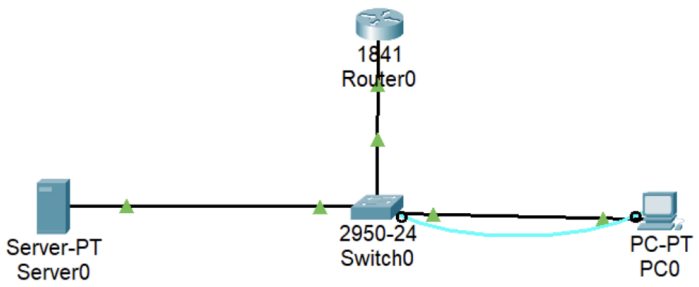
Result : Initial switch configuration and initial router configuration is performed using cisco packet tracer.

Experiment : 9

Aim : Configuring and Troubleshooting a Switched Network using packet tracer.

Software Used : Cisco Packet Tracer

Topology :



Switch Configuration :

```
Switch>enable
Switch#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#exit
S1(config)#interface vlan 1
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#interface vlan 1
S1(config-if)#ip default-gateway 172.17.99.1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#enable password class
S1(config)#service password-encryption
S1(config)#banner motd "Authorised Access Only"
S1(config)#
```

Router Configuration :

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#exit
R1(config)#enable password class


R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console


S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/2
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security mac sticky
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show mac?
mac  mac-address-table
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.be6b.b9c7    DYNAMIC     Fa0/2
   1    0060.5c73.6501    DYNAMIC     Fa0/3
   1    00e0.f9a4.212a    DYNAMIC     Fa0/1
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/2
S1(config-if)#switch port-security
Command rejected: FastEthernet0/2 is a dynamic port.
S1(config-if)#switchport mode access
S1(config-if)#switch port-security
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console


S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/2        1          0                0         Shutdown
---------------------------------------------------------------------
S1#
```

Result : Configured and troubleshooted a switched network using cisco packet tracer.