SRI CHANDRASEKHARENDRA SARASWATHI VISWA MAHAVIDYALAYA
(University established under section 3 of UGC Act 1956)
(Accredited With 'A' Grade by NAAC)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CS7P7- NETWORKING LABORATORY MANUAL

VII SEMESTER (B.E - ECE)

(For Private Circulation only)

Prepared By: Dr.M.Vinoth, Assistant Professor,
Dr.M.Sivakumar, Sr.Lab Instructor.

Approved By: Prof.V.Swaminathan, Professor & Head

LIST OF EXPERIMENTS

(Using CISCO Packet Tracer/MATLAB/NS2 Simulator)

1) **To analyse the performance of various configurations and protocols in LAN**
2) **To construct a VLAN and make the PC's communicate among a VLAN**
3) **To construct a Inter - VLAN and make the PC's communicate among a VLAN**
4) **To construct a Wireless LAN and make the PC's communicate wirelessly**
5) **To construct simple LAN and understand the concept and operation of Address Resolution Protocol (ARP)**
6) **To understand the concept and operation of Routing Information Protocol (RIP)**
7) **To construct multiple router networks and understand the operation of OSPF Protocol**
8) **To construct multiple router networks and understand the operation of EIGRP Protocol**
9) **To understand the operation of TELNET by accessing the router in server room from a PC in IT office.**
10) **To understand the operation of SSH by accessing the routers remotely by PCs**
11) **To understand the operation of AODV Routing using MATLAB Software**
12) **To understand the operation of Distance Vector Routing using MATLAB Software**
13) **To understand the operation of Pure Aloha protocol using MATLAB Software**
14) **To understand the operation of Slotted Aloha protocol using MATLAB Software**

Experiment: 1

Configuration of LAN

Aim:

To analyse the performance of various configurations and protocols in LAN

Requirements

- Windows pc – 3Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

Procedure

- Open the CISCO Packet tracer software
- Drag and drop 3 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PC1, PC2 and PC3 as 192.168.1.1, 192.168.1.2 and 192.168.1.3 respectively, ping between PCs and observe the transfer of data packets in real and simulation mode.

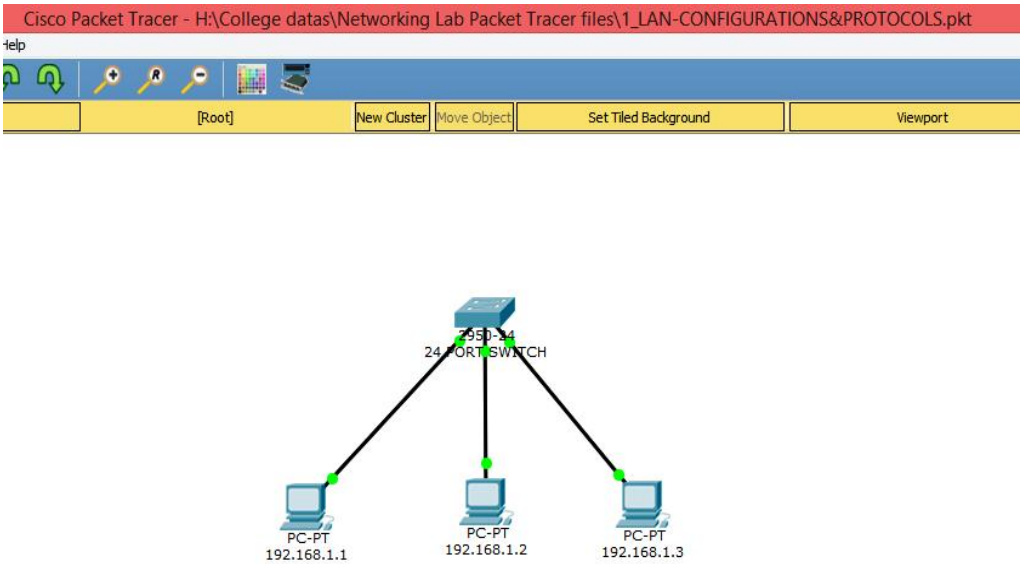
Theory

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

The advantages of a LAN are the same as those for any group of devices networked together. The devices can use a single Internet connection, share files with one another, print to shared printers, and be accessed and even controlled by one another.

Network Topology Diagram for LAN



Input Details for LAN

PC0	PC1	PC2
IP Address : 10.0.0.1 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Gate way : 10.0.0.50	IP Address : 10.0.0.3 Gate way : 10.0.0.50

LAN OUTPUT WINDOW: (PINGING FROM PC0-PC1)

Packet Tracer PC Command Line 1.0

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=8ms TTL=128
Reply from 10.0.0.2: bytes=32 time=4ms TTL=128
Reply from 10.0.0.2: bytes=32 time=4ms TTL=128
Reply from 10.0.0.2: bytes=32 time=4ms TTL=128

Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 8ms, Average = 5ms

LAN - MAC ADDRESS TABLE:

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0009.7c61.c0d0    DYNAMIC     Fa0/1
   1    000d.bdc2.3317    DYNAMIC     Fa0/2
   1    0090.0ce6.60c9    DYNAMIC     Fa0/3
```

Result

Hence, the various configurations and protocols in LAN are analysed and the experiment is performed successfully.

VIVA QUESTIONS

What is LAN and its uses?

A local-area network (LAN) is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

What are the advantages of LAN?

In LAN computers can exchange data and messages in the easy and fast way. It also saves time and makes our work fast. Every user can share messages and data with any other user on LAN. The user can log in from any computer on the network and access the same data placed on the server.

How does LAN work?

Early LAN (Local Area Network) networks were formed using coaxial cable, coax is an electric cable and it is used to carry radio signals. LAN (Local Area Network) setup is developed by connecting two or more than two computers with each other using a physical connection in order to share files and data overtime.

What is a disadvantage of LAN?

Disadvantages of LANs:

The use of email within the network can lead to problems of time wasting as people send messages that do not relate to work. ... If the dedicated file server fails, work stored on shared hard disk drives will not be accessible and it will not be possible to use network printers either.

Experiment:2

Configuration of VLAN

Aim:

To construct a VLAN and make the PC's communicate among a VLAN

Requirements

- Windows pc – 6 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

Procedure

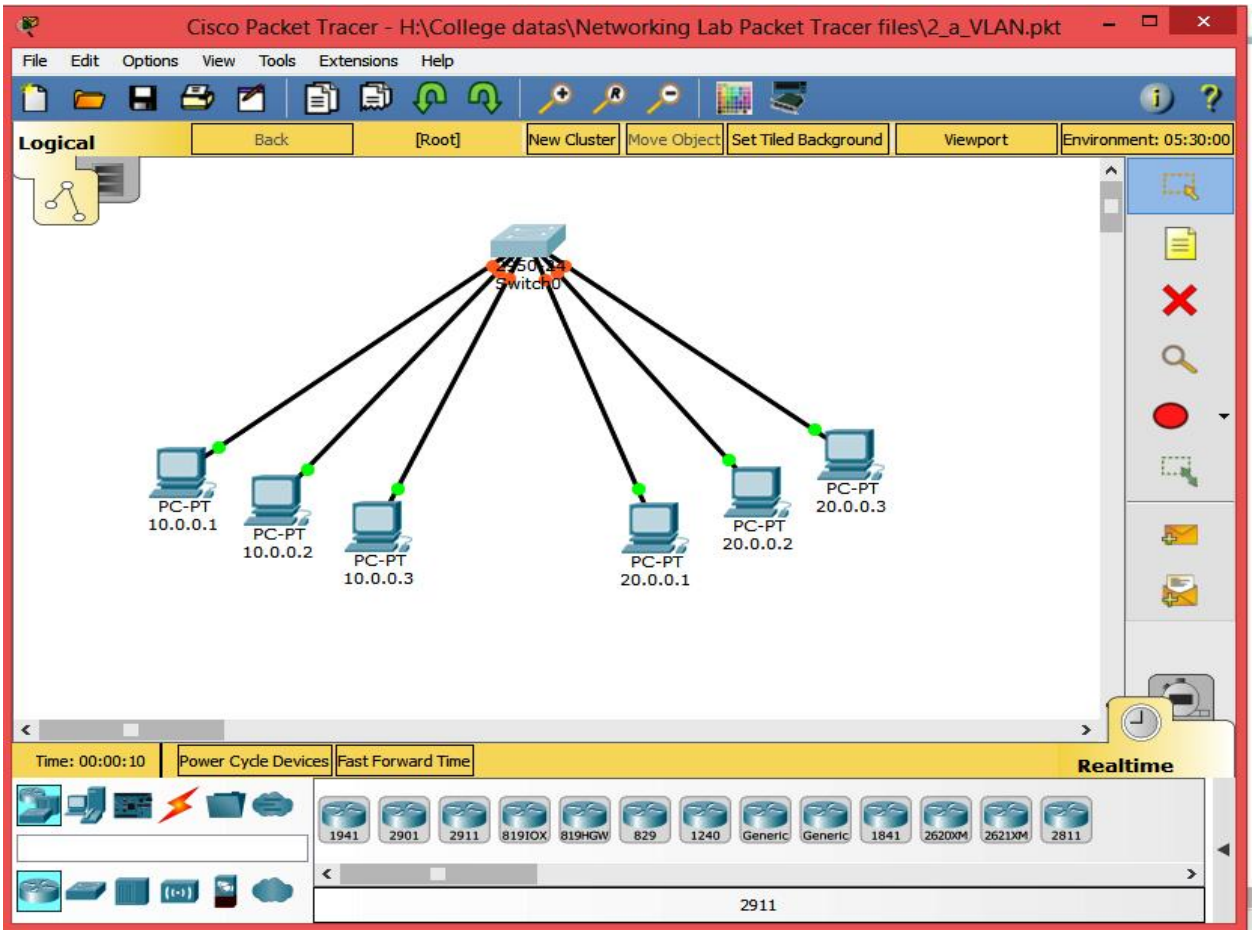
- Open the CISCO Packet tracer software
- Drag and drop 6 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PCs as per table, ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

Network Topology Diagram for VLAN



Input Details for VLAN 10

PC0	PC1	PC2
IP Address : 10.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.3 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50

Input Details for VLAN 20

PC0	PC1	PC2
IP Address : 20.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50	IP Address : 20.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50	IP Address : 20.0.0.3 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50

CONFIGURATION OF THE SWITCHPORT FOR VLAN:

Switch>en

Switch#config

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#ex

Switch(config)#vlan 20

Switch(config-vlan)#ex

Switch(config)#interface range fastEthernet 0/1-3

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

Switch(config-if-range)#ex

Switch(config)#interface range fastEthernet 0/4-6

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

Switch(config-if-range)#ex

Switch(config)#ex

Switch#

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

VLAN OUTPUT: (PINGING FROM PC0)

C:\>PING 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>PING 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

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

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

MAC- ADDRESS TABLE:

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------      -------------------------------------------

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

  10    0009.7c61.c0d0    DYNAMIC     Fa0/1        20    0060.3e8d.3936    DYNAMIC     Fa0/5
  10    000d.bdc2.3317    DYNAMIC     Fa0/2        20    00d0.bcb6.54aa    DYNAMIC     Fa0/6
  10    0090.0ce6.60c9    DYNAMIC     Fa0/3        20    00e0.a371.aec7    DYNAMIC     Fa0/4
```

Result

Hence, created VLAN structure and observed the communications of PCs within a VLAN

VIVA QUESTIONS

What is LAN and VLAN?

VLAN and LAN are two terms used frequently in the networking field. ... VLAN is an implementation of a private subset of a LAN in which the computers interact with each other as if they are connected to the same broadcast domain irrespective of their physical locations

What is VLAN? And how it is reduce the broadcast traffic?

A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. VLAN divides the broadcast domain so, the frames that will be broadcasted onto the network are only the ports logically grouped with in the same VLAN.

What is Inter VLAN Routing?

VLANs divide broadcast domains in a LAN environment so, by default only Hosts that are members of the same VLAN can communicate. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as Inter VLAN Routing.

Give the Command to Create VLAN?

Switch(config)#vlan 10

Switch(config-vlan)#ex

How can we add an interface to a VLAN?

Switch(config)#interface range fastEthernet 0/1-3

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

Switch(config-if-range)#ex

Which command is used to see all VLANs information?

Switch # show vlan 10

Experiment: 3

Configuration of Inter VLAN

Aim:

To construct a Inter - VLAN and make the PC's communicate among a VLAN

Requirements

- Windows pc – 4 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

Procedure

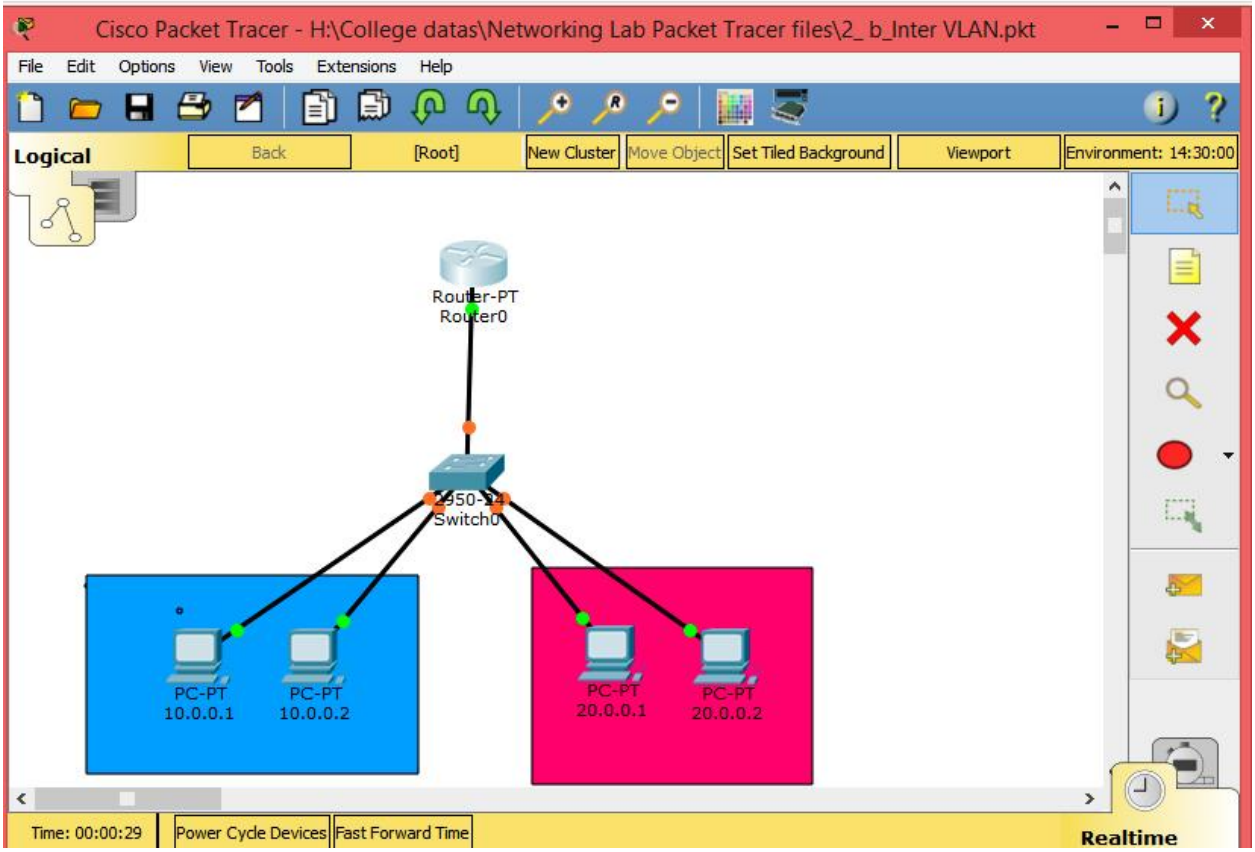
- Open the CISCO Packet tracer software
- Drag and drop 4 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PCs as per table, ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network. As we learnt previously, VLANs logically segment the switch into different subnets, when a router is connected to the switch, an administrator can configure the router to forward the traffic between the various VLANs configured on the switch. The user nodes in the VLANs forwards traffic to the router which then forwards the traffic to the destination network regardless of the VLAN configured on the switch.

The use of VLANs means that users would not be able to communicate across departments, i.e. a user in FINANCE, would not be able to send a message to a user in SALES since they are on different broadcast domains.

Network Topology Diagram for Inter VLAN



Input Details for VLAN 10

PC0	PC1
IP Address : 10.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50

Input Details for VLAN 20

PC0	PC1
IP Address : 20.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50	IP Address : 20.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50

CONFIGURING THE TRUNK PORT IN SWITCH:

Switch#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/7
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#no shut
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit

ROUTER CONFIGURATION:

Router>en

Router#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fastEthernet 0/0

Router(config-if)#no shut

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(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0.10

Router(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.0.0.50 255.0.0.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 20.0.0.50 255.0.0.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, FastEthernet0/0.10
C 20.0.0.0/8 is directly connected, FastEthernet0/0.20

OUTPUT:(PINGING PC3 IN VLAN20 FROM PC0 IN VLAN10)

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time=4ms TTL=127
Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 1ms

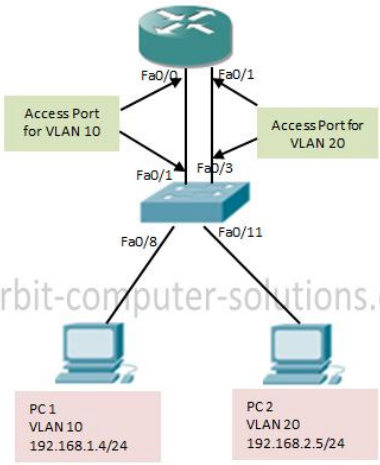
Result

Hence, We constructed Inter VLAN and made the communications of PCs between different VLANs.

VIVA QUESTIONS

What is Inter VLAN Routing ? Explained with Examples

Inter-VLAN routing using a router on a stick utilizes an external router to pass traffic between VLANs.



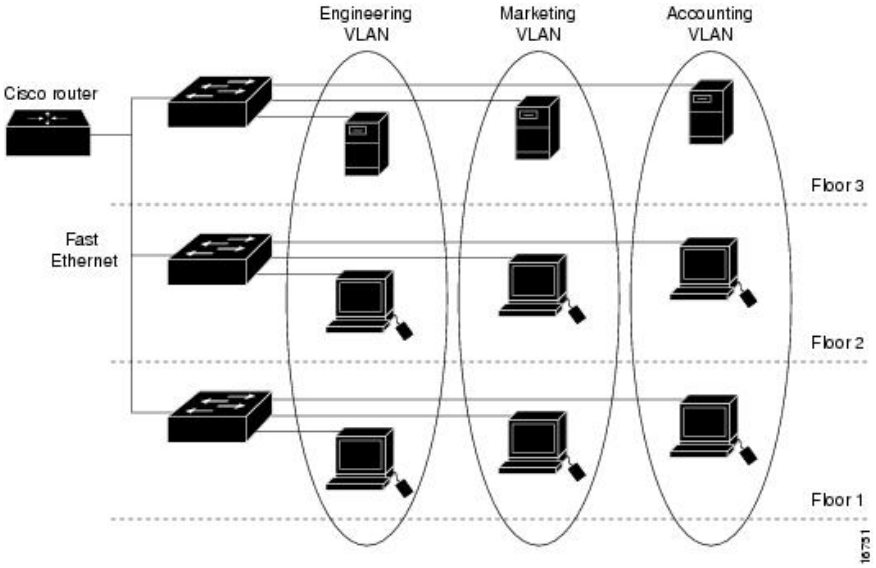
The figure above show a traditional inter-VLAN routing:

1 Traffic from PC1 on VLAN10 is routed through router R1 to reach PC3 on VLAN 20.

2. PC1 and PC3 are on different VLANs and have IP addresses on different subnets.

3. Router R1 has a separate interface configured for each of the VLANs.

Sample of VLAN



Experiment: 4

Configuration of Wireless LAN

Aim:

To construct a Wireless LAN and make the PC's communicate wirelessly

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

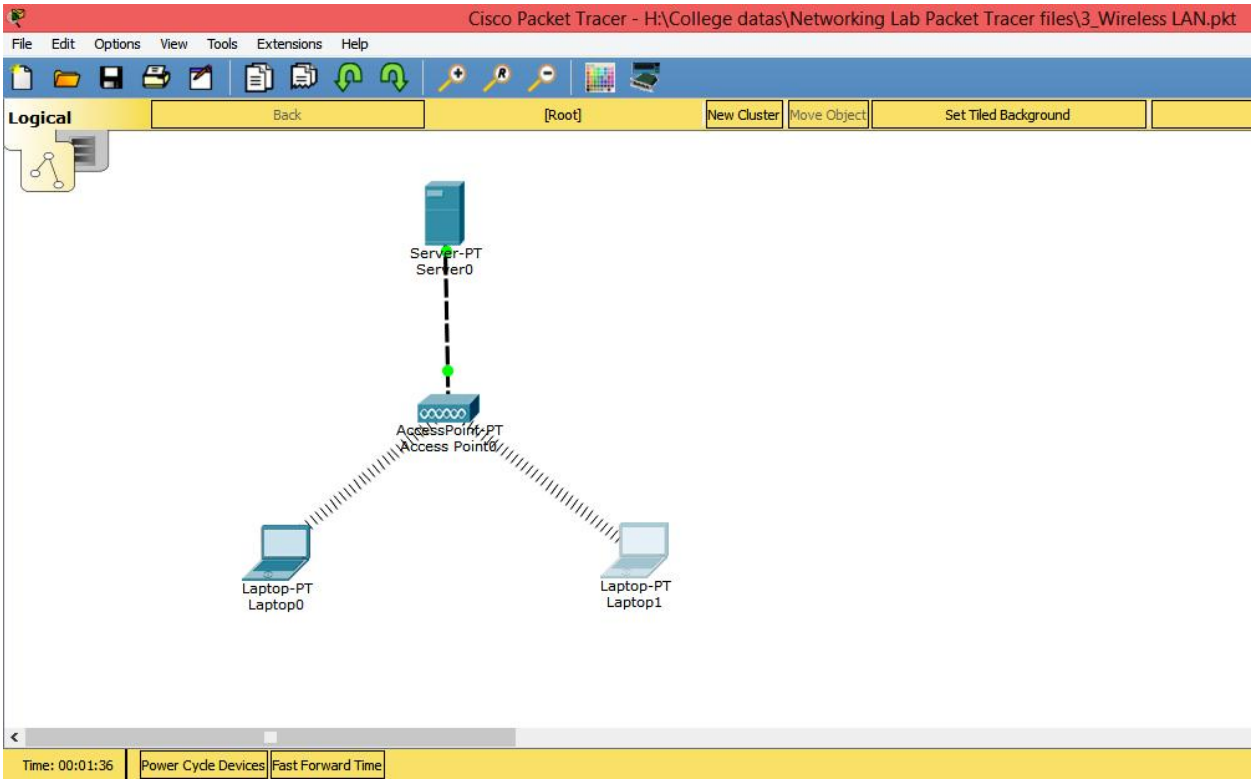
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 2 Laptop pcs using End Device Icons on the left corner
- Select Access point and server from wireless devices
- Select laptop-> physical-> OFF laptop-> remove LAN Module & replace WPC 300N Wireless module -> ON Laptop
- Observe the wireless connections between access point and laptops
- Give IP address of the PCs as per table, ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

A Wireless Local Area Network (WLAN) implements a flexible data communication system frequently augmenting rather than replacing a wired LAN within a building or campus. WLANs use radio frequency to transmit and receive data over the air, minimizing the need for wired connections.

Network Topology Diagram for Wireless LAN



WLAN OUTPUT WINDOW:(PINGING FROM laptop 1- laptop 0)

C:\>ping 169.254.129.204

Pinging 169.254.129.204 with 32 bytes of data:

Reply from 169.254.129.204: bytes=32 time=30ms TTL=128
Reply from 169.254.129.204: bytes=32 time=16ms TTL=128
Reply from 169.254.129.204: bytes=32 time=15ms TTL=128
Reply from 169.254.129.204: bytes=32 time=13ms TTL=128

Ping statistics for 169.254.129.204:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 13ms, Maximum = 30ms, Average = 18ms

Result:

Thus, constructed a WLAN and made the Laptops communicate wirelessly

VIVA QUESTIONS

What is a Wireless Network?

A wireless local-area network (WLAN) uses radio waves to connect devices, such as laptops, to the Internet and to your business network and applications.

What is mean by wireless LAN?

A wireless local area network (WLAN) is a wireless distribution method for two or more devices that 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.

What is the difference between WiFi and wireless LAN?

While wireless LANs refer to any local area network (LAN) that a mobile user can connect to through a wireless (radio) connection; Wi-Fi (short for "wireless fidelity") is a term for certain types of WLANs that use specifications in the 802.11 wireless protocol family.

What are the Benefits of a WLAN?

Small businesses can experience many benefits from a WLAN. A few examples:

- You can access network resources from any location within the wireless network's coverage area.
- Wireless access to the Internet and to company resources help your staff be more productive and collaborative.
- You don't have to string cables, as you do with wired networks. Installation can be quick and cost-effective.
- You can easily expand WLANs where and as needed, because no wires are involved.
- By eliminating or reducing wiring expenses, WLANs can cost less to operate than wired networks.

Who Uses WLANs?

WLANs are frequently offered in public places such as cafes, hotels, and airport lounges. In addition, many businesses have wireless networks throughout their office buildings or campuses for employee and guest use.

Experiment: 5

Configuration of Address Resolution protocol

Aim:

To construct simple LAN and understand the concept and operation of Address Resolution Protocol (ARP)

Requirements

- Windows pc – 5 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

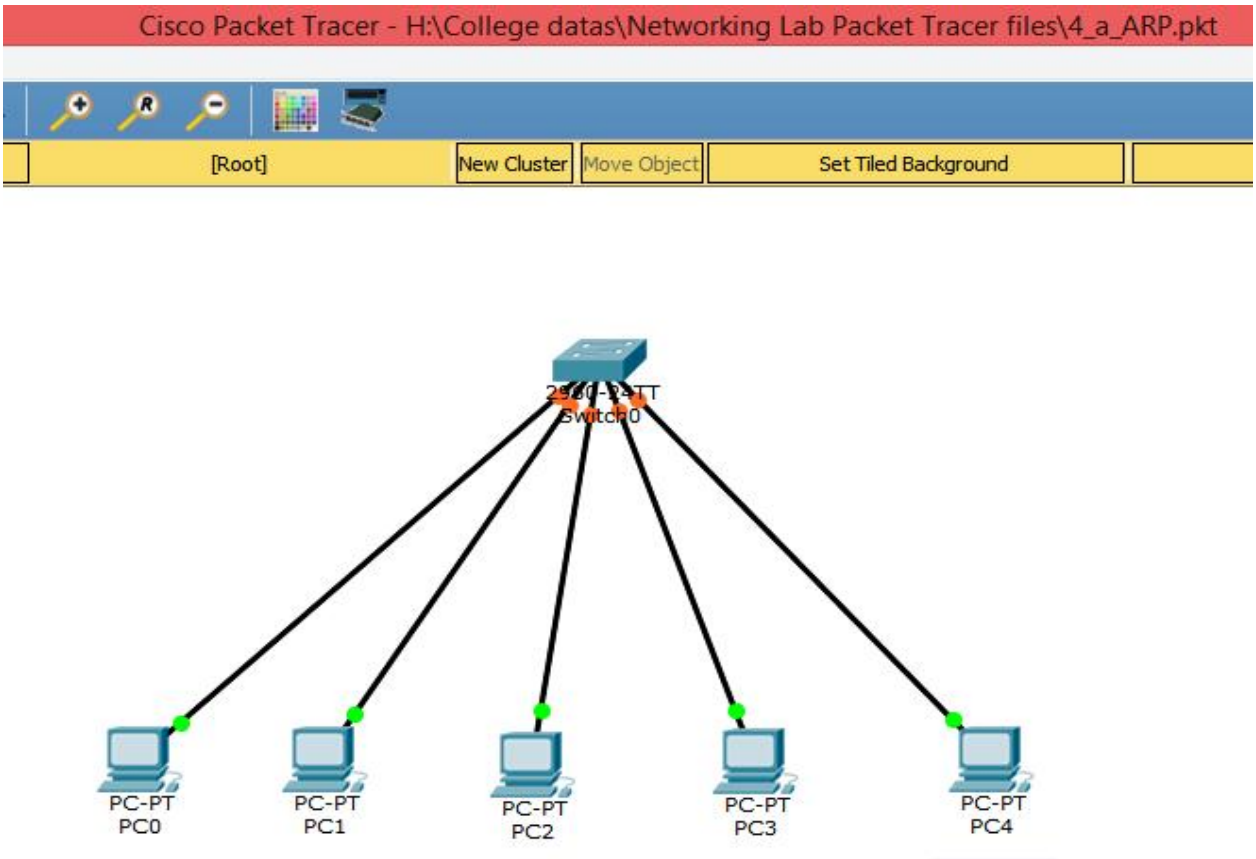
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PC1, PC2, PC3 and PC4 as per the input table respectively, observe the source and destination MAC address of all packets.
- Get cache from switch.

Theory

ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address. It is used when a device wants to communicate with some other device on a local network (for example on an Ethernet network that requires physical addresses to be known before sending packets). The sending device uses ARP to translate IP addresses to MAC addresses. The device sends an ARP request message containing the IP address of the receiving device. All devices on a local network segment see the message, but only the device that has that IP address responds with the ARP reply message containing its MAC address. The sending device now has enough information to send the packet to the receiving device.

Network Topology Diagram for ARP



Input Details for ARP

PC0	PC1	PC2	PC3	PC4
IP Address : 10.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.3 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.4 Subnet Mask: 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.5 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50

OUTPUT:

ARP CATCH TABLE OF PC1 (IP: 10.0.0.2):

C:\>arp -a

Internet Address Physical Address Type
10.0.0.1 0001.42c1.0547 dynamic
10.0.0.3 0001.6402.dab3 dynamic
10.0.0.4 0001.43e2.332b dynamic
10.0.0.5 0001.9665.3174 dynamic

SWITCH MAC ADDRESS TABLE:

```
Switch>
Switch>SHOW MAC ADDRESS-TABLE
          Mac Address Table
-------------------------------------------

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

   1    0001.42c1.0547    DYNAMIC     Fa0/1
   1    0001.43e2.332b    DYNAMIC     Fa0/4
   1    0001.6402.dab3    DYNAMIC     Fa0/3
   1    0001.9665.3174    DYNAMIC     Fa0/5
   1    0060.70c9.ba88    DYNAMIC     Fa0/2
```

Result:

Thus, constructed a simple LAN and understand the concept and operation of ARP and got the ARP Cache of given layout.

VIVA QUESTIONS

What is ARP?

Address Resolution Protocol (ARP) is a network protocol, which maps a network layer protocol address to a data link layer hardware address. For example, ARP is used to resolve IP address to the corresponding Ethernet address.

What is ARP process?

ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address.

What is a Address Resolution Protocol in networking?

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). ARP can also be used for IP over other LAN technologies, such as token ring, fiber distributed data interface (FDDI) and IP over ATM.

Where is ARP protocol used?

This is where ARP comes into the picture, its functionality is to translate IP address to physical address. The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.

What is the use of ARP?

A host in an Ethernet network can communicate with another host, only if it knows the Ethernet address (MAC address) of that host. The higher level protocols like IP use a different kind of addressing scheme (like IP address) from the lower level hardware addressing scheme like MAC address. ARP is used to get the Ethernet address of a host from its IP address. ARP is extensively used by all the hosts in an Ethernet network.

What is an ARP cache?

ARP maintains the mapping between IP address and MAC address in a table in memory called ARP cache. The entries in this table are dynamically added and removed.

Can ARP be used in a network other than Ethernet?

ARP is a general protocol, which can be used in any type of broadcast network. The fields in the ARP packet specifies the type of the MAC address and the type of the protocol address. ARP is used with most IEEE 802.x LAN media. In particular, it is also used with FDDI, Token Ring, and Fast Ethernet, in precisely the same way as it is with Ethernet.

Experiment: 6

Configuration of Routing Information protocol

Aim:

To understand the concept and operation of Routing Information Protocol (RIP)

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 2 No
- Router – 2 Nos
- Cat-5 LAN cable

Procedure

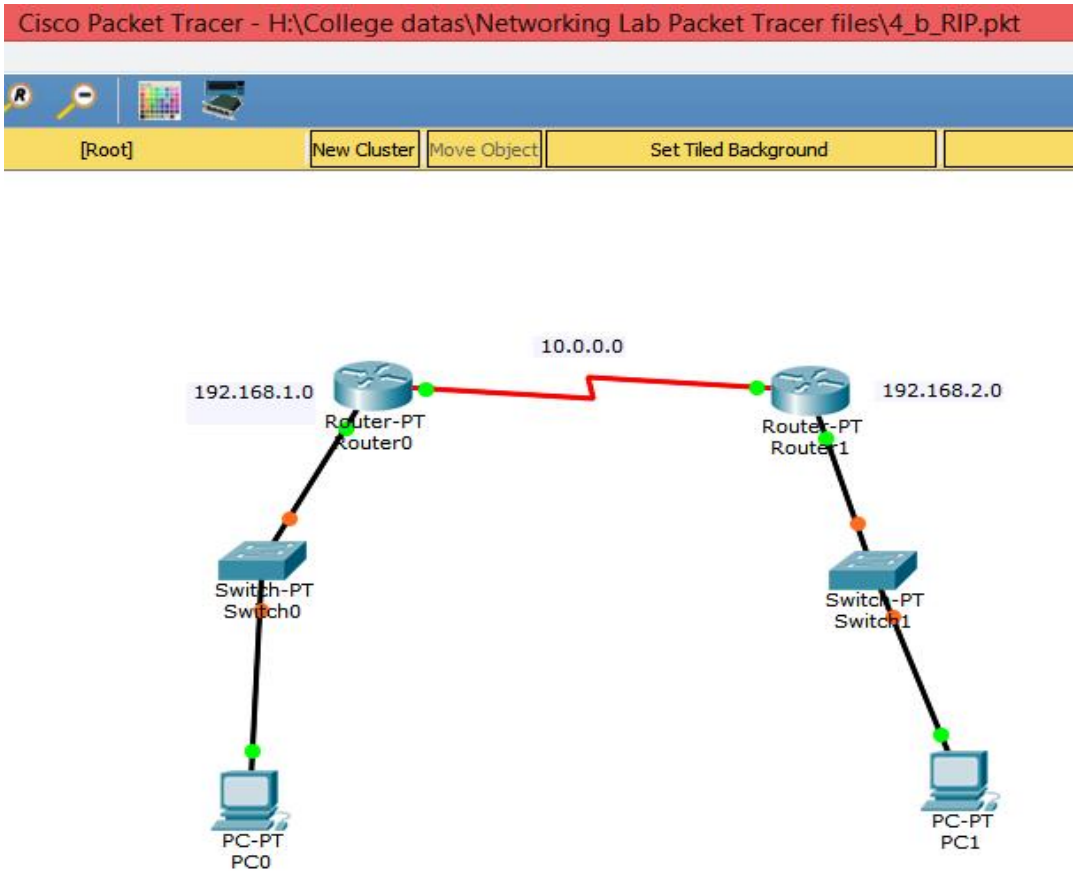
- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router and apply clock rate as per the table.
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

RIP (Routing Information Protocol) is one of the oldest distance vector routing protocols. It is usually used on small networks because it is very simple to configure and maintain, but lacks some advanced features of routing protocols like OSPF or EIGRP. Two versions of the protocol exists: version 1 and version 2. Both versions use hop count as a metric and have the administrative distance of 120. RIP version 2 is capable of advertising subnet masks and uses multicast to send routing updates, while version 1 doesn't advertise subnet masks and uses broadcast for updates. Version 2 is backwards compatible with version 1.

RIPv2 sends the entire routing table every 30 seconds, which can consume a lot of bandwidth. RIPv2 uses multicast address of 224.0.0.9 to send routing updates, supports authentication and triggered updates (updates that are sent when a change in the network occurs).

Network Topology Diagram for RIP



Input Details for RIP

PC0	PC1	Router 0	Router 1
IP Address : 192.168.1.2 Gate way : 192.168.1.1	IP Address: 192.168.2.2 Gate way : 192.168.2.1	Fast Ethernet 0/0 IP Address: 192.168.1.1 Serial 2/0 : 10.0.0.1 at 6400 clock rate	Fast Ethernet 0/0 IP Address : 192.168.2.1 Serial 2/0 : 10.0.0.2 no clock rate

OUTPUT:

RIP (PINGING FROM PC0 TO PC1):

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=11ms TTL=126

Reply from 192.168.2.2: bytes=32 time=12ms TTL=126

Reply from 192.168.2.2: bytes=32 time=13ms TTL=126

Reply from 192.168.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 11ms, Maximum = 13ms, Average = 11ms

Result:

Thus, understand the concept and operation of RIP and pinged from PC in are networks to PC to another network.

VIVA QUESTIONS

What is RIP routing?

RIP stand for Routing information Protocol. It is protocol which communicates to one router to another router. It update after 30sec send his routing table to another router. It is distance vector protocol which protocol work on metric hop count after that is transferred the packet from source to destination. It has to follow shortage distance basis transfer the data.

How do we configure rip? Specify the commands.

#Router rip

#network 10.0.0.0

Which command is used to check RIP routing?

#show ip route

#show ip protocols

Experiment: 7

Configuration of Open shortest Path First (OSPF) Algorithm

Aim:

To construct multiple router networks and understand the operation of OSPF Protocol

Requirements

- Windows pc – 3 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 3 No
- Router – 3 Nos
- Cat-5 LAN cable

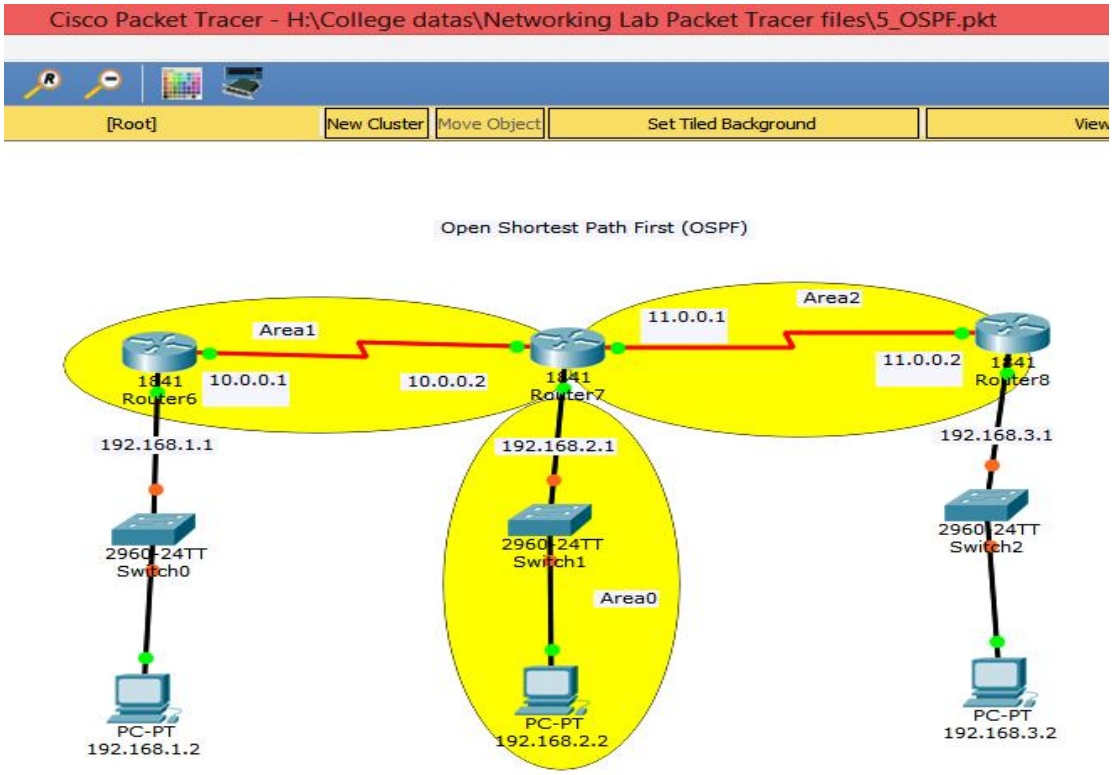
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router and apply clock rate
- Add HWIC -2T Peripheral to all routers, type CLI's for all routers
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

Network Topology Diagram for OSPF



Input Details for OSPF

PC0	PC1	PC2
IP Address : 192.168.1.2 Gate way : 192.168.1.1	IP Address: 192.168.2.2 Gate way : 192.168.2.1	IP Address: 192.168.3.2 Gate way : 192.168.3.1

Router 0	Router 1	Router 2
fa 0/0 IP Address: 192.168.1.1 Serial 0/0/0 : 10.0.0.1 @ 2000000 clock rate Serial 0/0/1 : -	fa 0/0 IP Address : 192.168.2.1 Serial 0/0/0 : 10.0.0.2 Serial 0/0/1 : - @ 2000000 clock rate	Fa 0/0 IP Address : 192.168.3.1 Serial 0/0/0 : 10.0.0.2 @ no clock rate Se 0/0/1 : 11.0.0.1

ROUTER0 CLI:

Router#en
Router#config
Configuring from terminal, memory, or network [terminal]?
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 1
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
00:19:21: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

ROUTER1 CLI:

Router(config)#router ospf 2
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
00:19:07: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
Router(config-router)#network 11.0.0.0 0.255.255.255 area 2
Router(config-router)#exit
00:25:52: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

ROUTER2 CLI:

Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
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 2
Router(config-router)#network 11.0.0.0 0.255.255.255 area 2
00:25:19: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done
Router(config)#exit

OUTPUT:

ROUTER0:

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

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, Serial0/0/0
O IA 11.0.0.0/8 [110/128] via 10.0.0.2, 00:04:43, Serial0/0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/65] via 10.0.0.2, 00:07:42, Serial0/0/0
O IA 192.168.3.0/24 [110/129] via 10.0.0.2, 00:00:53, Serial0/0/0

ROUTER1:

C 10.0.0.0/8 is directly connected, Serial0/0/0
C 11.0.0.0/8 is directly connected, Serial0/0/1
O 192.168.1.0/24 [110/65] via 10.0.0.1, 00:04:50, Serial0/0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
O 192.168.3.0/24 [110/65] via 11.0.0.2, 00:04:45, Serial0/0/1

ROUTER2:

O IA 10.0.0.0/8 [110/128] via 11.0.0.1, 00:06:55, Serial0/0/0
C 11.0.0.0/8 is directly connected, Serial0/0/0
O IA 192.168.1.0/24 [110/129] via 11.0.0.1, 00:06:45, Serial0/0/0
O IA 192.168.2.0/24 [110/65] via 11.0.0.1, 00:06:55, Serial0/0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/0

Result:

Thus, understand the concept and operation of OSPF and obtained the routing table and observe transfer data packets in real and simulation time.

VIVA QUESTIONS

What is the algorithm used by OSPF?

OSPF uses SPF (Shortest Path First) algorithm for calculating the best path and preparing OSPF database.

What are the characteristics of OSPF ?

1. OSPF supports only IP routing.
2. OSPF routes have an administrative distance i.e. 110.
3. OSPF uses cost as its metric, which is computed based on the bandwidth of the link. OSPF has no hop-count limit.

What are the different OSPF network types and give an example for each ?

Different OSPF network types with their examples are given below:
1) Broadcast Multi-Access – indicates a topology where broadcast occurs.
Examples include Ethernet, Token Ring, and ATM.
2) Point-to-Point – indicates a topology where two routers are directly connected.
An example would be a point-to-point T1.
3) Point-to-Multipoint – indicates a topology where one interface can connect to multiple destinations. Each connection between a source and destination is treated as a point-to-point link.
An example would be Point-to-Multipoint Frame Relay.
4) Non-broadcast Multi-access Network (NBMA) – indicates a topology where one interface can connect to multiple destinations; however, broadcasts cannot be sent across a NBMA network.

Name tables which OSPF maintain?

The OSPF process builds and maintains three separate tables:
1) A neighbor table – contains a list of all neighboring routers.
2) A topology table – contains a list of all possible routes to all known networks within an area.
3) A routing table – contains the best route for each known network.

Experiment: 8

Configuration of Enhanced Internal Gateway Routing Protocol

Aim:

To construct multiple router networks and understand the operation of EIGRP Protocol

Requirements

- Windows pc – 4 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 2 No
- Router – 3 Nos
- Cat-5 LAN cable

Procedure

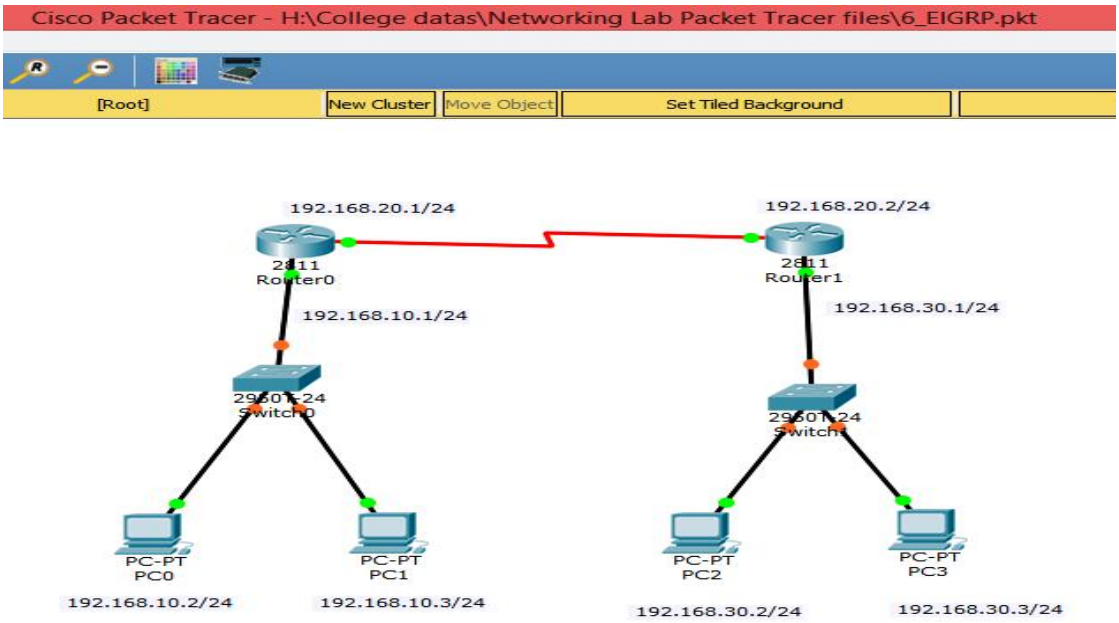
- Open the CISCO Packet tracer software
- Drag and drop 4 pcs using End Device Icons on the left corner
- Select TWO 8 port switch from switch icon list in the left bottom corner
- Select TWO Routers and Give the IP address for serial ports of router and apply clock rate as per the input table.
- Add WIC -IT Peripheral to all routers, type CLI's for all routers
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

Enhanced Interior Gateway Routing Protocol (EIGRP Protocol) is an enhanced distance vector routing protocol which Uses Diffused Update Algorithm (DUAL) to calculate the shortest path. It is also considered as a Hybrid Routing Protocol because it has characteristics of both Distance Vector and Link State Routing Protocols.

EIGRP supports classless routing and VLSM, route summarization, incremental updates, load balancing and other features.

Network Topology Diagram for EIGRP



Input Details for EIGRP

PC0	PC1	PC2	PC3
IP Address : 192.168.10.2 Gate way : 192.168.10.1	IP Address: 192.168.10.3 Gate way : 192.168.10.1	IP Address: 192.168.30.2 Gate way : 192.168.30.1	IP Address: 192.168.30.3 Gate way : 192.168.30.1

Router 0	Router 1
fa 0/0 IP Address: 192.168.10.1 Serial 0/0/0 : 192.168.20.1 @ 6400 clock rate	fa 0/0 IP Address : 192.168.30.1 Serial 0/0/0 : 192.168.20.2

ROUTER0 CLI:

Router(config)#router eigrp 10
Router(config-router)#network 192.168.10.0 255.255.255.0
Router(config-router)#network 192.168.20.0 255.255.255.0
Router(config-router)#exit

ROUTER1 CLI:

Router(config)#router eigrp 10
Router(config-router)#network 192.168.20.0 255.255.255.0
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.20.1 (Serial0/1/0) is up: new adjacency
Router(config-router)#network 192.168.30.0 255.255.255.0
Router(config-router)#exit

OUTPUT:

ROUTER0:

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

Gateway of last resort is not set

C 192.168.10.0/24 is directly connected, FastEthernet0/0
C 192.168.20.0/24 is directly connected, Serial0/3/0
D 192.168.30.0/24 [90/20514560] via 192.168.20.2, 00:04:51, Serial0/3/0

ROUTER1:

D 192.168.10.0/24 [90/20514560] via 192.168.20.1, 00:05:35, Serial0/1/0
C 192.168.20.0/24 is directly connected, Serial0/1/0
C 192.168.30.0/24 is directly connected, FastEthernet0/0

Result:

Thus, understand the concept and operation of EIGRP and obtained the routing table and observe transfer data packets in real and simulation time.

VIVA QUESTIONS

Why EIGRP is called hybrid protocol?

EIGRP is also called hybrid protocol because its metric is not just plain HOP COUNT (max-255, included in pure distance vector protocol) rather includes the links bandwidth, delay, reliability and Load parameter into the calculation. Thats why called Advanced or Hybrid protocol.

What are the different packets or message in EIGRP?

There are Six packets in EIGRP, 1-Hello , 2-Update, 3-Query, 4-Reply, 5-Acknoladgment, 6.Request

What are different route types in EIGRP?

There are three different types of routes in EIGRP:

- Internal Route—Routes that are originated within the Autonomous System (AS).
- Summary Route—Routes that are summarized in the router (for example, internal paths that have been summarized).
- External Route—Routes that are redistributed to EIGRP.

Experiment: 9

Configuration Telnet

Aim:

To understand the operation of TELNET by accessing the router in server room from a PC in IT office.

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Router – 1 Nos
- Cat-5 LAN cable

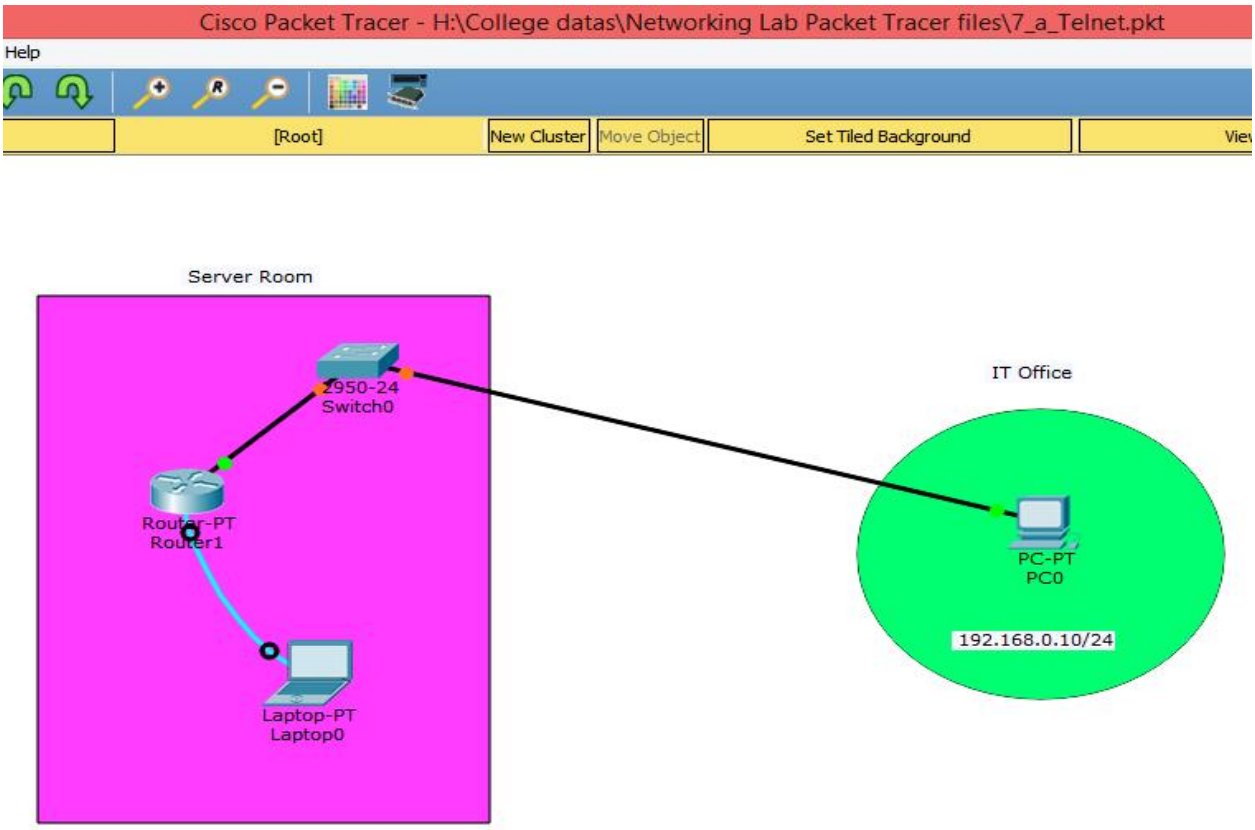
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 1 pc and 1 laptop using End Device Icons on the left corner.
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router
- Type CLI's for the router
- Make and verify the connections from any pc to the server by providing correct password; in command prompt of PC.
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

Telnet, developed in 1969, is a protocol that provides a command line interface for communication with a remote device or server, sometimes employed for remote management but also for initial device setup like network hardware. Telnet stands for Teletype Network, but it can also be used as a verb; 'to telnet' is to establish a connection using the Telnet protocol.
Telnet is a simple, text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet.

Network Topology Diagram for TELNET



Input Details for TELNET

Router 0	PC0	PC1
IP Address : 192.168.0.1 Gate way : -	IP Address : 192.168.0.2 Gate way : 192.168.0.1	IP Address : 192.168.0.3 Gate way : 192.168.0.2

ROUTER CLI:

Router#config

Configuring from terminal, memory, or network [terminal]?

Router(config)#line vty 0 4

Router(config-line)#password sai123

Router(config-line)#login local

Router(config-line)#exit

Router(config)#username sai privilege 4 password sai123

Router(config)#exit

OUTPUT:

PINGING FROM PC0 TO SERVER USING TELENET:

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.1:

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

C:\>telnet 192.168.0.1
Trying 192.168.0.1 ...Open
User Access Verification
Username: **sai**
Password: **<type the password---sai123(invisible)>**

Router#show ip route***(now router can be accessed from pc0)***
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
Router#

Result:

Thus, verified the operation of TELNET and accessed the router from Pcs.

VIVA QUESTIONS

What are common uses for Telnet?

Telnet can be used to test or troubleshoot remote web or mail servers, as well as for remote access to MUDs (multi-user dungeon games) and trusted internal networks.

How does Telnet work?

Telnet provides users with a bidirectional interactive text-oriented communication system utilizing a virtual terminal connection over 8 byte. User data is interspersed in-band with telnet control information over the transmission control protocol (TCP). Often, Telnet was used on a terminal to execute functions remotely.

The user connects to the server by using the Telnet protocol, which means entering Telnet into a command prompt by following this syntax: telnet hostname port. The user then executes commands on the server by using specific Telnet commands into the Telnet prompt. To end a session and log off, the user ends a Telnet command with Telnet.

Is Telnet secure?

Because it was developed before the mainstream adaptation of the internet, Telnet on its own does not employ any form of encryption, making it outdated in terms of modern security. It has largely been overlapped by Secure Shell (SSH) protocol, at least on the public internet, but for instances where Telnet is still in use, there are a few methods for securing your communications.

Experiment: 10

Configuration of Secured Shell (SSH) cryptographic Protocol

Aim:

To understand the operation of SSH by accessing the routers remotely by PCs

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Router – 1 Nos
- Cat-5 LAN cable

Procedure

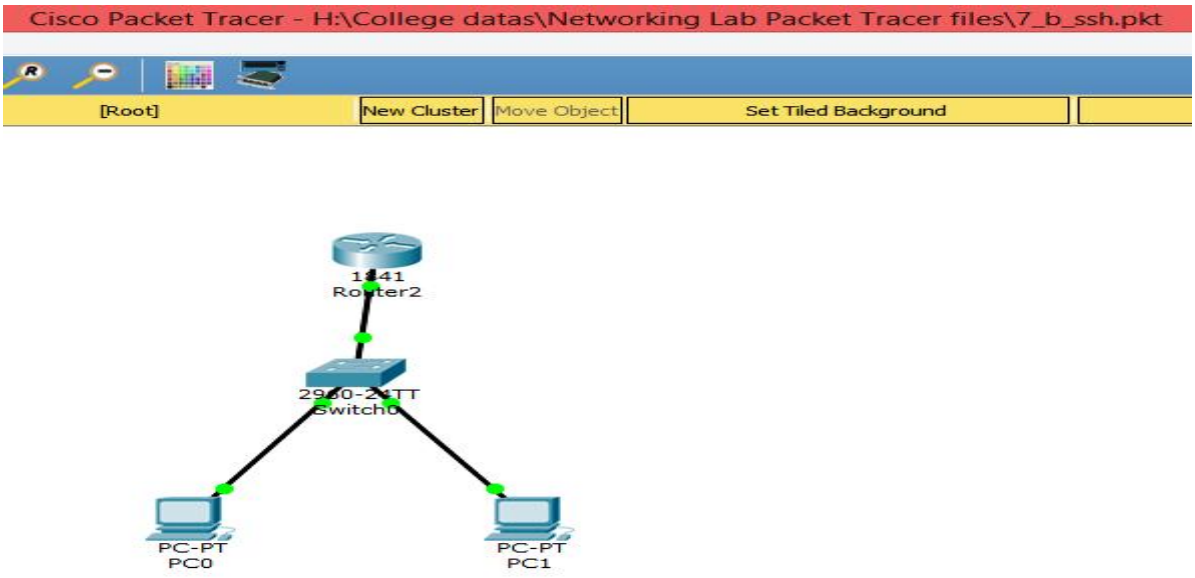
- Open the CISCO Packet tracer software
- Drag and drop 1 pc and 1 laptop using End Device Icons on the left corner.
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router
- Type CLI's for the router
- Make and verify the SSH operation by pinging in the command prompt of PC
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

SSH stands for Secure Shell is a network protocol, used to access remote machine in order to execute command-line network services and other commands over a Network. SSH is Known for its high security, cryptographic behavior and it is most widely used by Network Admins to control remote web servers primarily.

Both SSH and Telnet are network Protocol. Both the services are used in order to connect and communicate to another machine over Network. SSH uses Port 22 and Telnet uses port 23 by default. Telnet send data in plain text and non-encrypted format everyone can understand whereas SSH sends data in encrypted format. Not to mention SSH is more secure than Telnet and hence SSH is preferred over Telnet.

Network Topology Diagram for SSH



Input Details for SSH

Router 0	PC0	PC1
IP Address : 192.168.1.1 Gate way : -	IP Address : 192.168.1.2 Gate way : 192.168.1.1	IP Address : 192.168.1.3 Gate way : 192.168.1.1

ROUTER CLI:

Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password sai123
Router(config-line)#login local
Router(config-line)#exit
Router(config)#username saimukhesh privilege 4 password sai123
Router(config)#hostname r1
r1(config)#ip domain-name cisco
r1(config)#line vty 0 4
r1(config-line)#transport input ssh
r1(config-line)#exit
r1(config)#crypto key generate rsa
The name for the keys will be: r1.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

0r1(config)#
*Mar 1 0:3:53.842: %SSH-5-ENABLED: SSH 1.99 has been enabled
r1(config)#

OUTPUT:

PINGING FROM PC1 TO SERVER USING SSH:

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

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 = 0ms, Average = 0ms

C:\>ssh -l saimukhesh 192.168.1.1

Open
Password: <sai123>

r1#

(now router can be accessed from pc1)

Result:

Thus, verified the operation of SSH and accessed the router from a remote Pcs.

VIVA QUESTIONS

What is SSH?

Secure Shell protocol is abbreviated as SSH. It is a secure and most commonly using protocol to access remote servers. This protocol uses encryption while transferring data between two hosts.

What is SSH port forwarding ?

SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming.

Syntax : ssh -L localport:host:hostport user@ssh_server –N

where:
-L – port forwarding parameters
localport – local port (chose a port that is not in use by other service)
host – server that has the port (hostport) that you want to forward
hostport – remote port
-N – do not execute a remote command, (you will not have the shell)
user – user that have ssh access to the ssh server (computer)
ssh_server – the ssh server that will be used for forwarding/tunnelling

How to enable debugging in ssh command ?

To enable debugging in ssh command use '-v' option like 'ssh root@www.linuxtechi.com -v'. To increase the debugging level just increase the number of v's.

What is the difference between ssh & Telnet ?

In ssh communication between client & server is encrypted but in telnet communication between the client & server is in plain text . We can also say SSH uses a public key for authentication while Telnet does not use any authentication.SSH adds a bit more overhead to the bandwidth compared to Telnet. Default port of ssh is 22 and for telnet 23.

How to check SSH server's Version ?

Using the command ' ssh -V ' we can find the ssh server's version.

Experiment: 11

AODV ROUTING

Aim:

To understand the operation of AODV Routing using MATLAB Software

Apparatus required

- PC loaded Matlab Software

Procedure

- Open new M –file
- Type the program and save the file and Run.
- Apply input particulars and observe the output data as a Routing information table.

Theory

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing. The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is therefore considered an on-demand algorithm and does not create any extra traffic for communication along links.

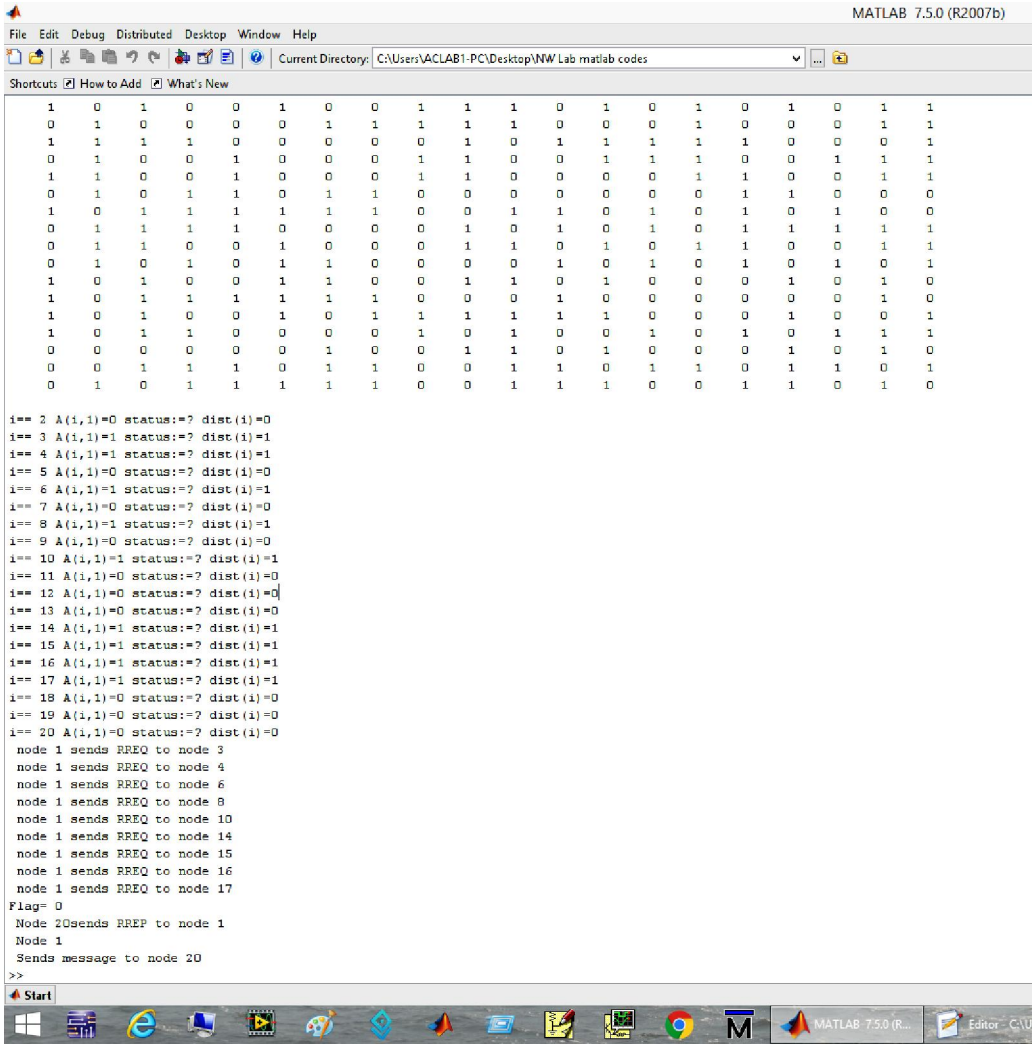
Matlab Program for AODV Routing.

```
x=1:20;
s1=x(1);
d1=x(20);
clc;
A=randint(20);
% Making matrix all diagonals=0 and A(i,j)=A(j,i),i.e. A(1,4)=a(4,1),
% A(6,7)=A(7,6)
for i=1:20
    for j=1:20
        if i==j
            A(i,j)=0;
        else
            A(j,i)=A(i,j);
        end
    end
end
disp(A);
```

```
            t=1:20;
            disp(t);
           disp(A);
           status(1)='!';
           dist(1)=0;
           next(1)=0;
 for i=2:20
        status(i)='?';
    dist(i)=A(i,1);
    next(i)=1;
  disp(['i== ' num2str(i) ' A(i,1)=' num2str(A(i,1)) ' status:=' status(i) ' dist(i)=' num2str(dist(i))]);
end

flag=0;
for i=2:20
      if A(1,i)==1
         disp([' node 1 sends RREQ to node ' num2str(i)])
            if i==20 && A(1,i)==1
                  flag=1;
            end
      end
end
disp(['Flag= ' num2str(flag)]);
while(1)

   if flag==1
         break;
   end

   temp=0;
   for i=1:20
      if status(i)=='?'
         min=dist(i);
         vert=i;
         break;
      end
   end
```

```
  for i=1:20
      if min>dist(i) && status(i)=='?'
          min=dist(i);
          vert=i;
      end
   end
   status(vert)='!';

   for i=1:20
      if status()=='!'
          temp=temp+1;
      end
   end

   if temp==20
      break;
   end
end

i=20;
count=1;
route(count)=20;

while next(i) ~=1
    disp([' Node ' num2str(i) 'sends RREP message to node ' num2str(next(i))])
    i=next(i);
    %disp(i);
    count=count+1;
    route(count)=i;
    route(count)=i;
end

disp([ ' Node ' num2str(i) 'sends RREP to node 1'])
disp(' Node 1 ')
for i=count: -1:1
    disp([ ' Sends message to node ' num2str(route(i))])
end
```

AODV OUTPUT



Result:

Thus, Simulated and verified the operation of AODV Routing Algorithm and understand its operation.

Experiment: 12

DISTANCE VECTOR ROUTING

Aim:

To understand the operation of Distance Vector Routing using MATLAB Software

Requirements:

- PC Loaded with Matlab Software

Procedure:

- Open new M –file
- Type the program and save the file and Run.
- Apply input particulars and observe the output data as a Routing information table.

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, on which a distance-vector protocol is implemented, 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 informs its neighbours of network topology changes periodically.

Distance-vector routing protocols use the Bellman–Ford algorithm and Ford–Fulkerson algorithm to calculate the best route. Another way of calculating the best route across a network is based on link cost, and is implemented through link-state routing protocols.

The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network. The distance vector algorithm was the original ARPANET routing algorithm and was implemented more widely in local area networks with the Routing Information Protocol (RIP).

Matlab Program for Distance Vector Routing

```
clc;
clear all;
ack=0;
s=input('Enter the source router no: ');
z=input('Enter the destination node: ');
while ack==0
%delay routing tables for 5 modes
A=randint(1,5,100);%metric may be delay or no of hops
B=randint(1,5,100);
C=randint(1,5,100);
D=randint(1,5,100);
E=randint(1,5,100);
A(1)=0;B(2)=0;C(3)=0;D(4)=0;E(5)=0;
r=vertcat(A,B,C,D,E);
disp('All routers are updated with routing tables of neighbouring routers');
fprintf('The routing tables for router %d is \n',s);
disp(r);
d(1,5)=0;
count=1;
for i=s
for j=1:5
if j~=i
for k=1:5
if k~=j && k~=i
for l = 1:5
if l~=k && l~=j && l~=i
for m = 1:5
if m~=k && m~=j && m~=i && m~=l
if(m==z)
d(count,:)=[i,j,k,l,m];
count=count+1;
end
end
end
end
end
```

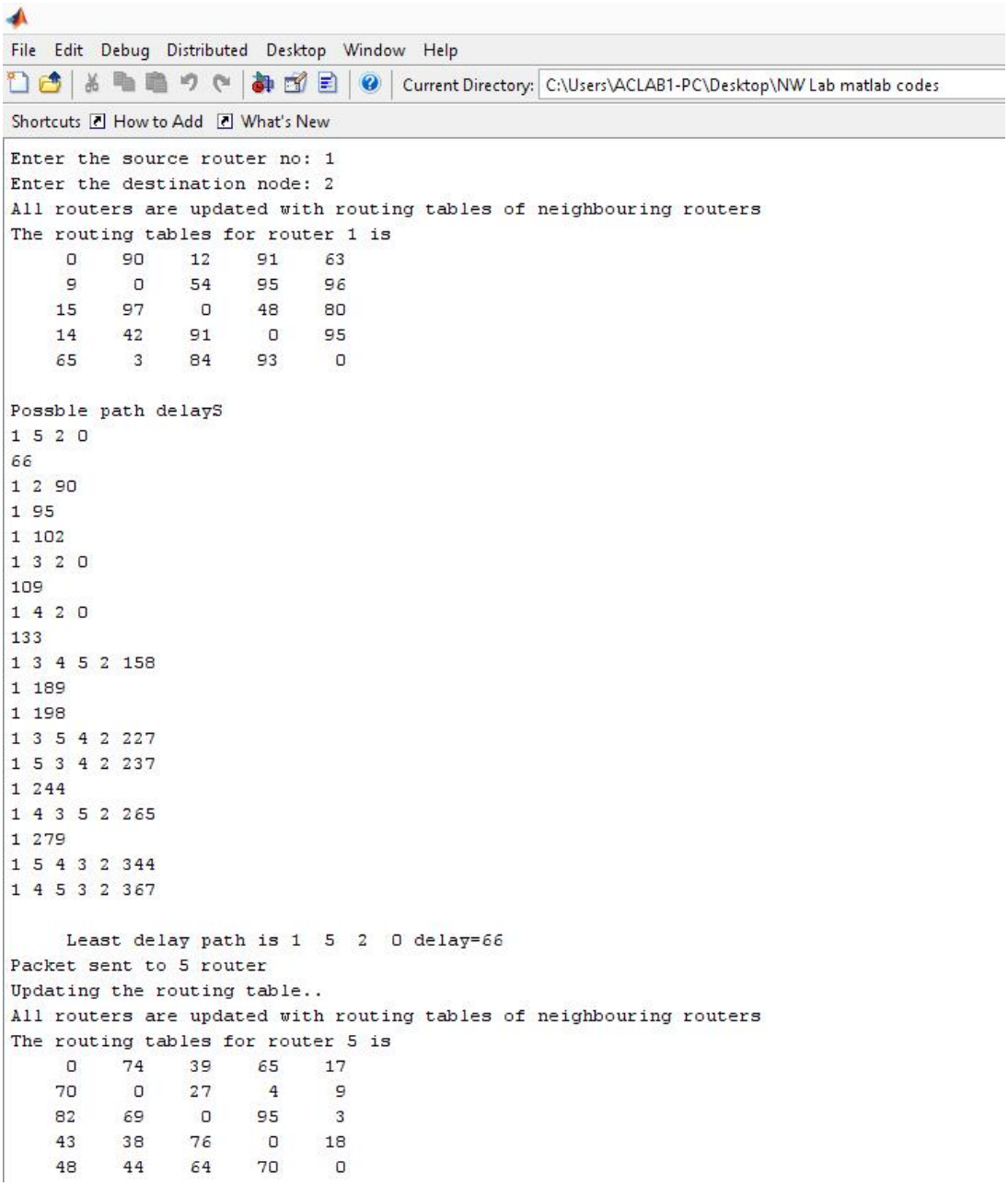
```
end
end
end
end
end
count1 =1;
for i=s
for j=1:5
if j~=i
for k=1:5
if k~=j && k~=i
for l=1:5
if l~=k && l~=j && l~=i
if l==z
c(count1,:)=[i,j,k,l];
count1= count1+1;
end
end
end
end
end
end
end
end
count2 = 1;
for i=s
for j=1:5
if j~=i
for k=1:5
if k~=j && k~=i
if k==z
e(count2,:) = [i,j,k,0];
count2= count2 + 1;
end
end
end
end
end
```

```
end
%finding the total delay of all possible paths
for i=1:6
del(i)=0;
for j=2:5
del(i)=del(i)+r(d(i,j-1),d(i,j));
end
end
count=i+1;
for i=1:6
del(count)=0;
for j=2:4
del(count)=del(count)+r(c(i,j-1),c(i,j));
end
count=count+1;
end
for i=1:3
del(count)=0;
for j=2:3
del(count)=del(count)+r(e(i,j-1),e(i,j));
end
count=count+1;
end
del(count)=r(s,z);
dc= sort(del);
%possible paths and latest delay paths
fprintf('Possble path delayS');
for i=1:count
for j=1:count
if dc(i)==del(j)
n(i)=j;
if j<=6
fprintf('\n%d %d %d %d %d %d %d',d(j,:),dc(i));
ma(i,:)=cellstr(num2str(d(j,:)));
elseif j<=12
fprintf('\n%d %d %d %d %d',c(j-6),dc(i));
ma(i,:)=cellstr(num2str(c(j-6)));
elseif j<=15
```

```
fprintf('\n%d %d %d %d',e((j-12),:),dc(i));
ma(i,:)=cellstr(num2str(e((j-12),:)));
elseif j==16
fprintf('\n%d %d %d',s,z,dc(i));
ma(i,:)=cellstr(num2str([s z]));
end
end
end
end
temp=dc(1);
for i=2:count
if(dc(i)<=temp)
temp=dc(i);
end
end
for i=1:count
if(dc(i)==temp)
break;
end
end
disp(sprintf('\n\n\t Least delay path is %s delay=%d',(char(ma(i))),dc(i)));
m(16,5)=0;
e=char(ma);
for i=1:length(ma)
m(i,1)=str2double(cellstr(e(i,1)));
m(i,2)=str2double(cellstr(e(i,4)));
m(i,3)=str2double(cellstr(e(i,7)));
m(i,4)=str2double(cellstr(e(i,10)));
m(i,5)=str2double(cellstr(e(i,13)));
end
k=m(1,2);
disp(sprintf('Packet sent to %d router',k));
disp('Updating the routing table..');
```

```
if (m(1,1)==s&&m(1,2)==z)
ack=1;
disp(sprintf('Packet sent to the destination router %d',z));
end
s=m(1,2);
z=m(1,3);
end
```

DVR OUTPUT




```
Enter the source router no: 1
Enter the destination node: 2
All routers are updated with routing tables of neighbouring routers
The routing tables for router 1 is
     0    90    12    91    63
     9     0    54    95    96
    15    97     0    48    80
    14    42    91     0    95
    65     3    84    93     0

Possble path delayS
1 5 2 0
66
1 2 90
1 95
1 102
1 3 2 0
109
1 4 2 0
133
1 3 4 5 2 158
1 189
1 198
1 3 5 4 2 227
1 5 3 4 2 237
1 244
1 4 3 5 2 265
1 279
1 5 4 3 2 344
1 4 5 3 2 367

     Least delay path is 1  5  2  0 delay=66
Packet sent to 5 router
Updating the routing table..
All routers are updated with routing tables of neighbouring routers
The routing tables for router 5 is
     0    74    39    65    17
    70     0    27     4     9
    82    69     0    95     3
    43    38    76     0    18
    48    44    64    70     0
```

Result:

Thus, Simulated and verified the operation of Distance Vector Routing Algorithm and understand its operation.

Experiment: 13

Pure ALOHA Protocol

Aim:

To understand the operation of Pure Aloha protocol using MATLAB Software

Requirements:

- PC Loaded with Matlab Software

Procedure:

- Open new M –file
- Type the program and save the file and Run.
- Apply input particulars and observe the output data

Theory

Pure ALOHA and Slotted ALOHA both are the Random Access Protocols, that are implemented on the Medium Access Control (MAC) layer, a sublayer of Data Link Layer. The purpose of the ALOHA protocol is to determine that which competing station must get the next chance of accessing the multi-access channel at MAC layer.

Pure ALOHA

The version of the protocol "Pure ALOHA" is quite simple:

1) If you have data to send, send the data

This first step implies that Pure ALOHA does not check whether the channel is busy before transmitting.Since collisions can occur and data may have to be sent again, ALOHA cannot use 100% of the capacity of the communications channel. How long a station waits until it transmits, and the likelihood a collision occurs are interrelated, and affects how efficiently the channel can be used.

2) If, while you are transmitting data, you receive any data from another station, there has been a message collision. All transmitting stations will need to try resending "later".

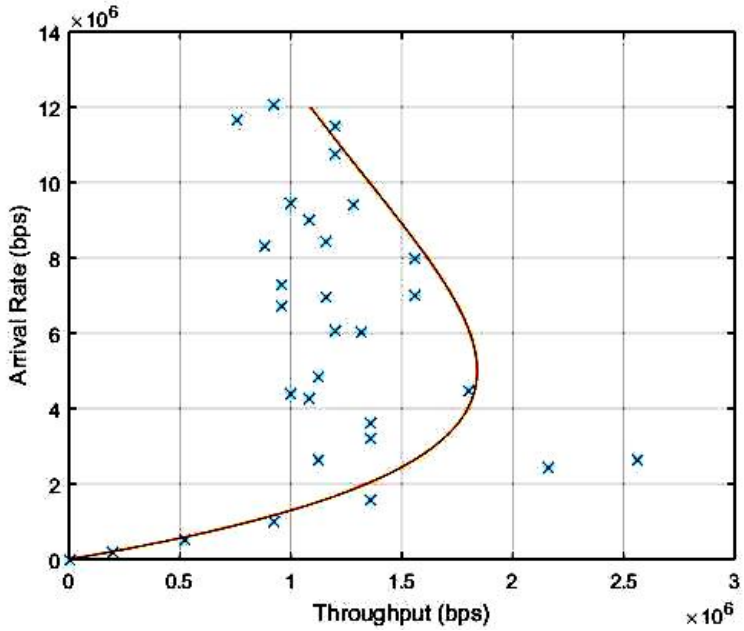
The concept of "transmit later" is a critical aspect: the quality of the backoff scheme chosen significantly influences the efficiency of the protocol, the ultimate channel capacity, and the predictability of its behavior.

Matlab Program for pure Aloha protocol

```
%total simulation time in seconds
        runtime=0.2;
%total number of stations
        nstation=10;
%transmission throughput of the media in bits per second
        netthrou=10e6;
%frame size in bits
        fsize=8000;
%avarage frame arrival rate per second for each station
%frate=10;
        for frate=1:5:150
%average frame arrival rate per simulation iteration
        trh=frate/10000;
%random wait window in number of simulation iterations
        wwind=100;
%EVENTS VARIABLES
%transmit active
        tr=zeros(1,nstation);
%transmit queue
        tq=zeros(1,nstation);
%transmit progress counter
        tcnt=zeros(1,nstation);
%collision keeper
        colis=zeros(1,10000*runtime);
%collision station index
        colin=zeros(1,nstation);
%random wait after collision
        rwait=zeros(1,nstation);
%transmit keeper
trkeep=zeros(nstation,10000*runtime);

%packet arrival keeper
pakeep=0;
for i=1:10000*runtime
for j=1:nstation
   %check if the transmitter is active
   if tr(j)==1
      trkeep(j,i)=1;
   end
   %check if the packet has been sent
    if tcnt(j)>0
      tcnt(j)=tcnt(j)-1;
      if tcnt(j)==0
         tr(j)=0;
```

```
 %check if the transmission is collision free
          if colin(j)==1
             rwait(j)=ceil(wwind*rand(1,1));
             tq(j)=tq(j)+1;
             colin(j)=0;
          end
       end
    else
       if tq(j)>0 & rwait(j)==0
          tr(j)=1;
          tcnt(j)=ceil(fsize/netthrou*10000);
          tq(j)=tq(j)-1;
       end
    end
    %check if a new packet has arrived
    pa=rand(1,1);
    if pa<trh
       pakeep=pakeep+1;
       %if the transmit is ready
       if tr(j)==0 & rwait(j)==0
         tr(j)=1;
         tcnt(j)=ceil(fsize/netthrou*10000);
       else
         tq(j)=tq(j)+1;
       end
    end
    %decrease random waiting count
    if rwait(j)>0
       rwait(j)=rwait(j)-1;
    end
end

%check for collision
if sum(tr)>1
       colis(i)=1;
       for k=1:nstation
          if tr(k)==1
             colin(k)=1;
          end
       end
end
end
px1(frate)=(pakeep-sum(tq));
py1(frate)=pakeep;
end
g1=[0:0.01:1.2];
s1=g1.*exp(-2*g1);
figure(1)
plot(px1*8000/runtime,py1*8000/runtime,'x',s1*1e7,g1*1e7,'-')
grid
xlabel('Throughput (bps)')
ylabel('Arrival Rate (bps)')
```

Pure Aloha output:



Result:

Thus, Simulated and verified the operation of Pure ALOHA Protocol Algorithm and understand its operation.

Experiment: 14

Slotted ALOHA Protocol

Aim:

To understand the operation of Slotted Aloha protocol using MATLAB Software

Requirements:

- PC Loaded with Matlab Software

Procedure:

- Open new M –file
- Type the program and save the file and Run.
- Apply input particulars and observe the output data

Theory

Slotted ALOHA

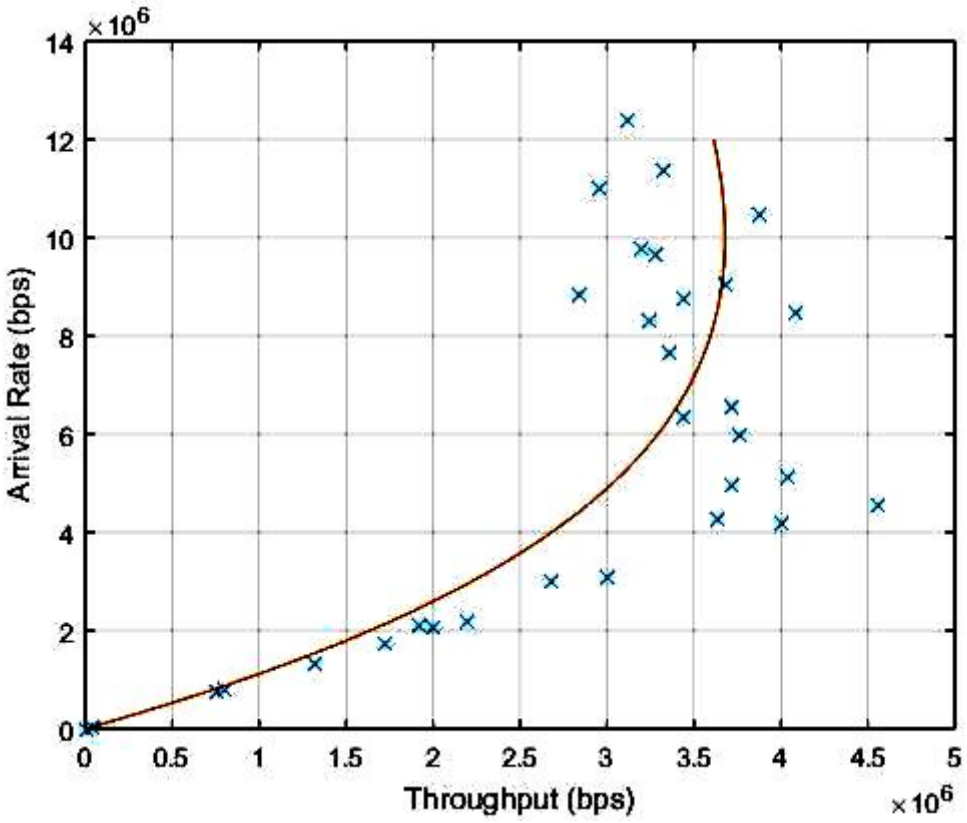
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.
- In this method it was proposed that the time be divided up into discrete intervals (T) and each interval correspond to one frame .i.e the user should agree on the slot boundaries and require each station to begin each transmission at the beginning of a slot.
- Even if station is ready to send in middle of a slot, it must wait until the beginning of the next one.

Matlab Program for slotted Aloha protocol

```
%total simulation time in seconds
        runtime=0.2;
%total number of stations
        nstation=10;
%transmission throughput of the media in bits per second
        netthrou=10e6;
%frame size in bits
        fsize=8000;
%avarage frame arrival rate per second for each station
%frate=10;
        for frate=1:5:150
%average frame arrival rate per simulation iteration
        trh=frate/10000;
%random wait window
        wwind=100;
% EVENTS VARIABLES
%transmit active
        tr=zeros(1,nstation);
%transmit queue
        tq=zeros(1,nstation);
%transmit progress counter
        tcnt=zeros(1,nstation);
%collision keeper
        colis=zeros(1,10000*runtime);
%collision station index
        colin=zeros(1,nstation);
%random wait after collision
        rwait=zeros(1,nstation);
%transmit keeper
        trkeep=zeros(nstation,10000*runtime);
%packet arrival keeper
        pakeep=0;
for i=1:10000*runtime
for j=1:nstation
   %check if the transmitter is active
   if tr(j)==1
      trkeep(j,i)=1;
   end
   %check if the packet has been sent
    if tcnt(j)>0
      tcnt(j)=tcnt(j)-1;
      if tcnt(j)==0
         tr(j)=0;
```

```
 %check if the transmission is collision free
          if colin(j)==1
             rwait(j)=ceil(wwind*rand(1,1));
             tq(j)=tq(j)+1;
             colin(j)=0;
          end
       end
    else
       if tq(j)>0 & rwait(j)==0 & mod(i,8)==0
          tr(j)=1;
          tcnt(j)=ceil(fsize/netthrou*10000);
          tq(j)=tq(j)-1;
       end
    end
    %check if a new packet has arrived
    pa=rand(1,1);
    if pa<trh
       pakeep=pakeep+1;
       %if the transmit is ready
       if tr(j)==0 & rwait(j)==0 & mod(i,8)==0
         tr(j)=1;
         tcnt(j)=ceil(fsize/netthrou*10000);
       else
         tq(j)=tq(j)+1;
       end
    end
    %decrease random waiting count
    if rwait(j)>0
       rwait(j)=rwait(j)-1;
    end
end
%check for collision
if sum(tr)>1
       colis(i)=1;
       for k=1:nstation
          if tr(k)==1
             colin(k)=1;
          end
       end
end
end
px2(frate)=(pakeep-sum(tq));
py2(frate)=pakeep;
end
g2=[0:0.01:1.2];
s2=g2.*exp(-g2);
figure
plot(px2*8000/runtime,py2*8000/runtime,'x',s2*1e7,g2*1e7,'-')
grid
xlabel('Throughput (bps)')
ylabel('Arrival Rate (bps)')
```

Slotted Aloha output:



Result:

Thus, Simulated and verified the operation of Pure ALOHA Protocol Algorithm and understand its operation.