Practical No.01

Aim :- Installation and introduction of simulation tools packet tracer.

Theory :-

→ Packet tracer is a network simulation and visualization tool developed by cisco system. It is commonly used for educational purpose particularly in networking courses and training programs.

→ With packet tracer, user can design, configue and troubleshoot virtual networks in simulation environment.

• Steps to install Packet Tracer on linux

Step① : Download Packet Tracer
→ Visit the cisco networking academy website or cisco official website to download linux version of packet tracer.

Step② : Extract the package
→ Once the download is complete navigate to directory where packet tracer package is downloaded. Extract the package.

Date :

Step ③ : Navigate the to extracted folder.

Step ④ : Rcen the installation script using command "/Install" terminal

Step ⑤ : Launch packet tracer using command packettraces in terminal.

Result :- Hence, the packet tracer, Simulation tool was successfully installed.

Checked
21/03/24

Date :

Practical no. 2

Aim:- Design of local area network (LAN) using packet tracer simulation tool.

Theory :-

- Network:
  When two or more entities or systems are interconnected and sending and receiving of data takes place, this is known as network.

- Topology:
  It refers to physical or logical layout or configuration of devices and connections within a network. It defines how data flows between them.

- LAN:
  It stands for local area network. It's a network that covers small geographical area, typically within a single building or campus. They are commonly used in homes, offices, schools, to facilitate local communication, file sharing, internet access and other networking activities.

- Packet Tracer
  It is a network simulation and visualization tool developed by cisco systems. It allows users

Date :

to create, configure and simulate networks in virtual environment, without the need for physical hardware.

Procedure :

Step ① : Launch the packet tracer application on your computer.

Step ② : drag and drop two devices onto the workspace.

Step ③ : Click on first PC (device) to select it. Select fast Ethernet interface.

Step ④ : click and drag copper cross over cable from 1st device to 2nd device.

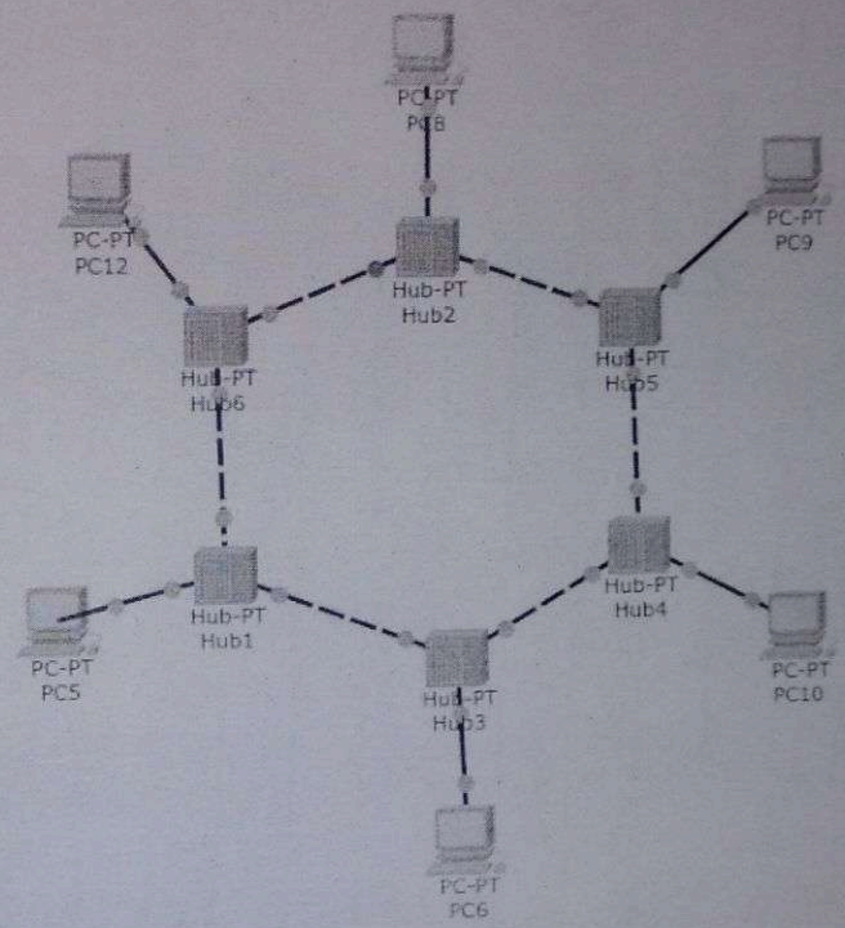
Step ⑤ : Click on each device to open its configuration window.

Step ⑥ : Go to 'desktop' tab, then click on "IP configuration".

Step ⑦ : Assign IP address to each PC.

Step ⑧ : Open command prompt on each device and try to ping each other's IP addresses to verify connectivity.

Logical [Root] New Cluster Move Object Set Tiled Background Viewport



Time: 01:30:45 Power Cycle Devices Fast Forward Time

Connections

Scenario 1 New Delete Toggle PDU List Window

Real

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC8	PC6	ICMP	
	Successful	PC9	PC5	ICMP	

Date :

Practical No. 03

Aim :- Execute basic network commands and network configuration.

Theory :-

- Basic Network Commands

① Ping :

- Syntax : 'ping [hostname or IP address]'
- Use :

→ It is used to test the reachability of a host on an Internet Protocol (IP) network. It sends ICMP echo request packets to the target hosts and waits for ICMP echo reply packets. It measures the round-trip time and any packets loss between the source and destination.

② IPconfig :

- Syntax : 'ipconfig'
- Use :

→ It displays the configuration of network interface on unix-like operating system. It can be used to view, configure and troubleshoot network

PC1

Physical | Config | Desktop | Custom Interface

Command Prompt

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0001.63B4.C1E9
   Link-local IPv6 Address.....: FE80::201:63FF:FEB4:C1E9
   IP Address.....: 26.27.28.2
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 0.0.0.0
   DNS Servers.....: 0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 Client DUID.....: 00-01-00-01-77-90-C8-AB-00-01-63-B4-C1-E9

PC>ping 26.27.28.2

Pinging 26.27.28.2 with 32 bytes of data:

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

Ping statistics for 26.27.28.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Time: 00:05:06 | Power Cycle Devices | Fast Forward Time

Scenario 0 | New | Delete

Fire | Last Status | Source | Destinatio

Logical [Root] New Cluster Move Object Set Tiled Background Viewpo

PC18

Physical Config Desktop Custom Interface

Command Prompt

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 00D0.BA77.C787
   Link-local IPv6 Address.....: FE80::2D0:BAFF:FE77:C787
   IP Address.....: 13.13.13.1
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: 0.0.0.0
   DNS Servers.....: 0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 Client DUID.....: 00-01-00-01-64-C0-66-A2-00-D0-BA-77-C7-87

PC>ping 13.13.13.2

Pinging 13.13.13.2 with 32 bytes of data:

Reply from 13.13.13.2: bytes=32 time=1ms TTL=128
Reply from 13.13.13.2: bytes=32 time=0ms TTL=128
Reply from 13.13.13.2: bytes=32 time=0ms TTL=128
Reply from 13.13.13.2: bytes=32 time=0ms TTL=128

Ping statistics for 13.13.13.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Time: 01:31:41

End Devices

Generic Generic Generic Generic IPPhone VoIP Device

Scenario 0 New Delete Toggle PDU List Window

Fire Last Status Source Destination

Date :

③ IP config all :

- Syntax : 'ip config/all'
- Uses :

→ The 'IPConfig/all' command in windows displays detailed information about all network interfaces, including their IP addresses. Subnet masks, default gateway, DNS servers, MAC addresses and more. It provides a comprehensive overview of the network configuration of system.

Result :-

Hence, all three basic network commands are executed successfully.

21/03/24

Date :

Practical NO. 04

Aim :- Implementation of different topology in Cisco packet tracer.

Theory :-

- Topology

Topology refers to physical or logical layout or configuration of devices and connections within a network. It defines how devices are interconnected and how data flows between them.

→ Different types of topology :-

1. Star Topology

In a star topology all devices are connected to a ~~control~~ central hub or switch communication between devices occurs through this central point. It's easy to add or remove devices, but if the central hub fails, the entire network can be affected.

2. Bus Topology

In as bus topology, all devices are connected to a single backbone cable. Data is transmitted along a cable, and each device receives the data but only processes data intended for it. It's simple but inexpensive, but if the backbone cable fails, the entire network can go down.

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

PC-PT PC15

PC-PT PC13

2960-24TT Switch1

2960-24TT Switch3

2960-24TT Switch2

2960-24TT Switch4

PC-PT PC12

PC-PT PC14

Time: 00:55:44 Power Cycle Devices Fast Forward Time

Connections

Scenario 0 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type
	Successful	PC12	PC13	ICMP
	Successful	PC14	PC13	ICMP
	Successful	PC15	PC12	ICMP

File Edit Options View

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

PC-PT
PC26

PC-PT
PC24

2960-24TT
Switch0

PC-PT
PC18

PC-PT
PC21

PC-PT
PC22

Realt

Time: 01:31:12 Power Cycle Devices Fast Forward Time

End Devices

Generic Generic Generic Generic IPPhone VoIP Device

Scenario 0

New Delete

Toggle PDU List Window

Console

Last Status Source Destination Type

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

PC-PT PC17
PC-PT PC18
PC-PT PC21
PC-PT PC22
PC-PT PC23
PC-PT PC16
2950-24 Switch10
2950-24 Switch11
2950-24 Switch14
2950-24 Switch15
PC-PT PC24
PC-PT PC19
PC-PT PC20

Realtime

Time: 01:12:48 Power Cycle Devices Fast Forward Time

Connections

Scenario 0 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC18	PC17	ICMP		0.000
	Successful	PC19	PC16	ICMP		0.000
	Successful	PC21	PC20	ICMP		0.000

Date :

3. Ring topology
In this topology, each devices is connected to two other devices, farming a ring, like structure. Data troubles in one direction around the ring until it reaches its destination its efficient, but if one devices or connection fails, the entire network can be affected.

4. Mesh topology
In this topology, every device is connected to every other device in the network. This provides redeendancy and multiple paths for data to travel, making it every reliable. However, it can be affected. complex and costly to implement.

5. Hybrid topology:
A hybrid topology is a combination of two or more basic topologies, such as a star-bus topology or star-ring topology. This allows for flexibility and scalability.

Result:-
Hence, all the different topologies are implemented successfully.

21/03/24

Date :

Practical No. 05

Aim :- Interior or exterior protocal
1] BGP - Border Gateway Protocal
2] OSPP - Open Shortest Path First

Theory :-
1] BGP (Border Gateway Protocol) : BGP is a standerdized exterior gateway protocol used to exchange information between autonomous system (Ases) on the internet between different service providers. Unlike interior gateway protocols (IGPS) such as OSPP or RIP, which operate within a single autonomous system. BGP is designed for interdomain roitings and operates between different autonomous system.

2] Path vector protocol : BGP is a path vector protocol which means it exchanges routing information along with the paths to reach those destination. Each BGP router advertises the list of autonomous System (Ases) it traversed to reach a particular destination network (prefix).

TCP - Based protocal : BGP operates over TCP (Transmission control protocals)

3] BGP sessions and peering : BGP router estableish. TCP connections, called BGP session with neighbouring routers in other (Ases).

Date :

4] Attributes :- BGP uses various attributes to describe and manipulate routing information
→ As path, NEXT.HOP, weight local, multe-Exit Discrimination (MED).

5] Route selection process : BGP router use a set of rules ~~of~~ to select the best route for a given destination.

6] Route Advertisement and propagation : BGP routes advertise routers to their neighbours based on local policies and route selection outcomes.

7] BGP communities :- BGP communities are tags that can be attached to routes to group them based on common policies or attributes.

8] Route Aggregation : BGP supports route aggregation which allows multiple contiguous IP prefixes to be represented by a single, summarized route.

9] OSPF - Open Shortest Path First :

Open Shortest Path First is a link state routing protocol that is used to find the best path between the source and the destination router using its own shortest path list first. OSPP is developed by internet engineering.

Date :

Task force. (IETF) as one of the Interior ~~gateway~~ gateway protocol (IGP), the protocol which works on protocol number 89 and uses. AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router CDR 1 Backup designated Router (BDR).

OSPF terms:

1) Router id : It is the highest active IP address present on the router. First, the highest address is considered.
2) Router priority : It is an 8 bit value assigned, to a router operating OSPF, used to select DR and BDR.
3) Designated Router (DR) : BDR is a backup to DR in a broadcast network.
4) DR and BDR election : DR and BDR election takes place in the broadcast network.

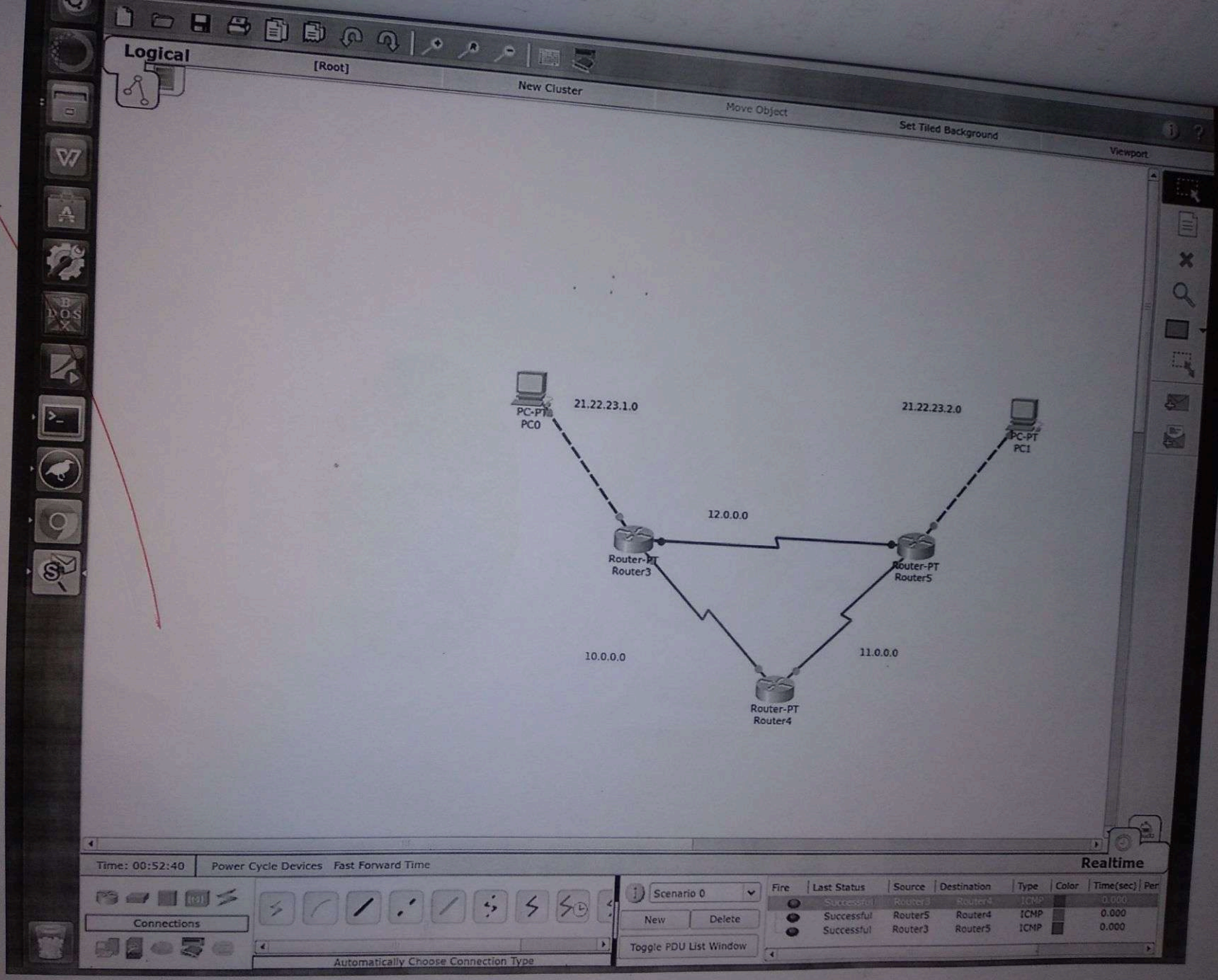
OSPF states :

1) Down : In this state, no hello packet have been received on the interface.

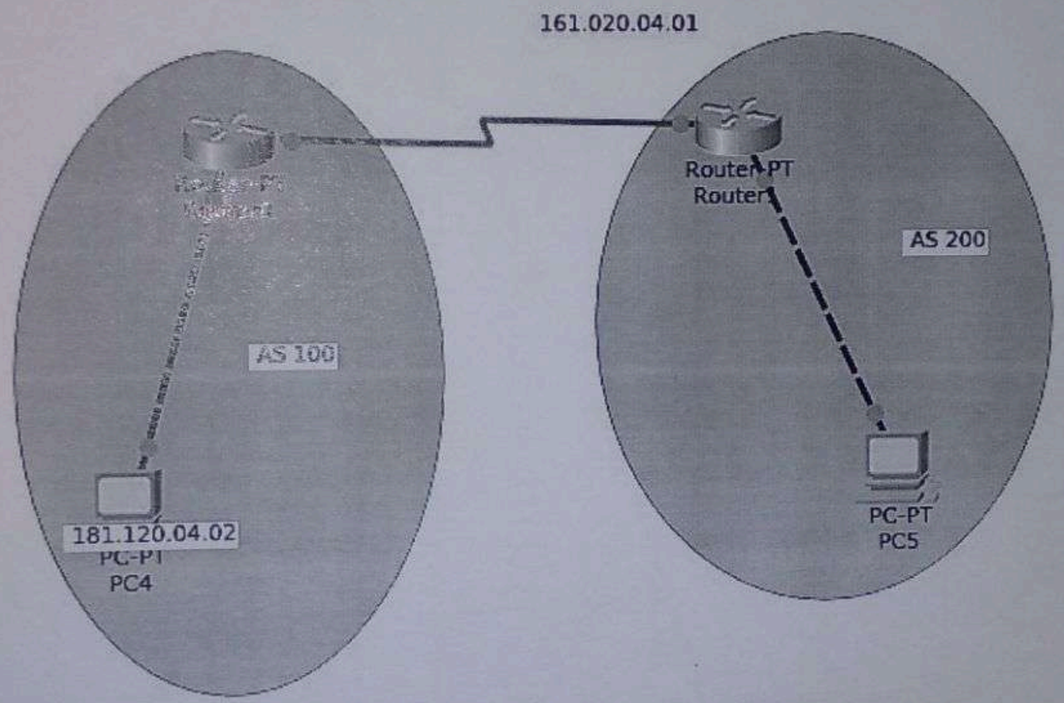
2) INIT : In this state, the hello packets have been received from the other routes.

3) 2 way : In this 2 way state, both the routers have received the hello packets from others.

Page No.


Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC-PT
PC0
21.22.23.1.0
21.22.23.2.0
PC-PT
PC1
12.0.0.0
Router-PT
Router3
Router-PT
Router5
10.0.0.0
11.0.0.0
Router-PT
Router4
Time: 00:52:40
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Per
Successful
Router5
Router4
ICMP
0.000
Successful
Router3
Router5
ICMP
0.000

Logical [Root] New Cluster Move Object Set Tiled Background



Time: 01:18:48 Power Cycle Devices Fast Forward Time

Connections

Automatically Choose Connection Type

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC5	Router1	ICMP	
	Successful	PC5	Router1	ICMP	
	Successful	PC5	Router1	ICMP	
	Successful	PC5	Router1	ICMP	

Date :

4) Exstart : In this, state, NULL DBD are exchanged In this state, the master and slave elections takeplace.

5) Exchange : In this state, the actual DBDs are exchanged.

6) Loading : In this state, LSR, LSU and LSA are exchanged.

7) FULL : In this state, synchronization of all the information takes place.

Result :- Hence a interior or exterior protocal are executed successfully.

Page No. 18

Date :

Practical No. 06

Aim :- Implementation of operation on Routing Information Protocal.

Theory :-

→ RIP stands for Routing Information Protocol this is an inter domain routing protocal, used within an autonomous system.

→ In simple terms, it helps routes packets within specific domain such as web browsing within an institutional area.

* Key points of RIP:

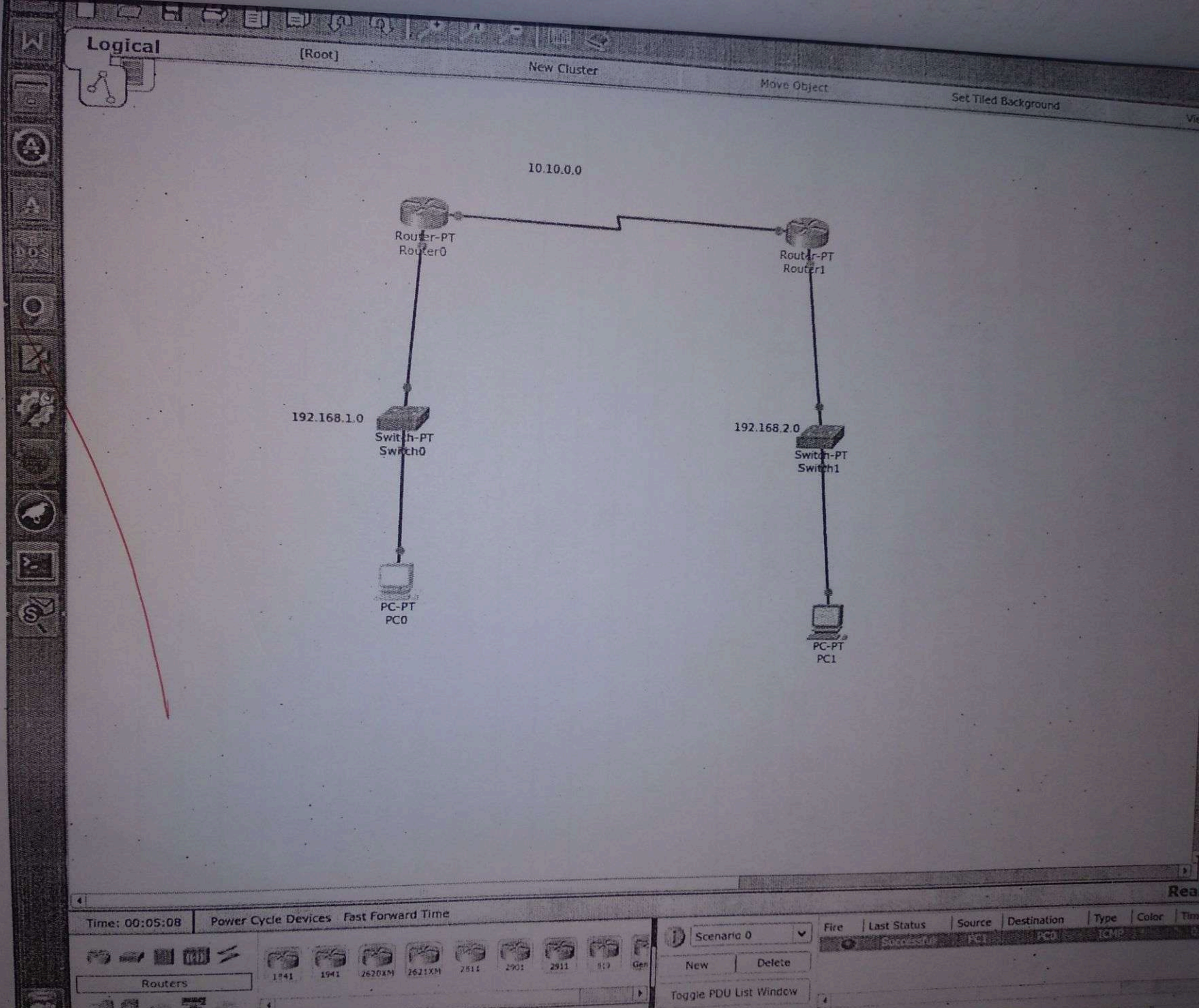
① Distance Vector Based Strategy:

→ RIP is based on distance vector approach, imagine entire network graph where nodes represent routers and link represent networks. The goal is to find best path to reach destination.

② NOP count metric:

→ RIP uses no. of nops as its routing metric each hop corresponds to moving from one network segment to another.

→ RIP is suitable for smaller networks. It can handle upto 15 hops.


Logical
[Root]
New Cluster
Move Object
Set Tiled Background
10.10.0.0
Router-PT
Router0
Router-PT
Router1
192.168.1.0
Switch-PT
Switch0
192.168.2.0
Switch-PT
Switch1
PC-PT
PC0
PC-PT
PC1
Time: 00:05:08
Power Cycle Devices
Fast Forward Time
Routers
1841
1941
2620XM
2621XM
2811
2901
2911
Router-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color

Date :

→ 8-bit field indicates whether its a requests or a reply.

→ RIP is an older distance vector protocol that uses hop count as its metric. It presents routing loops by limiting the no. of hops allowed in a path from source to destination.

Result :- Hence the operation on Routing Information Protocol implemented successfully.

15/04/24

Practical No: 07

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

Theory:-

ARP stands for Address Resolution Protocol.
It is a protocol used in ethernet and IP networks to map IP addresses to MAC addresses. Here some key components:

1. Address Resolution:- When a device in a network wants to communicate with another device. It needs to know the MAC address of the destination device.

2. ARP Request:
If the MAC address of the destination device is not known, the sending device broadcasts an ARP request packet onto the network. This request contains the IP address of the destination device.

3. ARP Reply:-
The device with the specified IP address responds to the ARP request with its MAC address, using an ARP reply packet.

4. Caching
Upon receiving the ARP reply, the sending device caches the mapping of the IP address to the

Cisco Packet Tracer Student

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background

Viewport

Switch0

PC-PT PC0 18.18.18.1

PC-PT PC1 18.18.18..2

PC-PT PC2 18.18.18.3

Simulation Panel

Event List

Vis.	Time(sec)	Last Devic	At Device	Type	Info
	0.000	–	PC0	ICMP	
	0.000	–	PC0	ARP	
	0.001	PC0	Switch0	ARP	
	0.002	Switch0	PC1	ARP	
	0.002	Switch0	PC2	ARP	
	0.003	PC2	Switch0	ARP	
	0.004	Switch0	PC0	ARP	
	0.004	–	PC0	ICMP	
	0.005	PC0	Switch0	ICMP	

Reset Simulation | Constant Delay | Captured to: 0.005 s

Play Controls

Back | Auto Capture / Play | Capture / Forward

Event List Filters - Visible Events

ARP, ICMP

Edit Filters | Show All/None

Time: 00:05:59.352 | Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward | Simulation

Connections

Automatically Choose Connection Type

Scenario 0 | New | Delete | Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Peri

Date :

MAC address in it ARP table. This caching helps to speed up future communication by avoiding the need for ARP requests. or known IP addresses.

5. Timeouts: ARP entries in the cache have a limited lifetime and expire after a certain period of time. This ensures that the ARP cache remains up to date with any changes in the network.

ARP is a critical protocol for communication within local networks, allowing devices to dynamically discover and maintain mapping between IP and MAC addresses without manual configuration. However its important to note that ARP operates at layer 2 (Data Link Layer) of the OSI model and is specific to ethernet networks.

Result:- Thus, this program has been executed successfully.

Page No. 17

control

Date :

Practical No. : 08

Aim :- Write a program for congestion control using leaky bucket algorithm.

Theory :- The leaky Bucket algorithm is a simple congestion control mechanism used in networking to regulate the rate at which data is transmitted from a source to a destination. It helps smooth out bursts of traffic and prevents network congestion by enforcing a maximum average rate of data transmission. Here's a theoretical explanation. Followed by a python program implementing the Leaky Bucket algorithm:

① Bucket : Imagine a bucket with a hole at the bottom. The bucket represents a buffer that can hold a limited amount of data (bucket size).

② Arrival of Packets : Incoming packets (data) are added to the bucket at a certain rate. These packets may arrive at irregular intervals, potentially leading to bursts of traffic.

③ Bucket Overflow :- If the rate at which packets arrive exceeds the bucket's capacity to hold them, the bucket overflows, and excess packets are discarded or marked for future processing.

try.c

```c
#include<stdio.h>

struct LeakyBucket {
    int size;
    int rate;
    int content;
};

int add_packet(struct LeakyBucket *b, int size) {
    if (b->content + size <= b->size) {
        b->content += size;
        return 1;
    } else {
        return 0;
    }
}

int process(struct LeakyBucket *b, int interval) {
    int sent = (b->content < b->rate * interval) ? b->content : b->rate * interval;
    b->content -= sent;
    return sent;
}

int main() {
    struct LeakyBucket b = {100, 20, 0};
    int sizes[] = {30, 40, 25, 15};
    for (int i = 0; i < sizeof(sizes) / sizeof(sizes[0]); ++i) {
        if (add_packet(&b, sizes[i])) {
            printf("Packet %d added.\n", sizes[i]);
        } else {
            printf("Packet %d dropped.\n", sizes[i]);
        }
    }
    int interval = 5;
    int sent = process(&b, interval);
    printf("Sent %d packets in %d seconds.\n", sent, interval);
    return 0;
}
```

```
computer@computer-desktop: ~/Documents
(base) computer@computer-desktop:~/Documents$ gcc try.c
(base) computer@computer-desktop:~/Documents$ ./a.out
Packet 30 added.
Packet 40 added.
Packet 25 added.
Packet 15 dropped.
Sent 95 packets in 5 seconds.
(base) computer@computer-desktop:~/Documents$
```

Date :

④ Leaking :- At regular intervals or ticks, the bucket "leaks" data at a controlled rate. This ensures that the average rate of data leaving the bucket does not exceed a predefined threshold, preventing network congestion.

⑤ Congestion Control: By regulating the rate at which data is transmitted, the Leaky Bucket algorithm helps manage network traffic and prevents congestion by smoothing out burst of incoming packets.

Algorithm:

1. Initialize a counter to n at the tick of the clock.
2. Repeat until n is smaller than the packet size of the packet at the head of the queue.
   1. Pop a packet out of the head of the queue, say P.
   2. Send the packet P, into the network.
   3. Decrement the counter by the size of packet P.
3. Reset the counter and go to step 1.

Result :- Hence a program for congestion control using leaky bucket algorithm are executed successfully

Bjull 15/04/24

Date :

Practical No. 09

Aim :- Configure and implementation of routers within network using packet tracer.

Theory :-

(1) Routers : (1) A Router is a networking devices that forwards data packets between computer networks. It operates at the network layer (layer 3) of the OSI model.

(2) Routers use routing tables to determine the best path for forwarding packets to their destination based on the destination IP address.

(3) They connect different network segments or subnets and enables communication between devices on different Network.

2] Basic Components of a Routers :

(1) Interfaces : Routers have multiple interface (ports) to connects to different networks. Each interfaces typically corresponds to a different network segment or subnet.

(2) Routing tables : This table contains information about known networks and the best paths to reach them. It helps the Router make forwarding decisions.

(3) Routing Protocols : Routers use routing protocols to exchange routing information with other routers and dynamically update their routing tables.
Ex. RIP, OSPF, EIGRP (Enhanced Interior Gateway Routing Protocol)

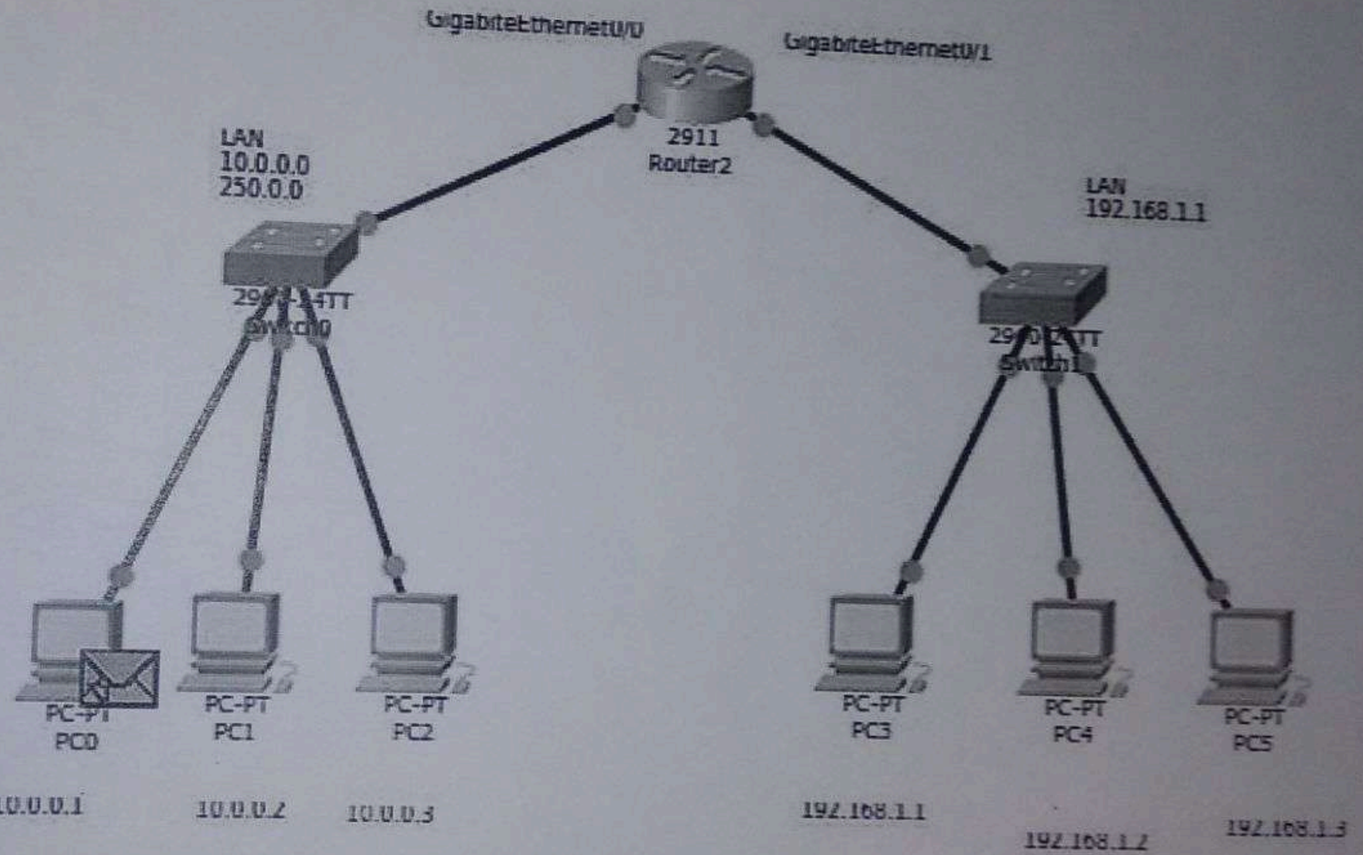
[Root]

New Cluster

Move Object

Set Tiled Background

Viewport



Time: 01:28:03.404

Power Cycle Devices

PLAY CONTROLS:

Back

Auto Capture / Play

Event List

Simulatio

Connections

Scenario 0

New

Delete

Toggle PDU List Window

Fire

Last Status

Source

Destination

Date :

3] Configuring a Router in Packet Tracer:
① Open Packet Tracer and add a router to your network topology from the device palette.
② connect the router's interfaces to the appropriate network segments or subnets by dragging connect. The router's interfaces to the appropriate network segments or subnets by dragging connections between them.
③ Access the router's command-line interface (CLI) by clicking on it and selecting "CLI" from the options.

4] Verifying and Testing:
① After configuring the router, verify connectivity between devices on different networks/subnets using Packet Tracer's simulation mode.
② Use commands such as 'ping' or 'traceroute' on devices connected to the network to test connectivity and verify that packets are being routed correctly by the router.

Result:- Hence a configuring and implementation of router within network using Packet Tracer are successfully.

Page No. 21

Date :

Practical No. 10

Aim :- Implementation of Distance Vector Protocol.

Theory :-

Implementing a Distance Vector Routing Protocol involves creating a network of Routers that exchange routing information to determine the best paths to each different destinations. One of the most well-known distances vector routing protocols is the Routing information protocols (RIP).

1] Understanding Distance Vector Routing :

(1) Distance vector routing protocols, also known as distributed algorithms, calculate the best path to a destination based on distance metrics. (typically hop count) and exchange routing information with neighbouring routers.

(2) Each router maintains a routing tables that lists known destinations and the number of hops required to reach them.

(3) Periodically, routers broadcast their routing tables to neighbouring routers, and based on received information they update their own routing tables accordingly.

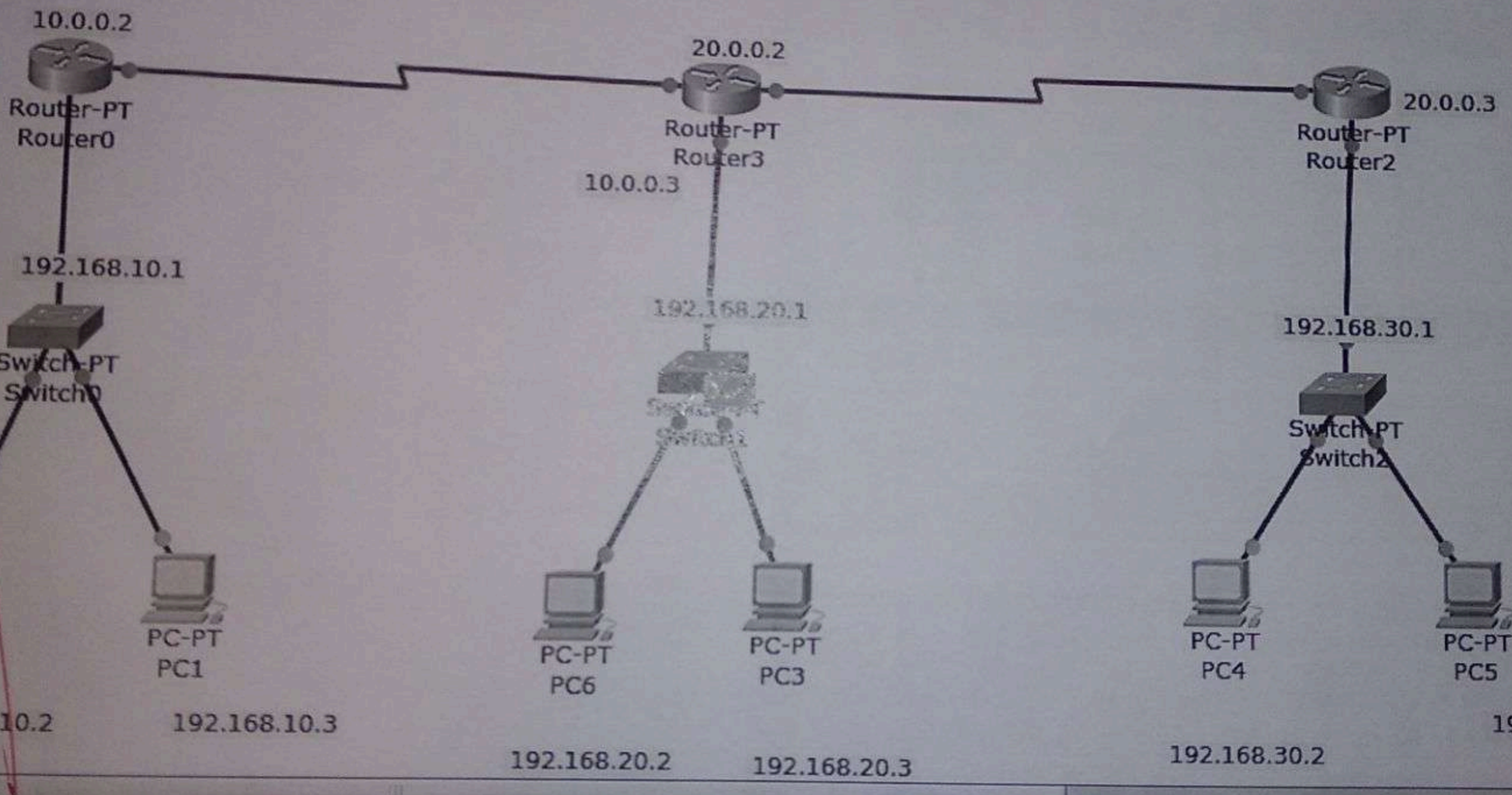
2] Basic components of a Distance Vector Routing Protocol:

(1) Routing Table : Each router maintains a routing table that includes entries for known destinations, next-hop routers, and metrices to reach those destinations.

packettracer6

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport



Time: 01:08:07.567 Power Cycle Devices PLAY CONTROLS: Back Capture / Forward Event List Simu

Connections

Automatically Choose Connection Type

Scenario 0 New Delete

Fire | Last Status | Source | Destination | Type | Color | Time(se

Successful PC0 PC0 ICMP 0.000

Simulation Panel

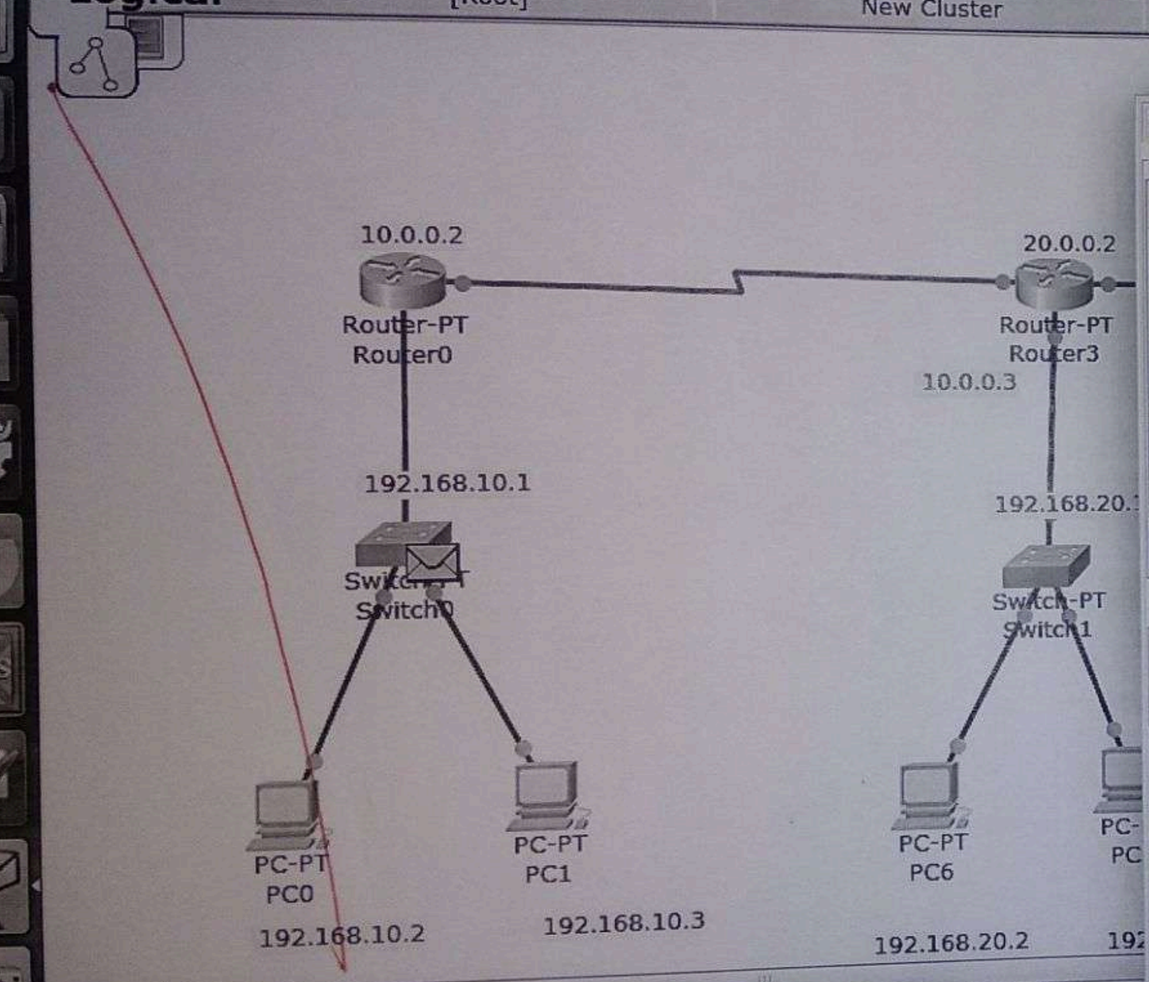
Event List

packettracer6

File Edit Options View Tools Extensions Help

12:38 PM

Logical [Root] New Cluster Move Object Set Tiled Background Viewport



Simulation Panel

Event List

Vis.	Time(sec)	Last Dev	At Devi	Type	Info
	3.406	--	Switc...	STP	
	3.407	Switch2	PC4	STP	
	3.407	Switch2	PC5	STP	
	3.407	Switch2	Rout...	STP	
	3.888	--	Switc...	STP	
	3.889	Switch1	PC6	STP	
	3.889	Switch1	PC3	STP	
	3.889	Switch1	Rout...	STP	
	4.308	--	Switc...	STP	

Reset Simulation | Constant Delay | Capturing...

Play Controls

Back | Auto Capture / Play | Capture / Forward

Event List Filters - Visible Events

ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Edit Filters | Show All/None

Time: 01:08:07.568 Power Cycle Devices PLAY CONTROLS: Back

Connections

Automatically Choose Connection Type

Scenario 0

New | Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC0	PC0	ICMP		0.000	N
	Successful	PC0	PC0	ICMP		0.000	N
	Successful	PC0	PC0	ICMP		0.000	N

Date :

(3) Routing updates : Routers periodically exchange routing updates with neighbouring routers to share information about known destinations and their associated metrices.

(4) Bellman-Ford Algorithm : Distance vector routing protocol is typically use the Baellman-Ford algorithm to calculate the shortest paths to reach destinations based on received routing information

3] Implementation steps :
(1) Topology Design
(2) Router Configuration
(3) Routing Updates
(4) Metric Calculation
(5) Convergence
(6) Monitoring and Verification.

4] Additional Considerations :
(1) Timers
(2) Split Horizon
(3) Route Poisoning

Result :- Hence a implementation of Distance Vector Routing Protocol are successfully.

15/04/24