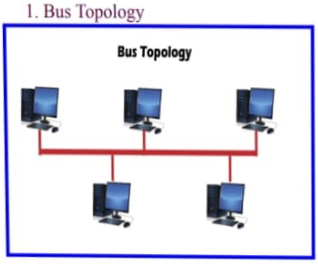
Experiment No: 2

Aim: To configure different network topologies using Cisco Packet Tracer

Software used: Cisco Packet Tracer

Theory:
Different Network Topologies are explained as

1. Bus Topology

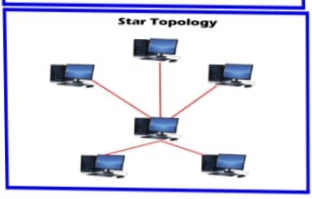


A ***Bus network topology*** supports a common transmission medium where each node is directly connected with the main network cable.
The data is transmitted through the main network cable and is received by all nodes simultaneously.
A signal is generated through the source machine, which contains the address of the receiving machine. The signal travels in both the directions to all the nodes connected to the bus network until it reaches the destination node.
Bus topology is not fault-tolerant and has a limited cable length

A ***Ring topology*** is a modified version of bus topology where every node is connected in a closed-loop forming peer-to-peer LAN topology.

Every node in a ring topology has precisely two connections. The Adjacent node pairs are connected directly, whereas the non-adjacent nodes are indirectly connected via various nodes.

Ring topology supports a unidirectional communication pattern where sending and receiving of data occurs via **TOKEN.**

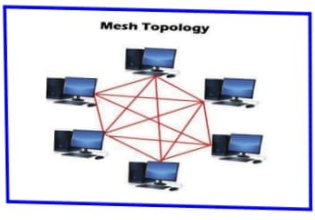


In a ***Star network topology,*** every node is connected using a single central hub or switch.

The hub or switch performs the entire centralized administration. Each node sends its data to the hub, and later hub shares the received information to the destination device.

Two or more-star topologies can be connected to each other with the help of a repeater.

Lokmanya Tilak Jankalyan Shikshan Sanstha's
LOKMANYA TILAK COLLEGE OF ENGINEERING
Navi Mumbai, Maharashtra (INDIA)



In a ***Mesh topology,*** every node in the network connection is directly connected to one another forming overlapping connections between the nodes.

This topology delivers better fault tolerance because if any network device fails, it won't affect the network, as other devices can transfer information.

The Mesh networks self-configure and self-organize, finding the quickest, most secure way to transmit the data

Procedure:

1. Design the Topology by placing Switches and PCs in work space
2. Make Connections
3. Then assign IP and Default gateway address to each PCs
4. Place the packet at sender and receiver PCs to check link is connected
5. Use Simulation to see hope by hope deliver of such packet flow with Protocol used
6. Repeat procedure from step 1 to 5 for other topology

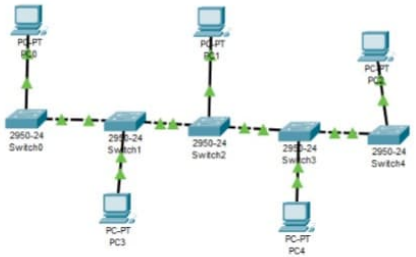
Results: Take the image of each topology, identify the protocol used

Conclusion:

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp2-1.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1734, y: 347 Root 00:49:30



Time: 00:01:38 Realtime Simulation

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841

1841

Scenario 1 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	PC0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC4	ICMP		0.000	N	2	(edit)	(delete)

Temps to plum... Thursday

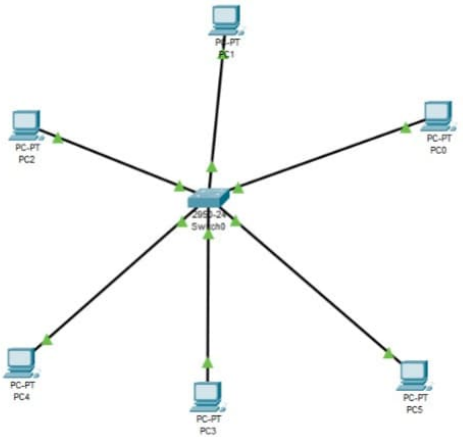
Search

ENG IN 05:59 PM 22-04-2025

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp2-2.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 314, y: 249 Root 00:31:30



Time: 00:01:03 Realtime Simulation

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620

1841

Scenario 1 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	PC5	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC4	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	PC4	ICMP		0.000	N	3	(edit)	(delete)

Activate Windows
Go to Settings to activate Windows.

Air: Severe Today

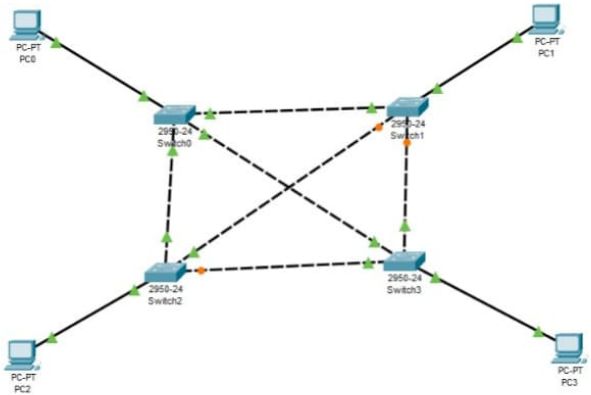
Search

ENG IN 06:01 PM 22-04-2025

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp2-3.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1643, y: 174 Root 02:24:30



Time: 00:04:47 Realtime Simulation

2620XM

Scenario 1 New Delete Toggle PDU List Window

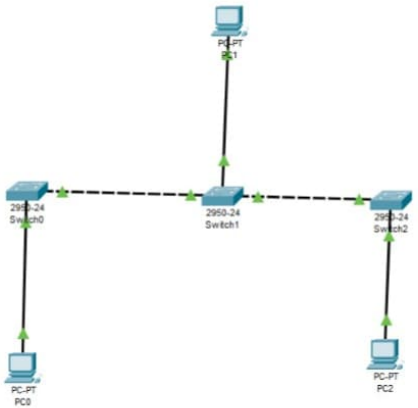
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC0	ICMP		0.000	N	3	(edit)	(delete)

33°C Smoke Search ENG IN 06:06 PM 22-04-2025

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp2-4.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 509, y: 139 Root 00:58:00



Time: 00:01:55 Realtime Simulation

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841

Router-PT-Empty

Scenario 1 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC2	ICMP		0.000	N	2	(edit)	(delete)

33°C Smoke

Search

ENG IN 06:08 PM 22-04-2025

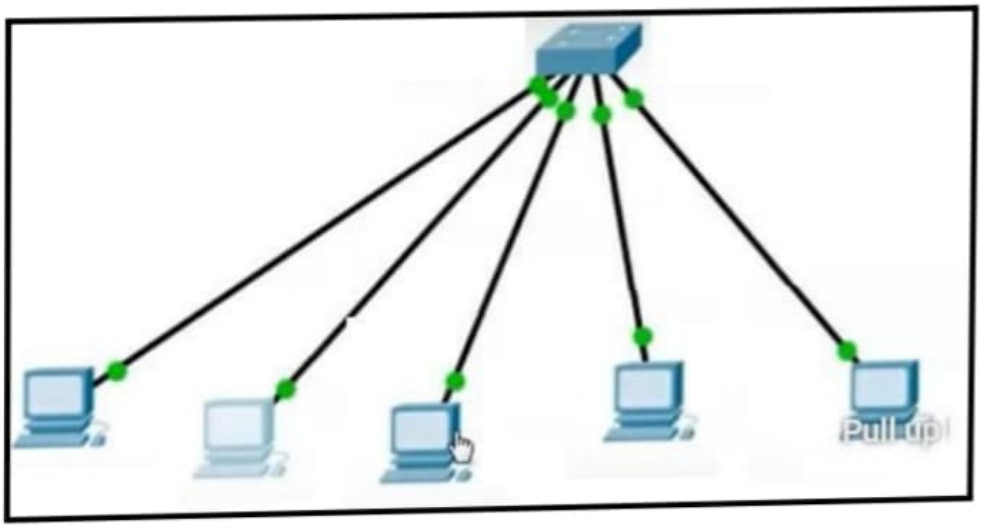
Experiment No: 3

Aim: To configure a basic network using Cisco Packet Tracer.

Software used: Cisco Packet Tracer

Theory:

Establish the basic network as shown in figure and verify the packet flow to understand the basics of network



Procedure:

Step 1: Choose End Devices.
Step 2: Select Network
Device.
Step 3: Establish Communication Links.
Step 4: Configure IP Address of Each End Device.
Step 5: Transfer Packet from one device to another device and check its flow
Step 6 : Repeat above procedure to verify packet flow from each end device to all other end devices are going successfully

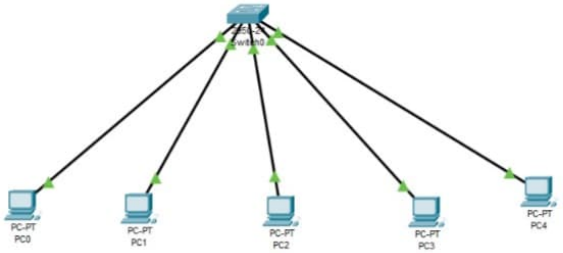
Result: Verify the flow of packets among various end device as well as the protocol

Conclusion:

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp3.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 8, y: 665 Root 03:51:30



Time: 00:07:40 Realtime Simulation

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841

829

Scenario 1 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC4	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2	PC0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC4	PC3	ICMP		0.000	N	3	(edit)	(delete)

Activate Windows
Go to Settings to activate Windows.

33°C Smoke Search ENG IN 06:16 PM 22-04-2025

Experiment No: 4

Aim: To Configure Router using Cisco Packet Tracer.

Software used: Cisco Packet Tracer

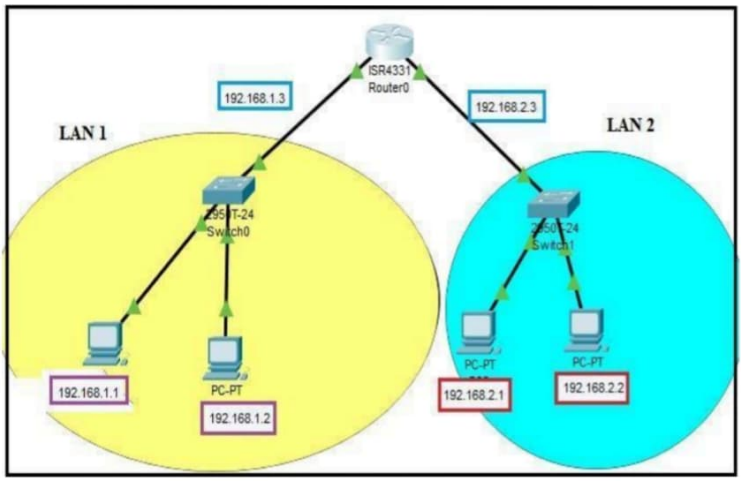
Theory:

To **configure a router** following a network scenario having one router, two switches and four PCs. Give the IP and Gateway address as mentioned. Here two LANs are created. LAN1 and LAN2 consist of PC0, PC1 and Switch 0 and PC2, PC3 and Switch 1 respectively.

For LAN 1, Use the IP address as 192.168.1.1 and 192.168.1.2 to PC0 and PC1 with Gateway address as 192.168.1.3 for both PCs. Gateway address is used for configuring router links connected to port 0/1.

For LAN 2, Use the IP address as 192.168.2.1 and 192.168.2.2 to PC0 and PC1 with Gateway address as 192.168.2.3 for both PCs. Gateway address is used for configuring router links connected to port 0/2.

Configure the router with the gateways assigned to respective LANs.



Procedure:

1. Select 1 Router, 02 switches and 04 PCs
2. Place them in the work space of CPT.
3. Make appropriate connections with Fast Ethernet port of PCs respectively
4. Assign the IP and Gateway Address to PCs respectively
5. Now configure Router with appropriate Gateway address as IP for particular connection
6. Now wait for color to change to Green for all connections.
7. Now verify LAN by passing the packets among PCs in it.
8. Now pass the Packet from each PCs to Router to check connectivity
9. Finally pass packet form one PC of LAN1 to other PC from LAN2

Result:

If packets are successfully reaching in above process, Router configuration is done successfully

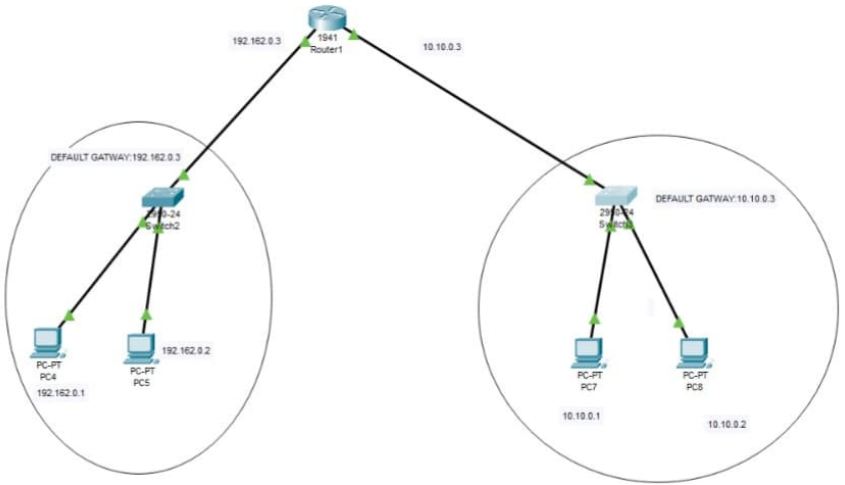
Take the screenshot of Step 9 in CPT with simulation window open to understand the sequence of hop the packet travels with the particular protocol used.

Conclusion:

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp4.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1694, y: 587 Root 07:33:00



Time: 00:14:58 Realtime Simulation

2620XM

Scenario 5 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC5	PC7	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC4	Router1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC7	PC8	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC5	PC4	ICMP		0.000	N	4	(edit)	(delete)

33°C Smoke Search ENG IN 06:32 PM 22-04-2025

Experiment No: 5

Aim: To configure a network with Distance Vector Routing Protocol-RIP using Cisco Packet Tracer

Software Used: Cisco packet tracer

Theory:

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

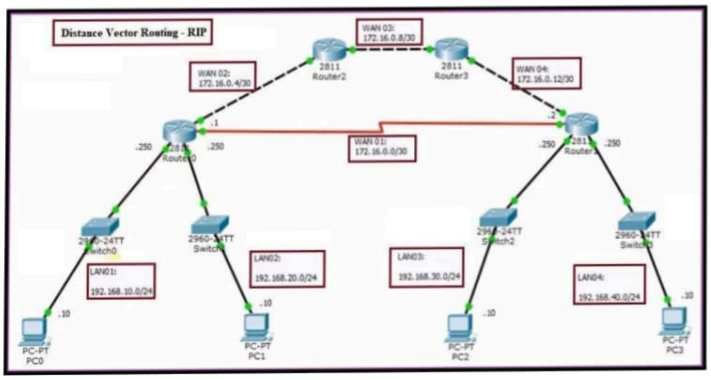
Hop Count

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Features of RIP

1.Updates of the network are exchanged periodically.
2.Updates (routing information) are always
broadcast. 3.Full routing tables are sent in updates.
4. Routers always trust routing information received from neighbor router

Create the following network in CPT to understand RIP



Lokmanya Tilak Jankalyan Shikshan Sanstha's
LOKMANYA TILAK COLLEGE OF ENGINEERING
Navi Mumbai, Maharashtra (INDIA)

Procedure:

Establish the scenario shown in above figure in workspace of CPT

1. Select 4 Router, 04 switches and 04 PCs
2. Place them in the work space of CPT.
3. Make appropriate connections with Fast Ethernet port of PCs respectively
4. Assign the IP and Gateway Address to PCs respectively
5. Now configure Router with appropriate Gateway address as IP for particular connection
6. Now wait for color to change to Green for all connections.
7. Now verify LAN by passing the packets among PCs in it.
8. Now pass the Packet from each PCs to Router to check connectivity
9. Finally pass packet from one PC of LAN1 to other PC from LAN2
10. Check the packet flow path at Router with two paths available

Result:

If packets are successfully reaching end to end device with the defined path by router then RIP is verified y

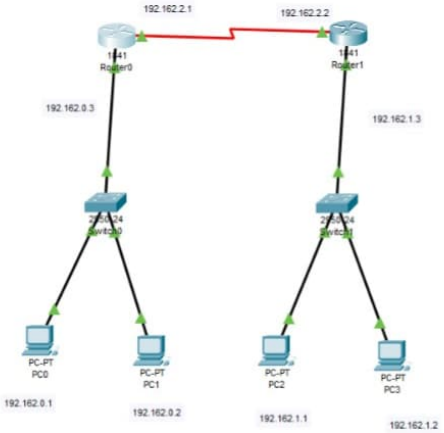
Take the screenshot of Step 9 in CPT with simulation window open to understand the sequence of hop the packet travels with the particular protocol used.

Conclusion:

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\CCNEXP5.1.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1280, y: 10 Root 01:30:30



Time: 00:02:59 Realtime Simulation

Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	--	PC0	PC2	ICMP		0.000	N	0	(edit)	(delete)

31°C Smoke

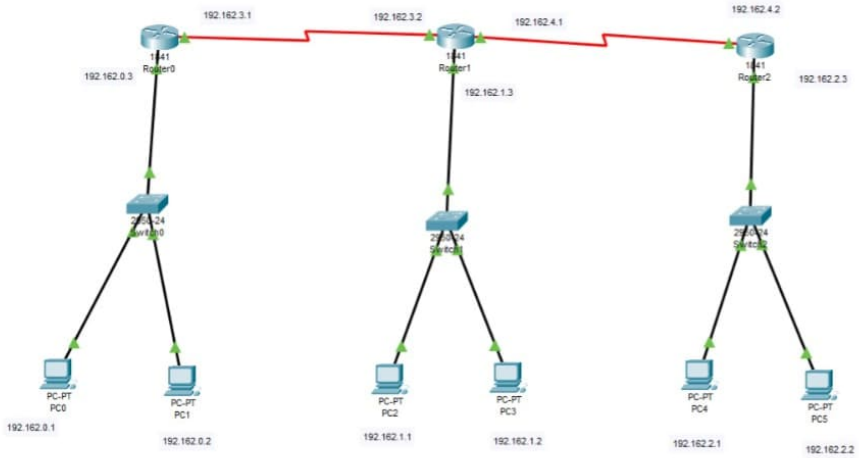
Search

ENG IN 11:21 PM 22-04-2025

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp5.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 130, y: 120 Root 00:48:00



Time: 00:01:34 Realtime Simulation

Router-PT

Scenario 3 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	Router0	ICMP		0.000	N	2	(edit)	(delete)

33°C Smoke Search ENG IN 06:34 PM 22-04-2025

Experiment No: 6

Aim: To configure a network with Path Vector Routing Protocol- BGP using Cisco Packet Tracer

Software Used: Cisco Packet Tracer

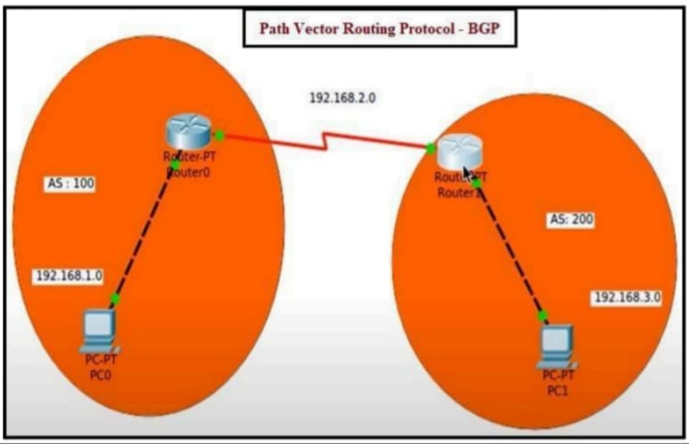
Theory:

A path-vector routing protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates that have looped through the network and returned to the same node are easily detected and discarded. This algorithm is sometimes used in Bellman–Ford routing algorithms to avoid "Count to Infinity" problems.

It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.

Border Gateway Protocol (BGP) is an example of a path vector protocol. In BGP, the autonomous system boundary routers (ASBR) send path-vector messages to advertise the reachability of networks. Each router that receives a path vector message must verify the advertised path according to its policy. If the message complies with its policy, the router modifies its routing table and the message before sending the message to the next neighbor. It modifies the routing table to maintain the autonomous systems that are traversed in order to reach the destination system. It modifies the message to add its AS number and to replace the next router entry with its identification.

Illustration of Path Vector Routing Protocol – BGP



Procedure:

Establish the scenario shown in above figure in workspace of CPT

1. Select 2 Routers and 02 PCs
2. Place them in the work space of CPT.
3. Make appropriate connections with Fast Ethernet port of PCs respectively
4. Assign the IP and Gateway Address to PCs respectively
5. Now configure Router with appropriate Gateway address as IP for particular connection
6. Now wait for color to change to Green for all connections.
7. Now pass the Packet from each PCs to Router to check connectivity
8. Finally pass packet from one PC of AS to other PC of another AS

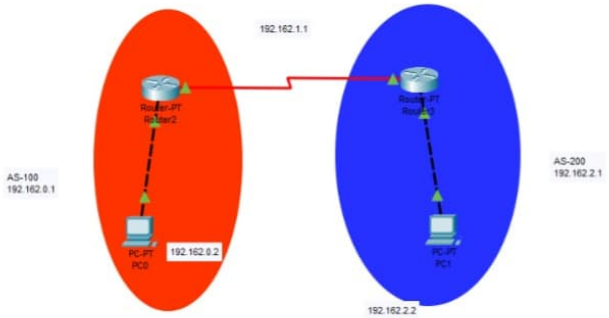
Result:

Conclusion:

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp6.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1703, y: 597 Root 00:48:00



Time: 00:01:36 Realtime Simulation

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841

ISR4331

Scenario 2 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Router2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	Router3	ICMP		0.000	N	1	(edit)	(delete)

33°C Smoke Search ENG IN 06:36 PM 22-04-2025

Experiment No: 8

Aim: To create a wired network and compare the performance of TCP and UDP using NS2

Software Used: Cisco Packet Tracer

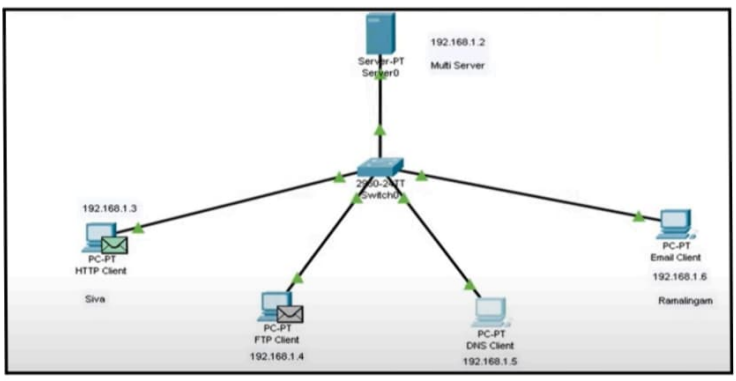
Theory:

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

1. TCP: TCP (Transmission Control Protocol) is a connection-oriented protocol designed to facilitate reliable and ordered delivery of data between applications. It establishes a connection before transmitting data, employing features such as flow control, congestion control, and error detection through mechanisms like acknowledgments and retransmissions. TCP headers contain fields for source and destination ports, sequence numbers, acknowledgment numbers, window size for flow control, checksum for error detection, and various control flags.

2. UDP: UDP (User Datagram Protocol) is a connectionless protocol offering a simpler form of communication between applications. Unlike TCP, UDP does not provide reliability or ordering guarantees, making it more lightweight with lower overhead. UDP packets are typically smaller and contain fields for source and destination ports, length, and a checksum for error detection. It lacks features like flow control and congestion control found in TCP.

Illustration of TCP and UDP



Procedure:

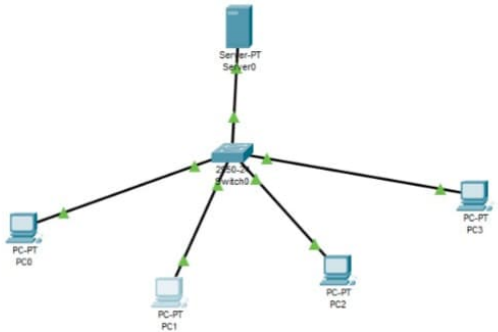
Establish the scenario shown in above figure in workspace of CPT

1. Set up a wired network topology in NS2.
2. Implement TCP protocol in the network.
3. Implement TCP protocol in the network by specifying TCP agents for data transmission and reception.
4. Implement UDP protocol in the network.
5. Implement UDP protocol in the network by specifying UDP agents for data transmission and reception.
6. Configure the network to measure performance metrics for TCP.
7. Configure the network to measure performance metrics for UDP.
8. Run simulations for TCP and record performance results.
9. Run simulations for UDP and record performance results.
10. Analyze and compare the performance metrics obtained for TCP and UDP.

Cisco Packet Tracer - C:\Users\sachi\Cisco Packet Tracer 8.2.2\saves\ccnexp8.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 119, y: 20 Root 00:41:30



Time: 00:49:05 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

Automatically Choose Connection Type

32°C Smoke Search ENG IN 10:51 PM 22-04-2025

Experiment No: 9A

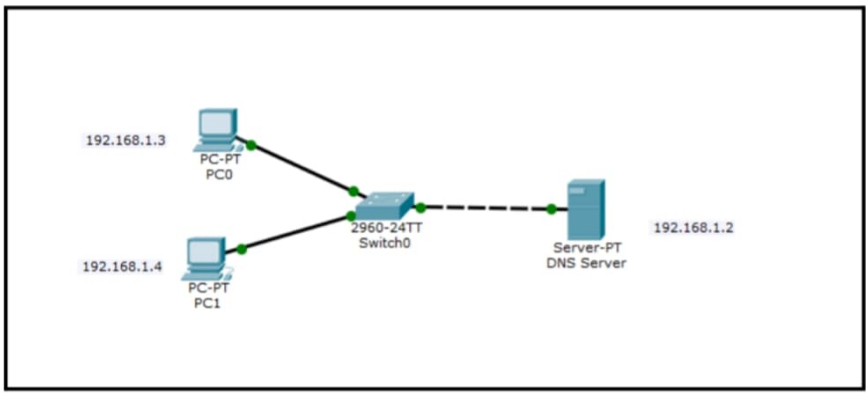
Aim: To configure DNS using Cisco Packet Tracer

Software Used: Cisco Packet Tracer

Theory:

DNS: DNS(Domain Name System) is a fundamental protocol used in computer networks to translate human-readable domain names into IP addresses. It functions as a distributed database system, providing a hierarchical naming structure for resources on the internet. DNS operates through a distributed network of servers, organized in a hierarchical fashion, with each server responsible for resolving domain names within its zone. When a user requests the IP address associated with a domain name, their device sends a DNS query to a DNS resolver, typically provided by their internet service provider (ISP) or configured within the network. The resolver then recursively queries other DNS servers until it finds the authoritative server responsible for the requested domain, returning the corresponding IP address to the user's device.

Illustration of DNS



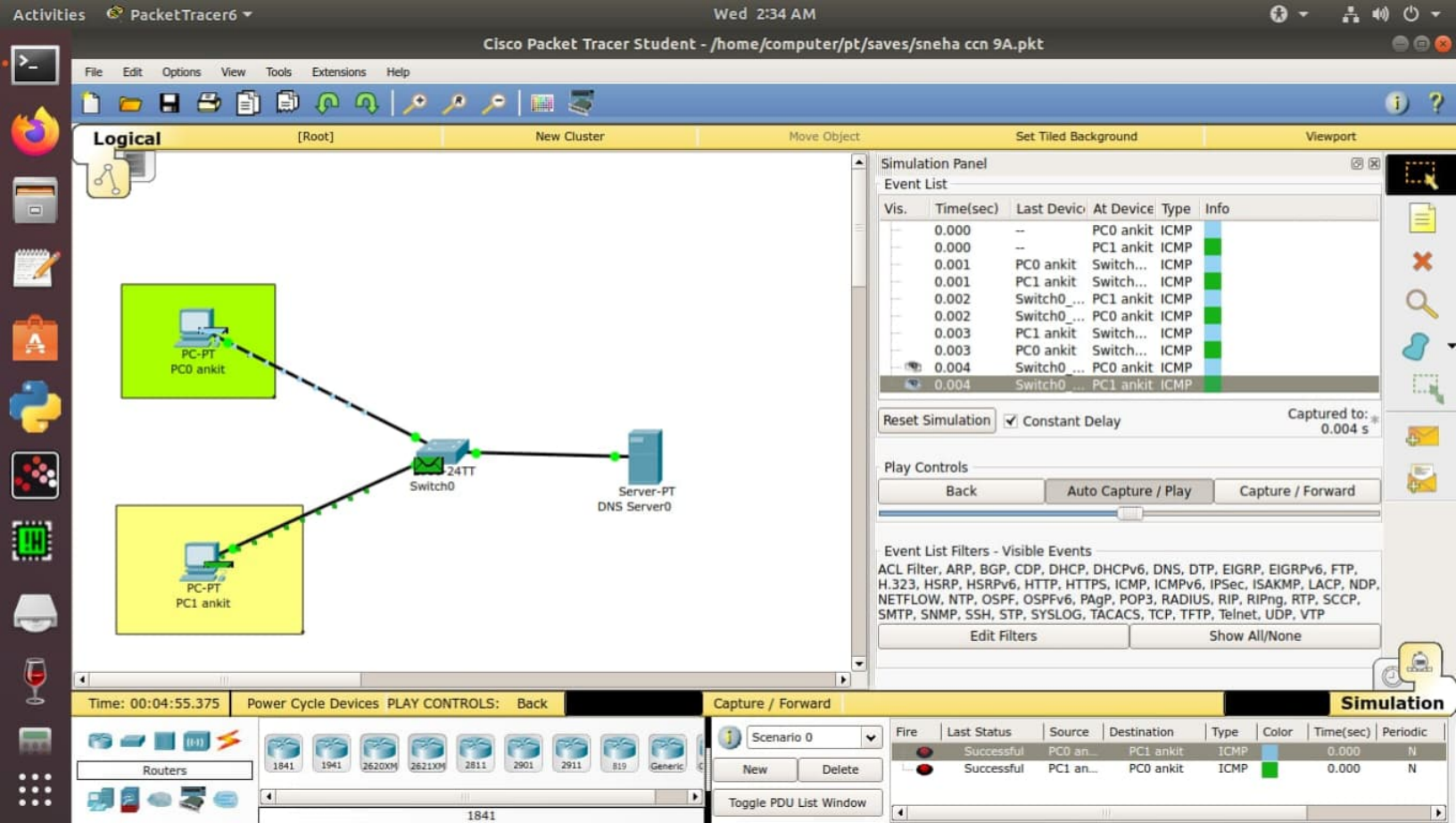
Procedure:

Establish the scenario shown in above figure in workspace of CPT

1. Build the network topology.
2. Configure static IP addresses on the PCs and the server.
3. Configure DNS service on the generic server.
4. Ping the hosts from one another using their names instead of their IP addresses

Result:

Conclusion:


Activities
PacketTracer6
Wed 2:34 AM
Cisco Packet Tracer Student - /home/computer/pt/saves/sneha ccn 9A.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC-PT
PC0 ankit
PC-PT
PC1 ankit
24TT
Switch0
Server-PT
DNS Server0
Simulation Panel
Event List
Vis. Time(sec) Last Devic At Device Type Info
0.000 -- PC0 ankit ICMP
0.000 -- PC1 ankit ICMP
0.001 PC0 ankit Switch... ICMP
0.001 PC1 ankit Switch... ICMP
0.002 Switch0_... PC1 ankit ICMP
0.002 Switch0_... PC0 ankit ICMP
0.003 PC1 ankit Switch... ICMP
0.003 PC0 ankit Switch... ICMP
0.004 Switch0_... PC0 ankit ICMP
0.004 Switch0_... PC1 ankit ICMP
Reset Simulation
Constant Delay
Captured to: 0.004 s
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: 00:04:55.375
Power Cycle Devices
PLAY CONTROLS: Back
Capture / Forward
Simulation
Routers
1841
1941
2620XM
2621XM
2811
2901
2911
819
Generic
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic
Successful PC0 an... PC1 ankit ICMP 0.000 N
Successful PC1 an... PC0 ankit ICMP 0.000 N

Experiment No: 9B

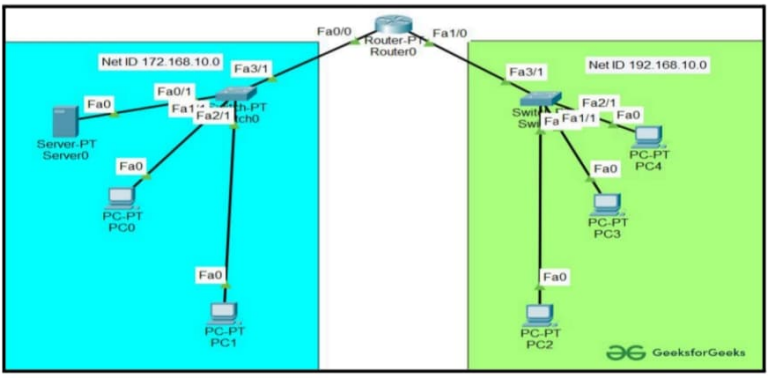
Aim: To configure DHCP using Cisco Packet Tracer

Software Used: Cisco Packet Tracer

Theory:

DHCP(Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign IP addresses and other network configuration parameters to devices on a network. It operates on a client-server model, where DHCP servers lease IP addresses and configuration information to client devices, such as computers, smartphones, and network printers. When a device connects to a network, it sends out a DHCP discover message, broadcasted to locate DHCP servers. DHCP servers respond with DHCP offer messages containing lease information, including the IP address and network configuration settings. The client selects an offer and sends a DHCP request message, confirming the lease. Finally, the DHCP server acknowledges the request, and the client configures its network interface with the provided information, allowing seamless network connectivity without manual configuration. DHCP helps streamline network administration by automating IP address management and ensuring efficient resource allocation.

Illustration of DHCP



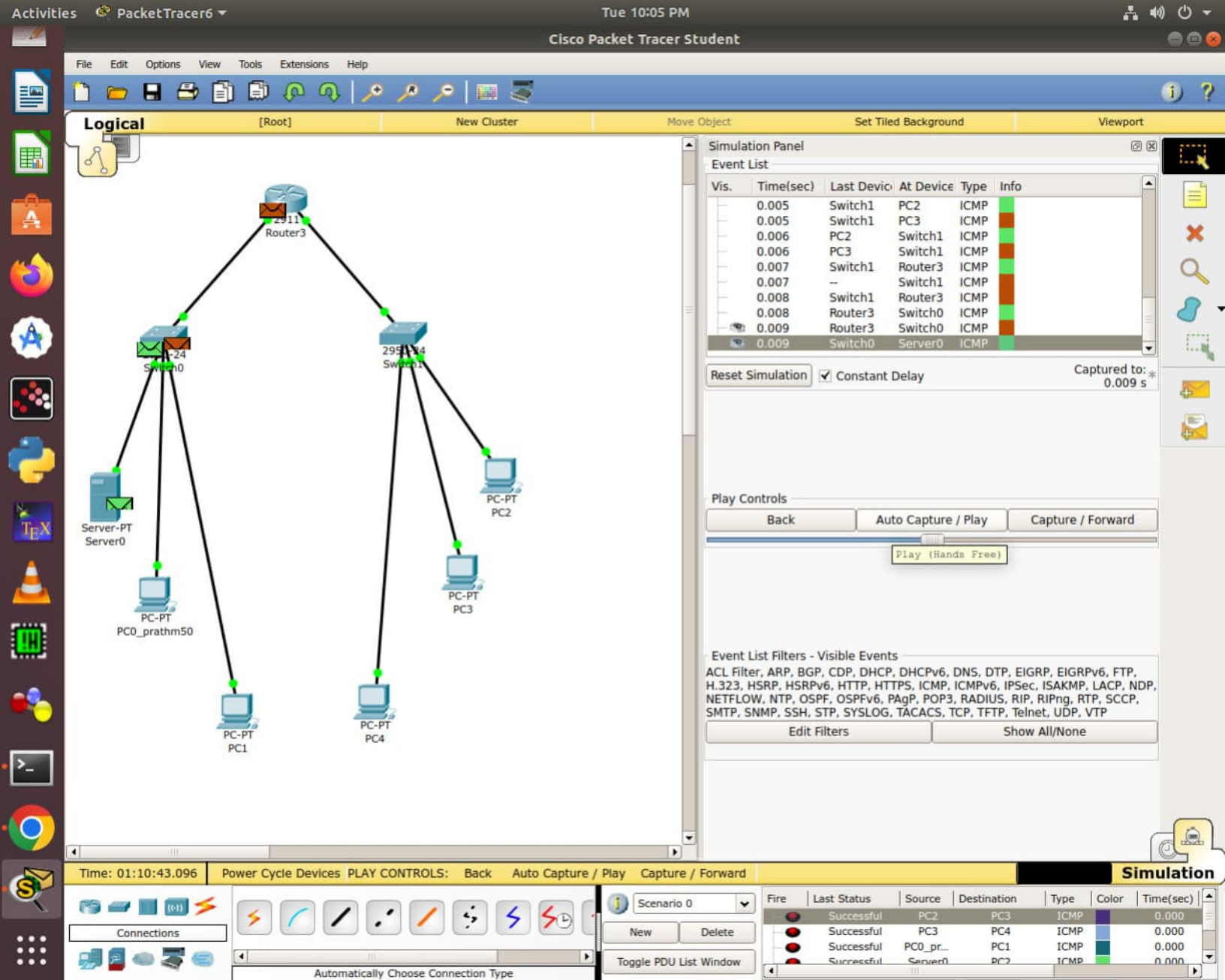
Procedure:

Establish the scenario shown in above figure in workspace of CPT

1. Select 01 Routers, 05 PCs, 01 Server and 02 Switches
2. Create a network topology as shown above in the image.
3. Configure the server with IPV4 addressing and subnet mask
4. Assign IP address using the ipconfig command.
5. Configure the DHCP server.
6. Configure Router with IPv4 Address and Subnet Mask.
7. Configure the PCs and change the IP configuration.

Result:

Conclusion:


Activities
PacketTracer6
Tue 10:05 PM
Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Router3
Switch0
Server-PT Server0
PC-PT PC0_prathm50
PC-PT PC1
PC-PT PC4
PC-PT PC3
PC-PT PC2
Simulation Panel
Event List
Vis. Time(sec) Last Devic At Device Type Info
0.005 Switch1 PC2 ICMP
0.005 Switch1 PC3 ICMP
0.006 PC2 Switch1 ICMP
0.006 PC3 Switch1 ICMP
0.007 Switch1 Router3 ICMP
0.007 -- Switch1 ICMP
0.008 Switch1 Router3 ICMP
0.008 Router3 Switch0 ICMP
0.009 Router3 Switch0 ICMP
0.009 Switch0 Server0 ICMP
Reset Simulation
Constant Delay
Captured to: 0.009 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Play (Hands Free)
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: 01:10:43.096
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)
Successful PC2 PC3 ICMP 0.000
Successful PC3 PC4 ICMP 0.000
Successful PC0_pr... PC1 ICMP 0.000

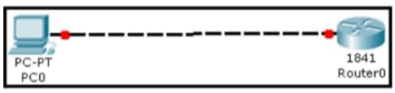
Experiment No: 10A

Aim: To configure TELNET using Cisco Packet Tracer

Software Used: Cisco Packet Tracer

Theory: TELNET, a protocol operating at the application layer of the TCP/IP suite, facilitates bidirectional text-oriented communication between client and server over networks. Unlike path-vector routing protocols such as BGP, Telnet's primary function isn't routing data packets but enabling interactive sessions. However, similarities exist in their communication models and message modification processes. In Telnet, intermediary devices like firewalls may modify or interpret data exchanged between client and server, akin to how routers in BGP adjust routing messages as they propagate. Moreover, both Telnet and path-vector routing protocols involve verification and policy application at intermediary points. For instance, routers in BGP verify advertised paths against policies before adjusting routing tables, while Telnet sessions may be subject to access control lists or authentication mechanisms. Additionally, both systems maintain state information: Telnet sessions track session states and timeouts, while path-vector routing protocols maintain network topology and routing decisions. Thus, while Telnet and path-vector routing protocols differ in their primary functions and OSI layer, they share similarities in communication mechanisms, message modification processes, policy enforcement, and state maintenance.

Illustration of TELNET



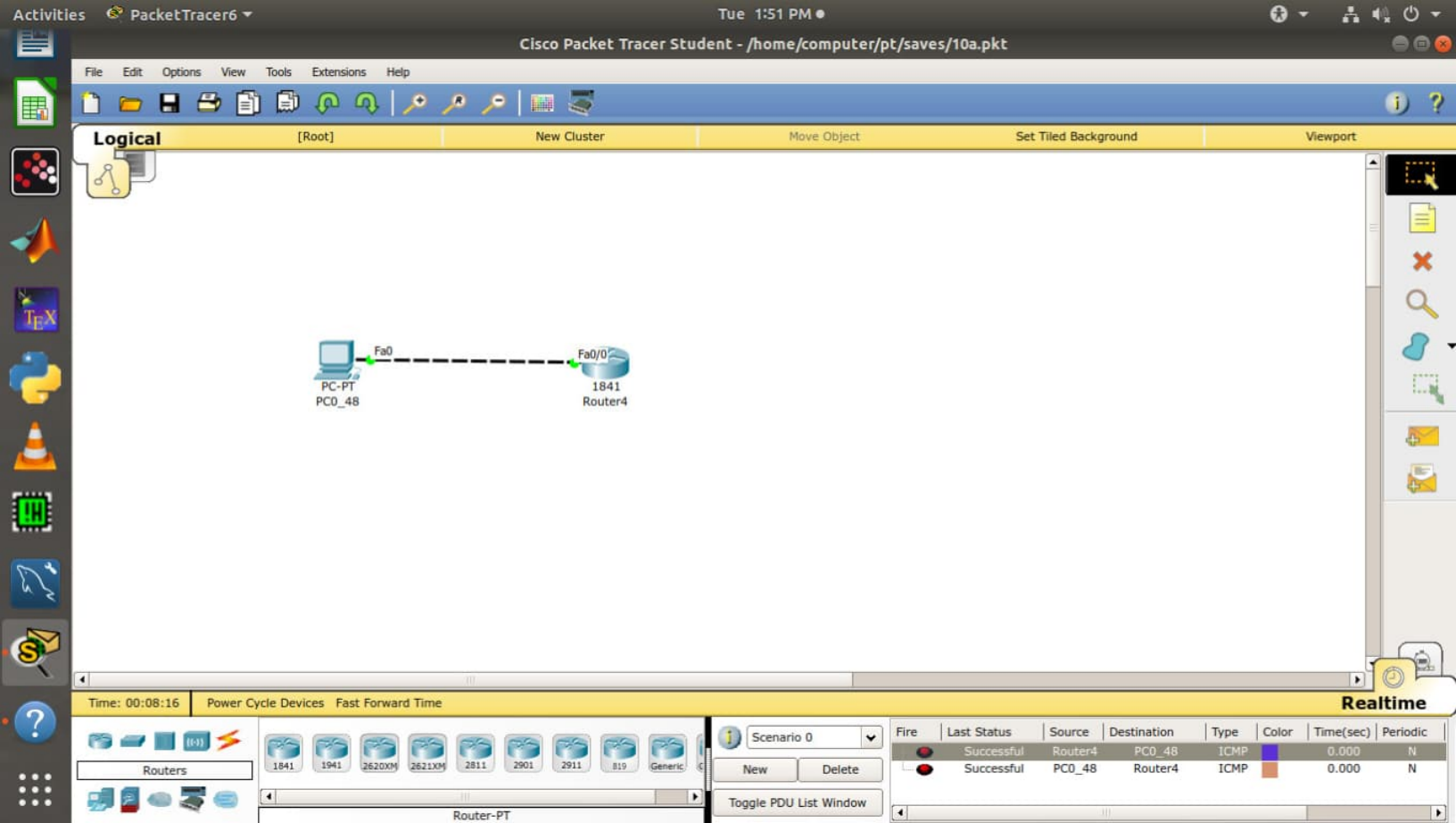
Procedure:

Establish the scenario shown in above figure in workspace of CPT

1. Select 02 PCs
2. Place them in the work space of CPT.
3. Set interface fast Ethernet 0/0 IP address to 192.168.1.1/24
4. Set privileged mode password to Cisco
5. Enable TELNET lines on router
6. Test TELNET connection via your PC

Result:

Conclusion:


Activities
PacketTracer6
Tue 1:51 PM
Cisco Packet Tracer Student - /home/computer/pt/saves/10a.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Fa0
Fa0/0
PC-PT
PC0_48
1841
Router4
Time: 00:08:16
Power Cycle Devices
Fast Forward Time
Realtime
Routers
1841
1941
2620XM
2621XM
2811
2901
2911
819
Generic
Router-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Successful
Router4
PC0_48
ICMP
0.000
N
Successful
PC0_48
Router4
ICMP
0.000
N