Lab 1: Basic Networking Commands

Objective(s): To understand basic networking command using terminal for network configuration, testing and verification.

Theory:

The network infrastructure is a very complex structure of cables, routers, access points, data packets, and a million other small components that together make the entire network work seamlessly. Any issue in any of these smaller components may lead to an overall collapse of the network infrastructure. This may lead to disruption of Wi-Fi, cellular and wired (Ethernet) infrastructure. This is the reason why it's very important to have an access to how the network is performing and know troubleshooting techniques, namely networking commands, which are used at the command prompt to get network information.

Basic Network Commands

IPCONFIG

ipconfig (stands for "Internet Protocol configuration") is a console application program of some computer operating systems that displays al current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. It is also used to release and renew the IP address of a device.

```
C:\Users\Acer>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8ec:955f:4322:6b9%19
   Autoconfiguration IPv4 Address. . : 169.254.0.118
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : worldlink.com.np
   IPv6 Address. . . . . . . . . . . : 2400:1a00:b070:7d00::4
   IPv6 Address. . . . . . . . . . . : 2400:1a00:b070:7d00:da61:7552:7b6:6c91
   Temporary IPv6 Address. . . . . . : 2400:1a00:b070:7d00:b004:6eff:a2ca:3601
   Link-local IPv6 Address . . . . . : fe80::a74a:e7ff:5b1d:b242%20
   IPv4 Address. . . . . . . . . . . : 192.168.1.67
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%20
```

IPCONFIG/ALL

Without the use of any parameter, the command shows only the basic network information. But information about the DNS and DHCP servers isn't displayed by default. To show all the information about your network adapter, you will need to use the / all parameter.

```
C:\Users\Acer>IPCONFIG/ALL

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Admin
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : worldlink.com.np

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-13
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8ec:955f:4322:6b9%19(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.0.118(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 638189607
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-80-A0-43-9C-2F-9D-61-3E-F5
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 9E-2F-9D-61-1E-D5
```

NSLOOKUP

Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system DNS record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address. Network administrators use nslookup to troubleshoot server connections or for security reasons.

```
C:\Users\Acer>NSLOOKUP
Default Server:  vip6-safenet-kmd01.wlink.com.np
Address:  2400:1a00:0:32::165

> www.manjilgautam.com.np
Server:  vip6-safenet-kmd01.wlink.com.np
Address:  2400:1a00:0:32::165

Non-authoritative answer:
Name:    manjilgautam.com.np
Addresses:  2a02:4780:11:772:0:1309:877a:7
          217.21.84.4
Aliases:  www.manjilgautam.com.np
```

PING

The full form of PING is the Packet InterNet Groper. It is computer network management system software or utility software used to test the network communication between two devices. It sends an ICMP request to the destination device and waits for reply. If the destination device is not reachable, it will not reply.

```
C:\Users\Acer>ping youtube.com

Pinging youtube.com [2404:6800:4002:81c::200e] with 32 bytes of data:
Reply from 2404:6800:4002:81c::200e: time=32ms
Reply from 2404:6800:4002:81c::200e: time=34ms
Reply from 2404:6800:4002:81c::200e: time=33ms
Reply from 2404:6800:4002:81c::200e: time=32ms

Ping statistics for 2404:6800:4002:81c::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 34ms, Average = 32ms
```

TRACE ROUTE/TRACERT

The traceroute commands is used to determine the path between two connections. Often a connection to another device will have to go through multiple routers. The traceroute commands will return the names or IP address of all routers between two devices.

```
C:\Users\Acer>tracert 192.168.1.10

Tracing route to 192.168.1.10 over a maximum of 30 hops

  1  Admin.worldlink.com.np [192.168.1.67]  reports: Destination host unreachable.

Trace complete.
```

Conclusion:

Hence, we learnt to use basic network commands to check, diagnose and troubleshoot network and network related problem.

Lab 2: Network Wiring

Objective(s):

a. To understand the color coding standard of UTP cable
b. To create straight and crossover cable and test/verify its connectivity.

Theory:

Network

A network is a group of computers and other devices connected together to share information. Networks can be as small as two computers or as large as billions of devices. The Internet is the world's largest network.

Network Architecture

The way in which the network is designed is called its architecture. The most common network architectures are Ethernet, Token Ring, and FDDI.

Ethernet

Ethernet is the most common network architecture. It is a bus topology that uses CSMA/CD to avoid collisions. Ethernet networks can operate at 10 Mbps, 100 Mbps, 1Gbps, or 10 Gbps.

Network Wiring

Network wiring is the physical wiring of the network. The most common network wiring is twisted pair cable. Twisted pair cable is made up of four pairs of wires. Each pair of wires is twisted together to reduce interference. Twisted pair cable is available in two types: shielded twisted pair (STP) and unshielded twisted pair (UTP). STP has a metal shield around the wires to reduce interference. UTP does not have a metal shield. UTP is the most commonly used network wiring.

Network Wiring Tools

The tools used to wire twisted pair cable are a cable stripper, a cable crimper, and a cable tester. The cable stripper is used to remove the outer jacket from the cable. The cable crimper is used to attach the RJ-45 connectors to the cable. The cable tester is used to test the cable after it is wired.

Network Wiring Standards

The T568A and T568B standards are used to wire twisted pair cable. The T568A standard is used in government installations. The T568B standard si used in most other installations. There are other standards as well for wiring twisted pair cable. The 1568A and 1568B standards are the most common. Likewise, there are other network wiring types and they come with their own standards.

The T568A and T568B standards are shown below:

Procedure:

Step 1: The outer jacket of the cable was carefully stripped using a cable stripper or a sharp blade, ensuring not to cut or damage the inner wires. The jacket was removed to expose the individual wires inside.

Step 2: The pairs of wires were gently untwisted while maintaining the twisted structure as much as possible. This helps reduce crosstalk and interference between the wires, ensuring better signal quality.

Step 3: The wires were arranged in the correct order following the specified color-coding sequence of the chosen wiring standard (eg., T568A or T568B). Each wire was placed in the appropriate position according to the wiring diagram, ensuring proper connectivity.

Step 4: Using wire cutters, the wires were carefully trimmed to the correct length. It was ensured that all the wires were of equal length to avoid any imbalances or excess slack within the cable.

Step 5: The stripped wires were inserted into the corresponding slots of the RJ-45 connector. Each wire was placed in its designated slot according to the wiring diagram, ensuring a precise and accurate connection.

Step 6: With the RJ-45 connector held securely, a suitable crimping tool was used to crimp the connector onto the cable. Sufficient pressure was applied to create a strong and reliable connection, ensuring that the wires were securely held in place by the connector's contacts.

Step 7: Finally, the cable was tested for proper connectivity and functionality. This involved using a cable tester or connecting the cable between appropriate devices to verify that data could be successfully transmitted and received without any issues or errors.

Conclusion:

Hence, we learned how to clamp a network wire and also tested whether the connection is functional.

Lab 3: Introduction to packet tracer and basic LAN setup.

Objective(s): To Understand and implement basic LAN setup using cisco packet tracer

Theory:

Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. it allows users to create virtual network topologies and simulate the behavior of network devices such as routers, switches, hubs, and computers. With a user-friendly interface, users can design, configure, and troubleshoot networks without physical hardware. It offers hands-on experience in networking concepts, supports real-time traffic simulation, and provides learning materials for networking skills development. Packet Tracer is an invaluable tool for network engineers, students, and anyone interested in practicing and exploring network design and configurations in a virtual environment.

LAN (Local Area Network) is a data communication network that locally connects network devices such as workstations, servers, routers, etc. to share the resources within a small area such as a building or campus. Physical or wireless connections are set up between workstations to share the resources. Ethernet and Wi-Fi are the most important technologies of LAN.

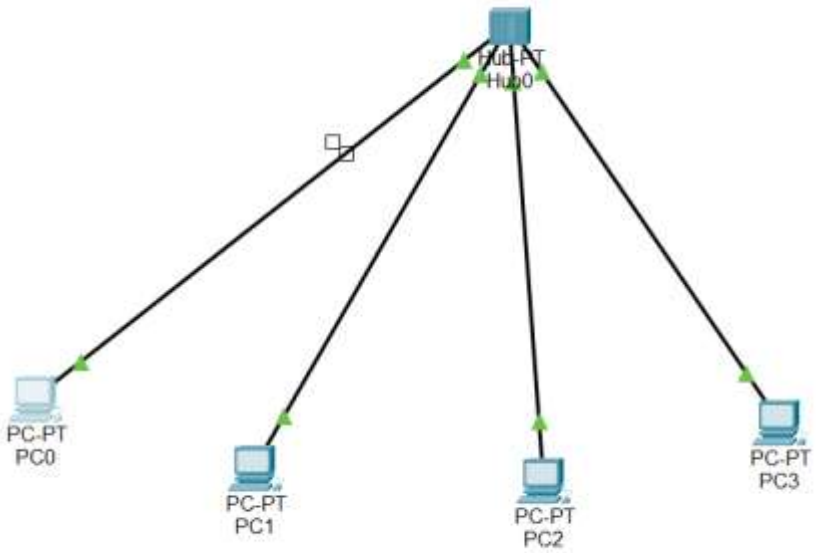
Procedure:

Step 1: Launch Cisco Packet Tracer to begin the network setup.

Step 2: Navigate to the "Devices" pane and expand the "Network Devices" category and drag a hub onto the workspace area.

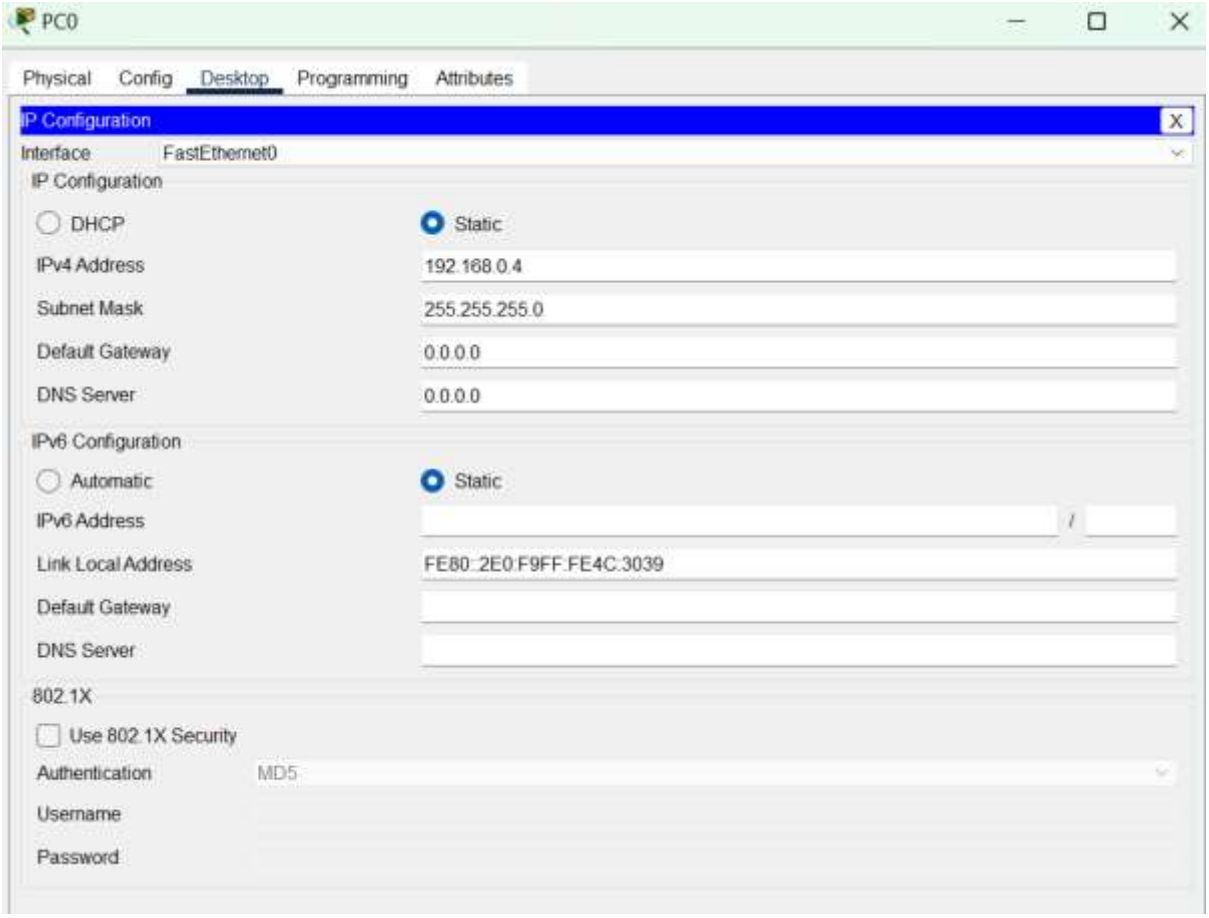
Step 3: Now switch to the "End Devices" pane, and drag some PCs onto the workspace near the hub.

Step 4: As we are connecting two different devices hub and computers we use ""Copper Straight-through" cable from connection pane. And connect the computers Ethernet port to respective port in the hub.



Step 5: Proceed to configure IP addresses and other settings on the PCs if required.

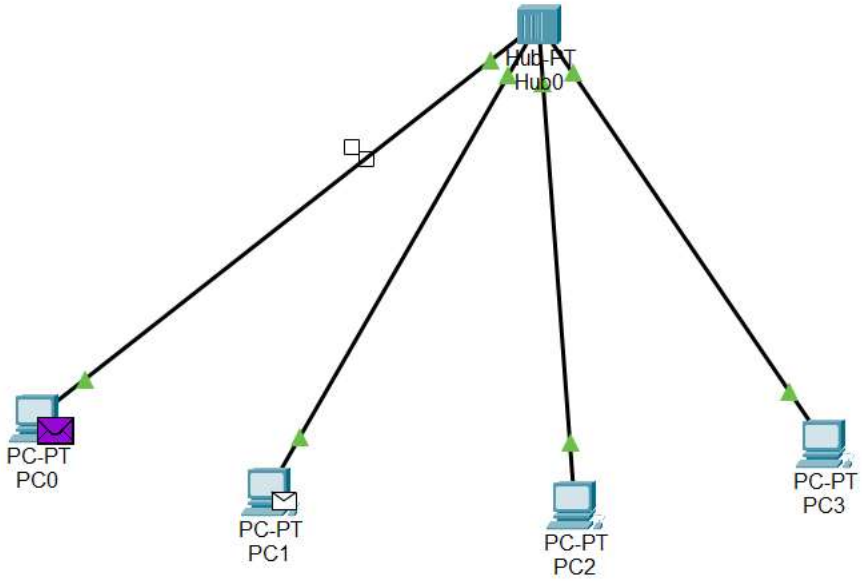
a. Click on the “Desktop” tab of PC0
b. Click on the “IP configuration” icon.
c. Enter the IP address and Subnet mask
d. After done, close the configuration window.
e. Repeat this for other PCs as well if required.



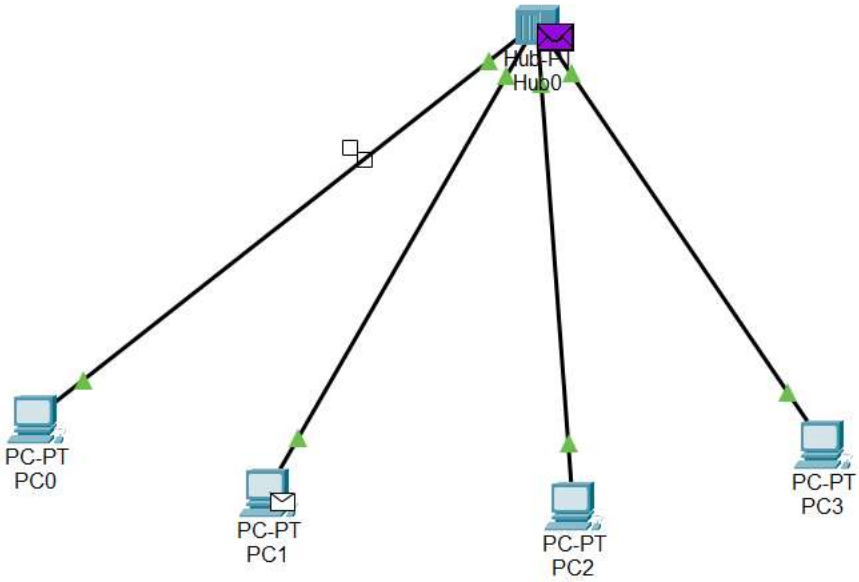
Step 6: Now, test the connection

a. Click on the “Add Simple PDU” icon in toolbar.
b. Click on PC0 and then click on PC1.
c. A packet is sent from PC0 to PC1.

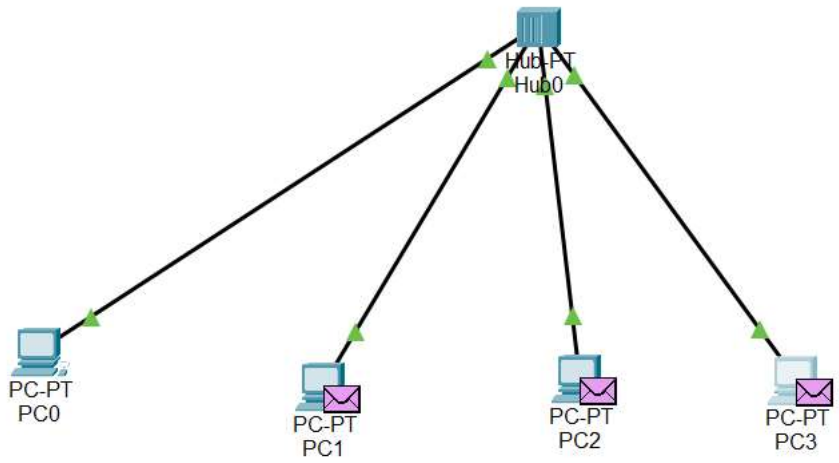
Output



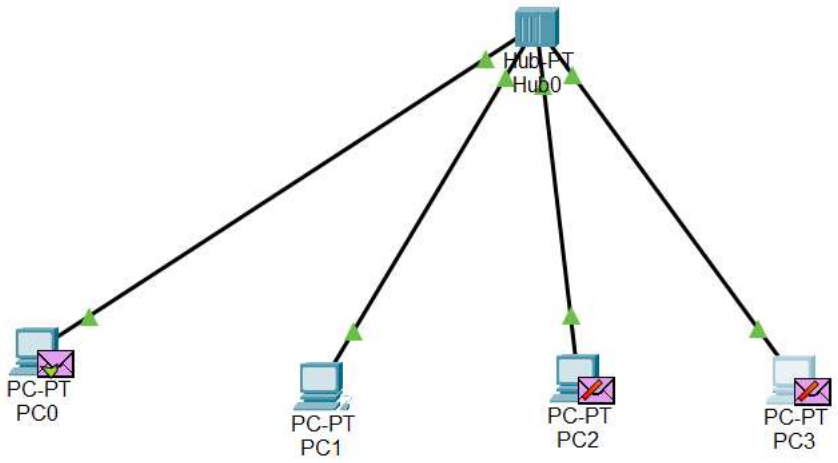
(packet sent from PC0 to hub)



(packet received by hub)



(packet distributed to all ports except PC0 and accepted by PC1 only)



(Acknowledgement from PC1 to PC0 about received packet)

Conclusion

In this way, we can implement basic LAN setup using the networking device hub and observe the router that a packet takes to reach to its destination.

Lab 4: DHCP, DNS and Web server setup

Objective(s): To Understand the Working Principle of DHCP, WEB server, DNS using cisco packet tracer

Theory:

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients. A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic PI address, which changes when the client's lease for that IP address has expired.

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP

addresses so browsers can load Internet resources. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:b00:2048:1::629:d7a2 (in IPv6).

A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job

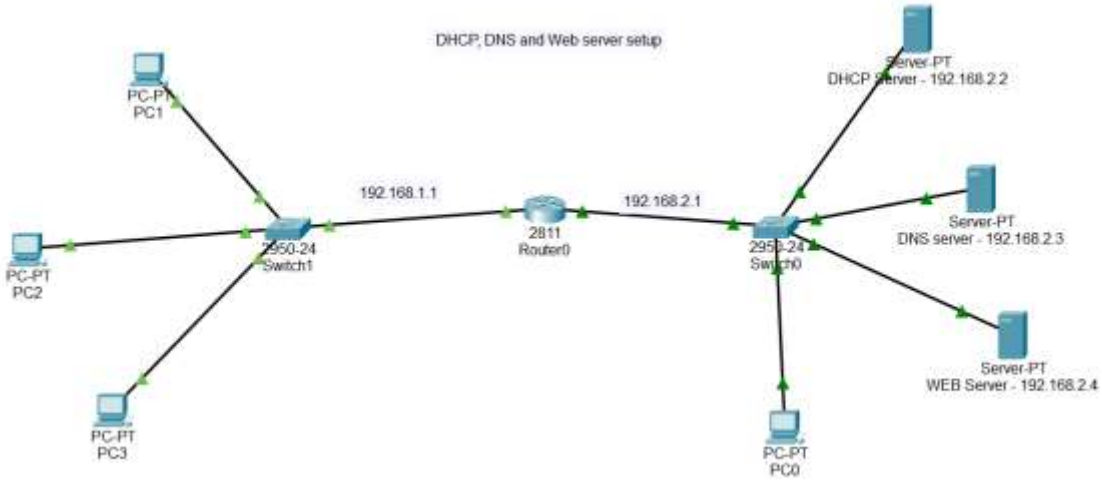
of a web server is to display website content through storing, processing and delivering webpages to users. Besides HTTP, web servers also support SMTP (Simple Mail Transfer Protocol) and FTP (File Transfer Protocol), used for email, file transfer and storage. Web server hardware is connected to the internet and allows data to be exchanged with other connected devices, while web server software controls how a user accesses hosted files.

The web server process is an example of the client/server model. Al computers that host websites must have web server software.

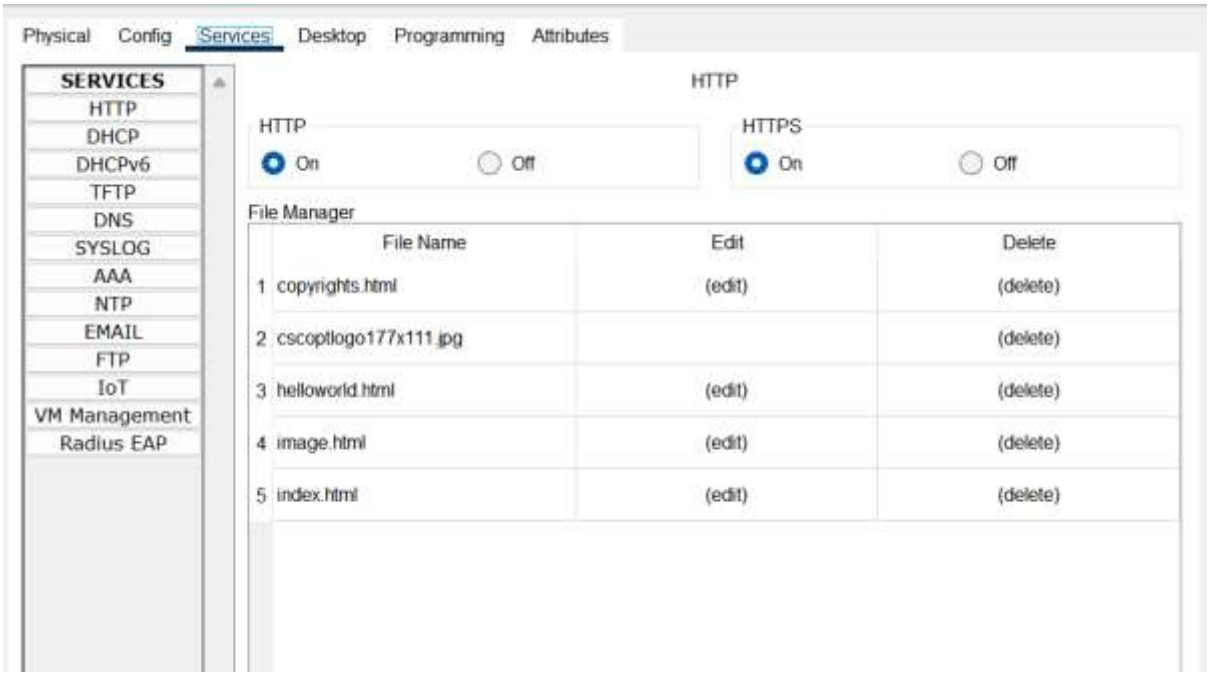
Procedure:

Step 1: Setup 3servers for DHCP, DNS and web servers and connect them to switch. Also connect some computers to another switch.

Step 2: Connect the both switches using a single router and then assign IP address to each of the server along with the gateway address for both end connections as shown in the figure.



Step 3: Now, enable the services for each of the servers. For this select respective server and then to services and enable them as per their functionalities.



Step 4: after enabling their services of the server, check for proper working of the servers by going to the web browser in PC0.

Step 5: Now, enable the working of the router for communication between the two ends of the switch from server to client computer.

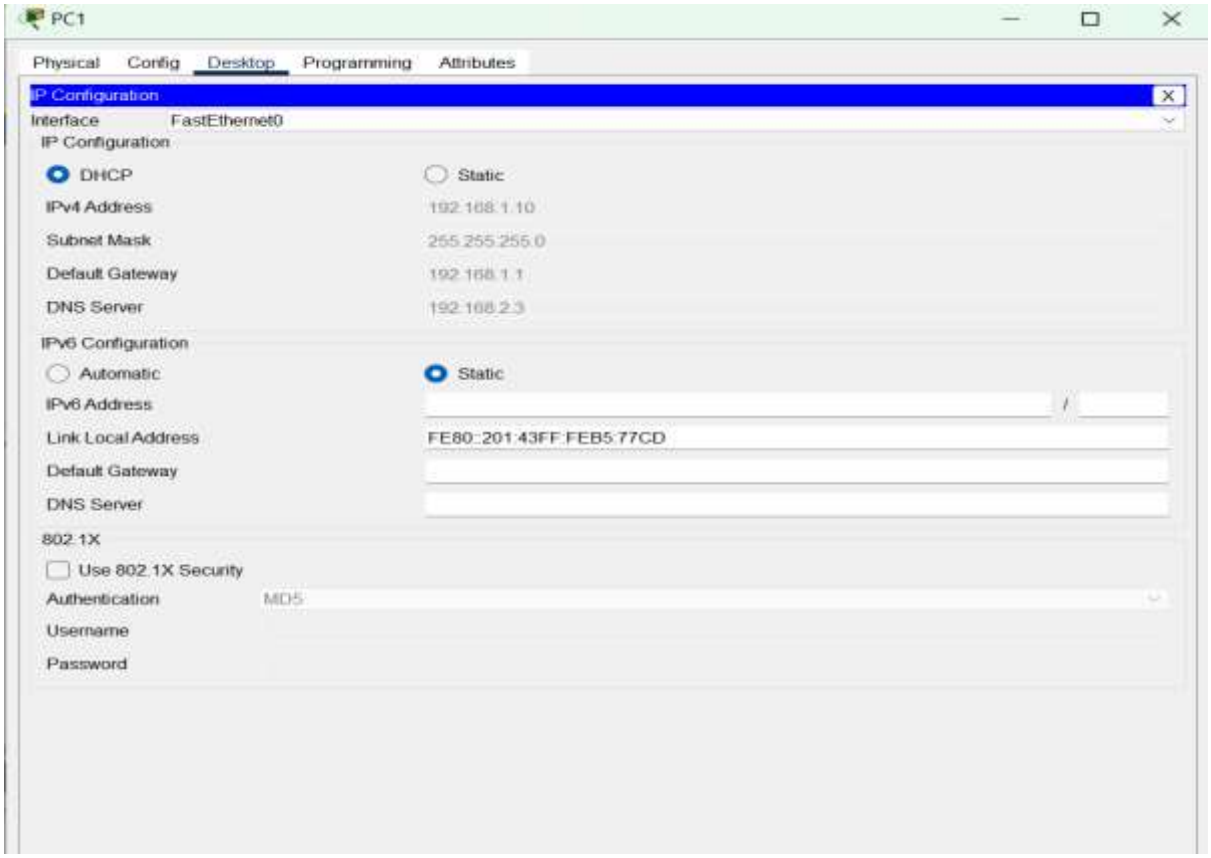
IOS Command Line Interface

```
Press RETURN to get started!



Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host
% Incomplete command.
Router(config)#nostname R1
               ^
% Invalid input detected at '^' marker.

Router(config)#hostname R1
R1(config)#int f0/0
R1(config-if)#ip add 192.168.2.1 255.255.255.0
R1(config-if)#no sh

R1(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

R1(config-if)#int f0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#int f0/1
R1(config-if)#ip hel
% Ambiguous command: "ip hel"
R1(config-if)#ip help
% Incomplete command.
R1(config-if)#ip helper-address 192.168.2.2
R1(config-if)#
```

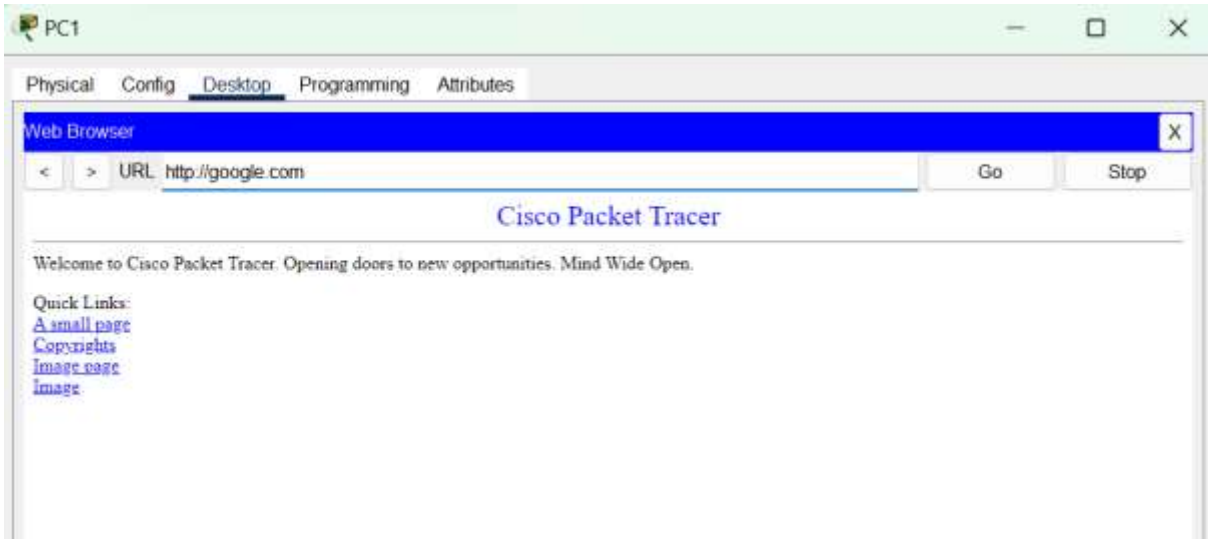
Output

The request from client to server can be given by:

For DHCP



For Web Server:



Conclusion:

Thus, the setup for DHCP, DNS and Web Server was successful using cisco packet tracer.

Lab 5: Basic router setup with DHCP

Objective(s): To understand and implement DHCP services in router using cisco packet tracer.

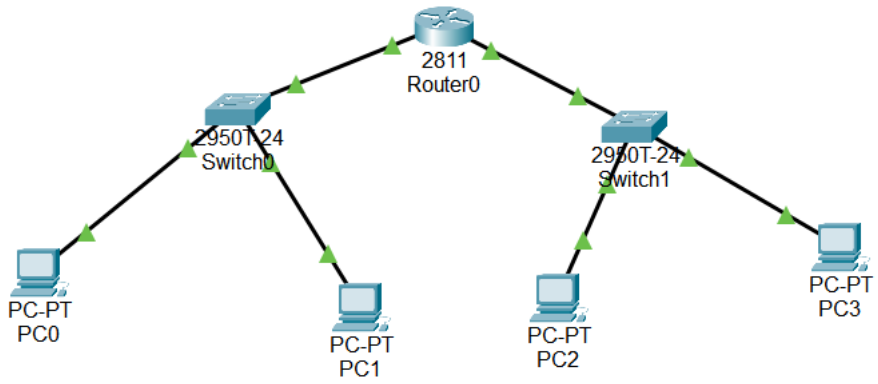
Theory:

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

A DHCP Server is a network server that automatically provides and assigns PI addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients. ADHCP server automatically sends the required network parameters for clients to properly communicate on the network.

Procedure:

Step 1: Setup a router connected to the two switches and then to the end devices.



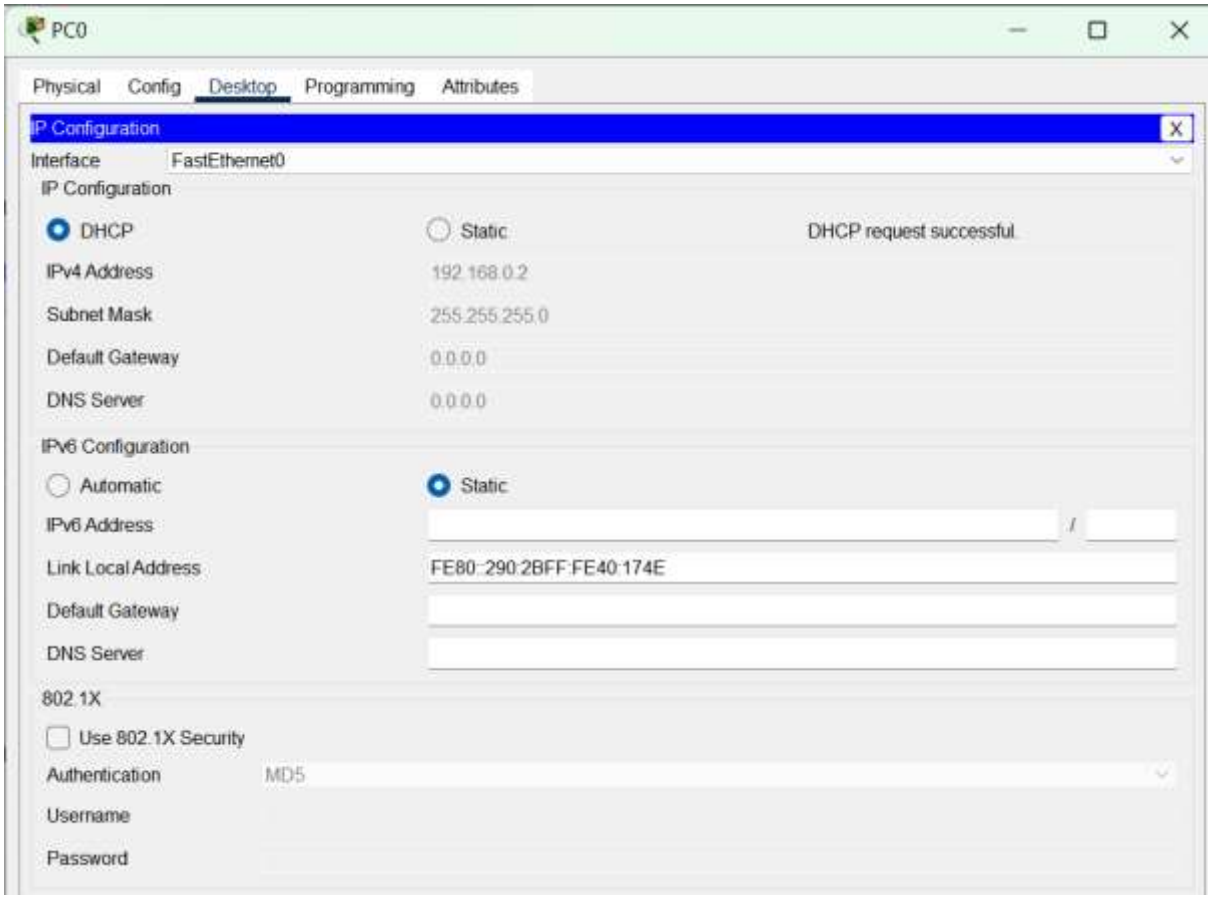
Step 2: Allocate the IP address for the computer system connecting system to the switches using commands in CLI of router.

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int fa0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#shutdown
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Step 3: Enable the DHCP services in the router.

```
Router(config-if)#do write memory
Building configuration...
[OK]
Router(config-if)#ip dhcp pool net1
Router(dhcp-config)#netwok 192.168.0.1 255.255.255.0
                         ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#netwok 192.168.0.1 255.255.255.0
                         ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#network 192.168.0.1 255.255.255.0
Router(dhcp-config)#exit
Router(config)#
```

Step 4: Check for the DHCP services in the end computer.



Conclusion:

Thus, DHCP services was implemented in router.

Lab 6: Static routing Implementation

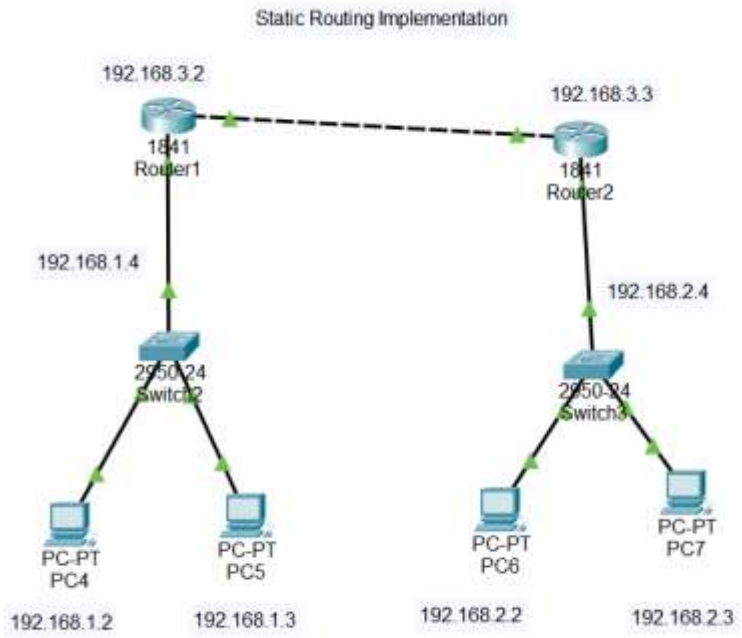
Objective(s): To understand and implementing the Static Routing.

Theory

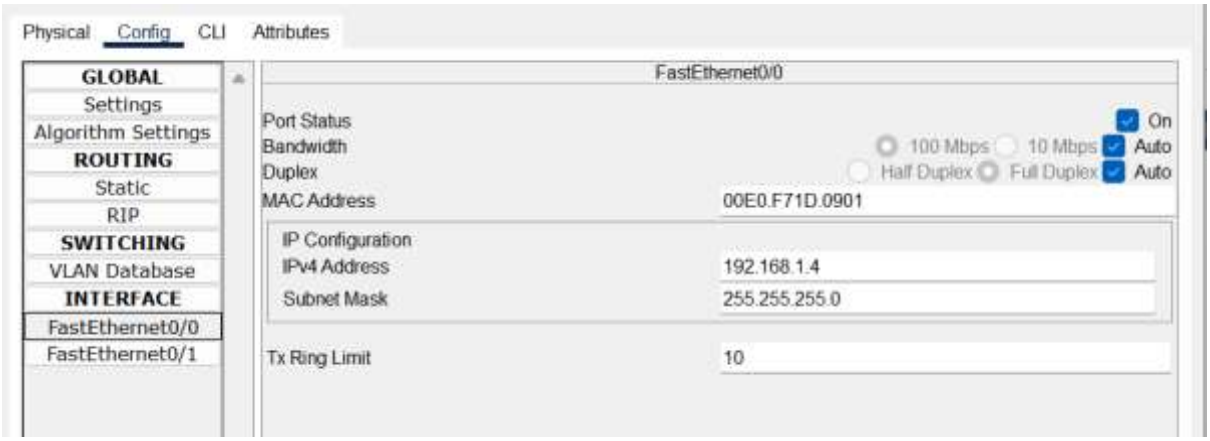
static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator. It is employed in scenarios where the network parameters and environment are expected to remain constant.

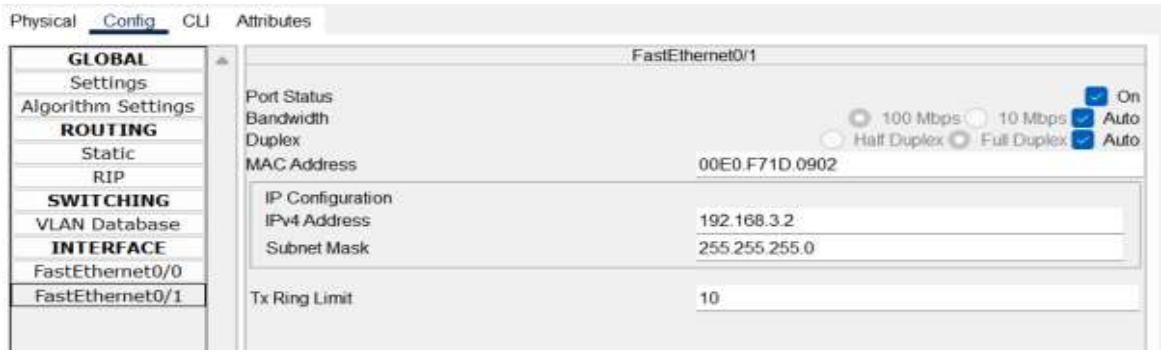
static routing is only optimal in a few situations. Network degradation, latency and congestion are inevitable consequences of the non-flexible nature of static routing because there is on adjustment when the primary route is unavailable

step :1 Configure to routers with its corresponding connection to switches and end devices and assign IP address to them.

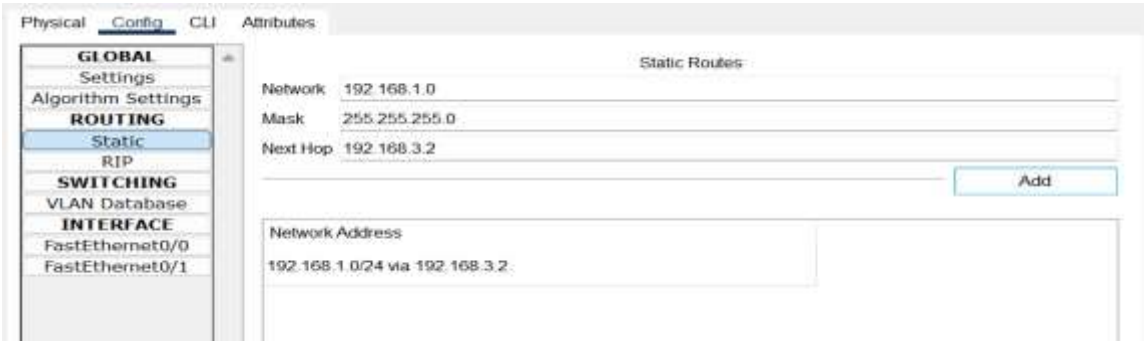


Step 2: Now, Configure each routers and the end computers.





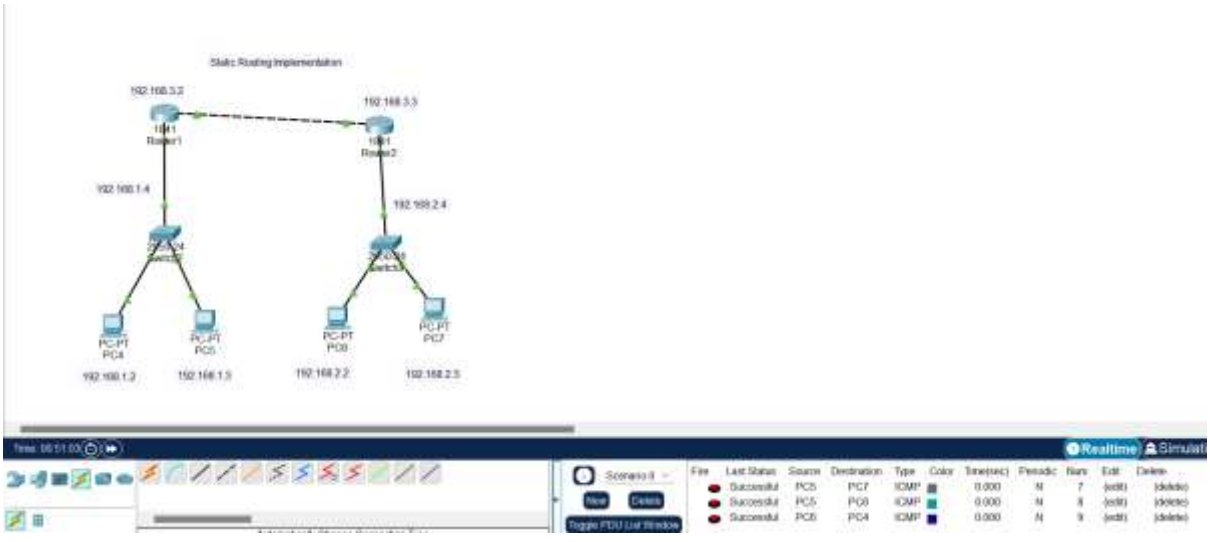
Step 3: Configure Static routing address in each router.



As we have statically configured the routing path any computer can communicate with any computer.

Output:

Thus, any computer can interact with any computer within two routers as shown below:



Conclusion: In this way, static routing was implemented between ant two routers and their end computing devices.

Lab 7: Dynamic routing implementation with RIP

Objective(s): To Understand the Basic Operation and implementation of RIP for dynamic routing using cisco packet tracer.

Theory:

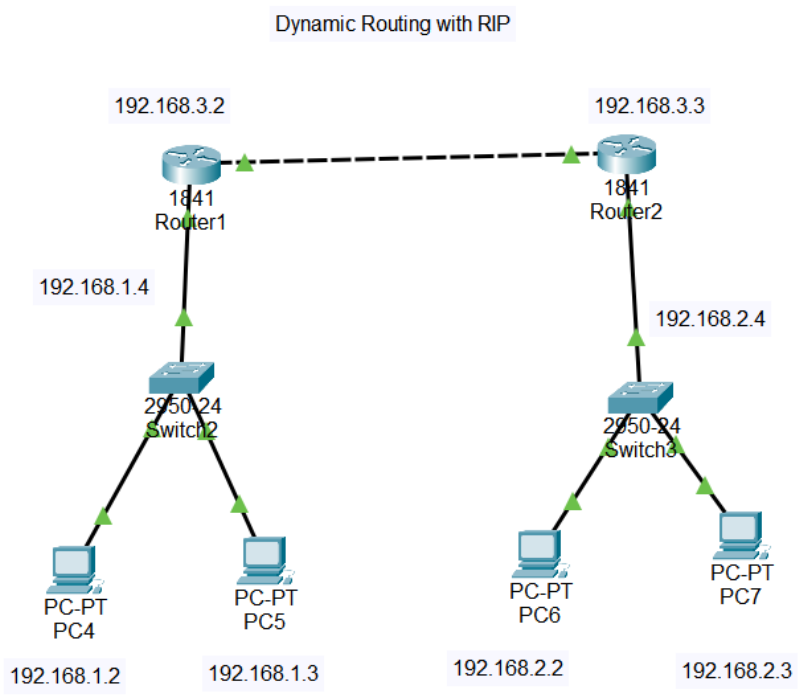
Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing dynamic routing enables routers to select paths according to real-time logical network layout changes. Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSP). Dynamic routing protocols allow routers to share information about the network with other routers to allow them to select the best path to reach a destination.

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

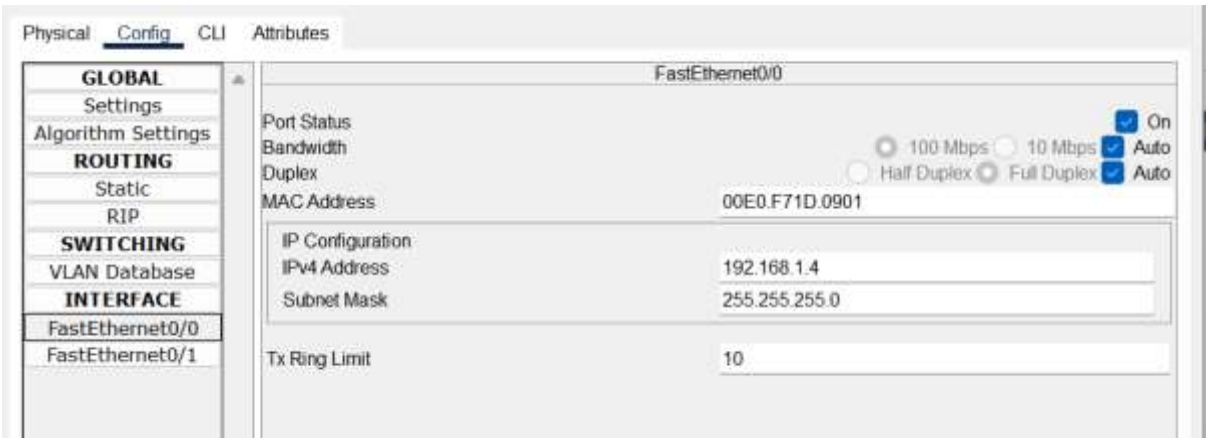
layer of the OSl model. RIP uses port number 520. Hop Count Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing 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.

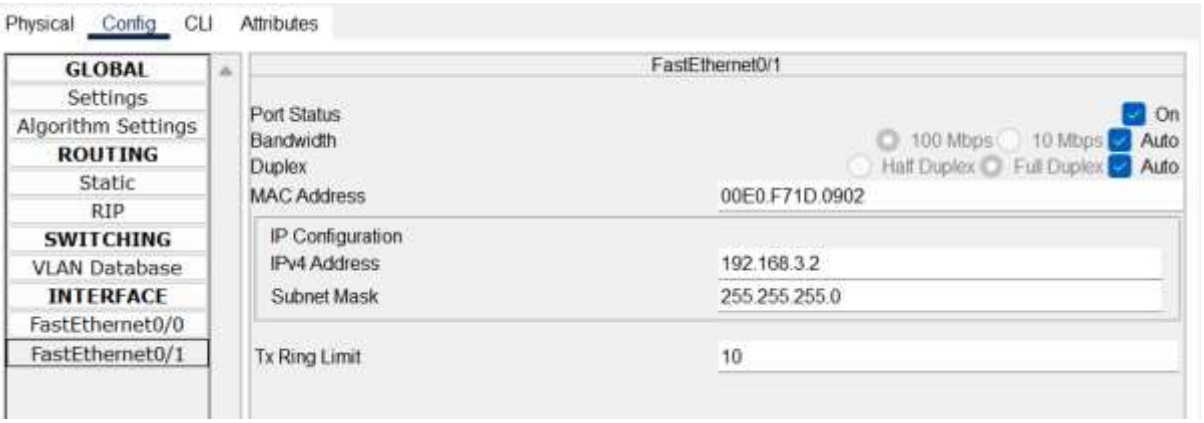
Procedure:

Step 1: Design the topology with two routers connecting to switch and then to corresponding computer / end devices.

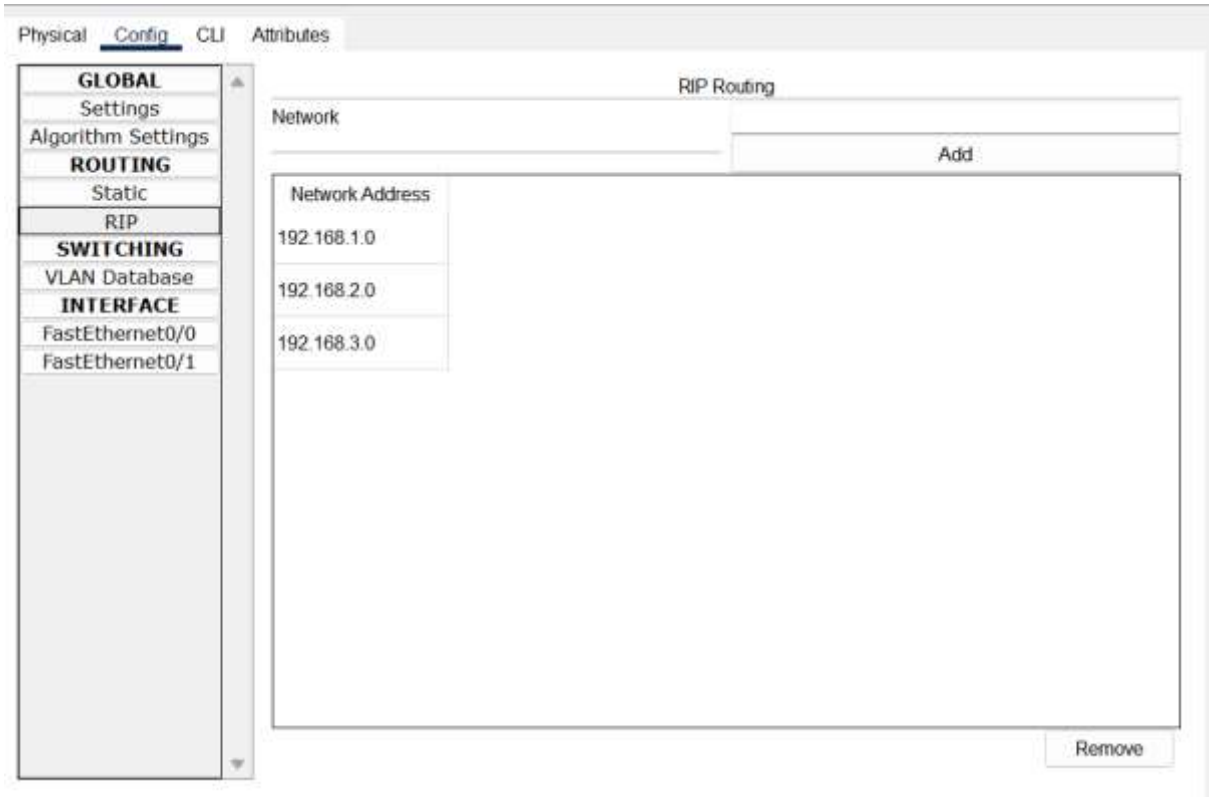


Step2: Assign IP address and gateways address to router and end devices



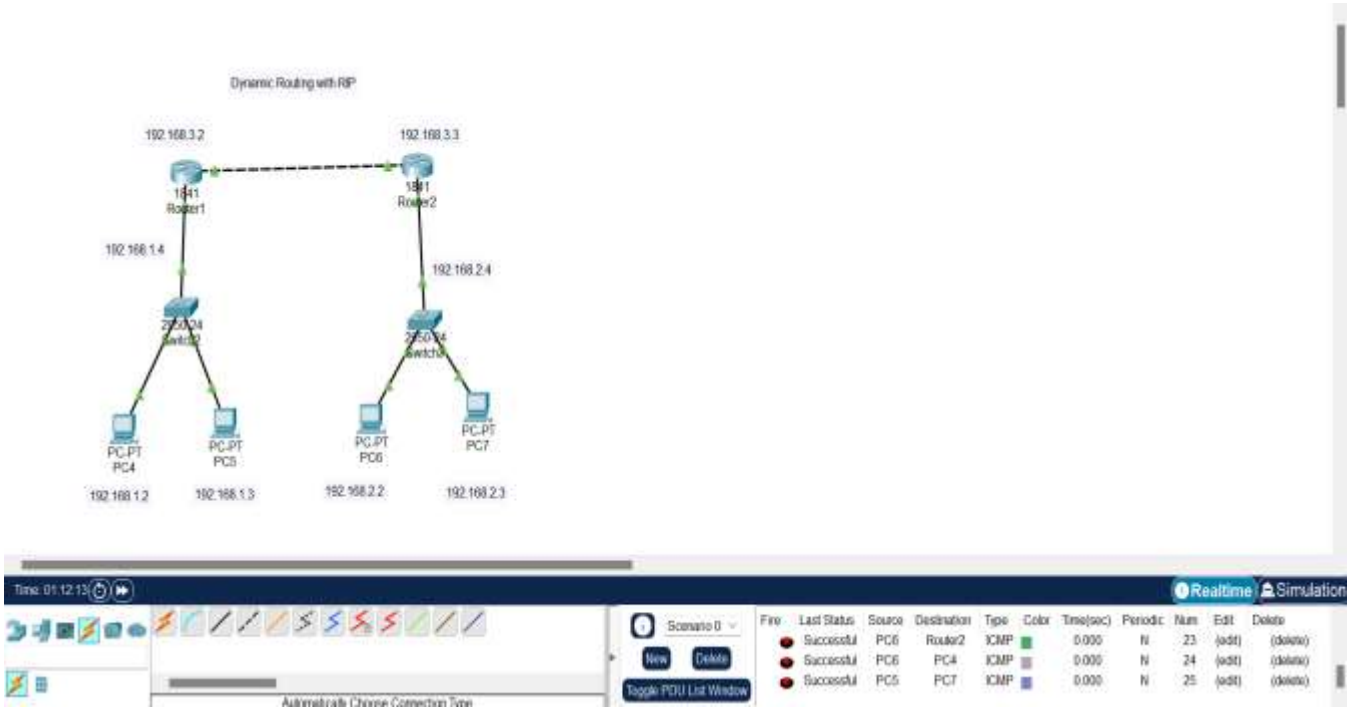


Step 3: Now, add RIP routing addresses to both of the routers.



Step 4: Dynamic routing with RIP is implemented of communication with two end devices from different routers if it is successful.

Output:



Conclusion:

In this way, dynamic routing with implementation of RIP is carried out using cisco packet tracer.

Lab 8: VLAN setup and inter – VLAN

Objective(s): To understand LAN networking, creation of VLAN, IP addressing in the VLAN and VLAN Trunk.

Theory:

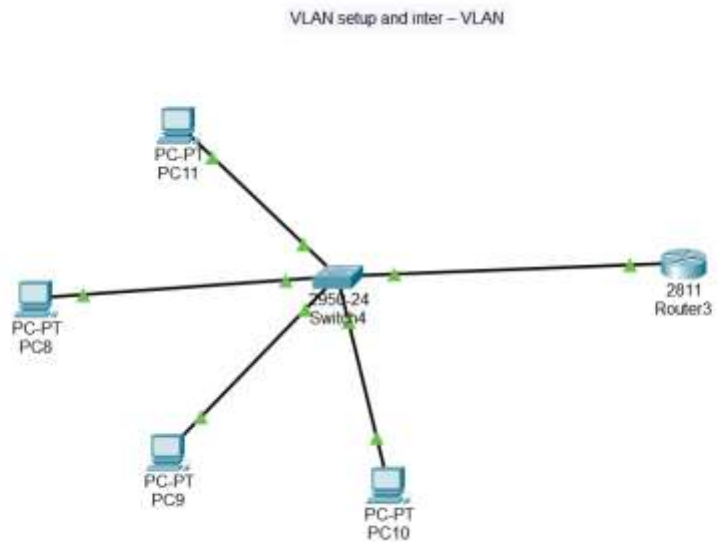
A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group. ALAN is a group of computers or other devices in the same place - e.g, the same building or campus - that share the

same physical network. ALAN is usually associated with an Ethernet (Layer 2) broadcast domain, which is the set of network devices an Ethernet broadcast packet can reach. Computers on the LAN connect to the same network switch, either directly or through wireless access points (APs) connected to the same switch. Computers can also connect to one of a set of interconnected switches, such as asset of access switches that al connect up to a backbone switch. Once traffic crosses a router and engages Layer 3(IP-related) functions, it is not considered to be on the same LAN, even if everything stays in the same building or floor. As a result, a location could have many interconnected LANs. AVLAN, like the LAN it sits atop, operates at Layer 2 of the network, the Ethernet level. VLANs partition a single switched network into a set of overlaid virtual networks that can meet different functional and security requirements. This partitioning avoids the need to have multiple, distinct physical networks for different use cases.

In some cases, administrators must completely isolate VLANs and disallow any traffic between them. However, it is usually necessary to allow some traffic to flow between VLANs so certain services and systems are available on any network segment. That's where inter-VLAN routing comes in. Inter-VLAN routing enables routers or Layer 3 switches to route traffic between VLANs. Because the use case is so common, network administrators need to understand inter-VLAN routing.

Procedure:

Step 1: Create two VLANS (VLAN 10 and VLAN 20) with configuration of a switch connecting to four different pc and a router.



Step 2: Now assign the IP address to each end devices.

Step 3: configure switch for VLAN creation and routing in CLI

IOS Command Line Interface

```
Switch>
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# vlan 10
Switch(config-vlan)#name HR
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name IT
Switch(config-vlan)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#swithport access vlan 10
                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/2
Switch(config-if)#switchport access
% Incomplete command.
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa
%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#int fa0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
```

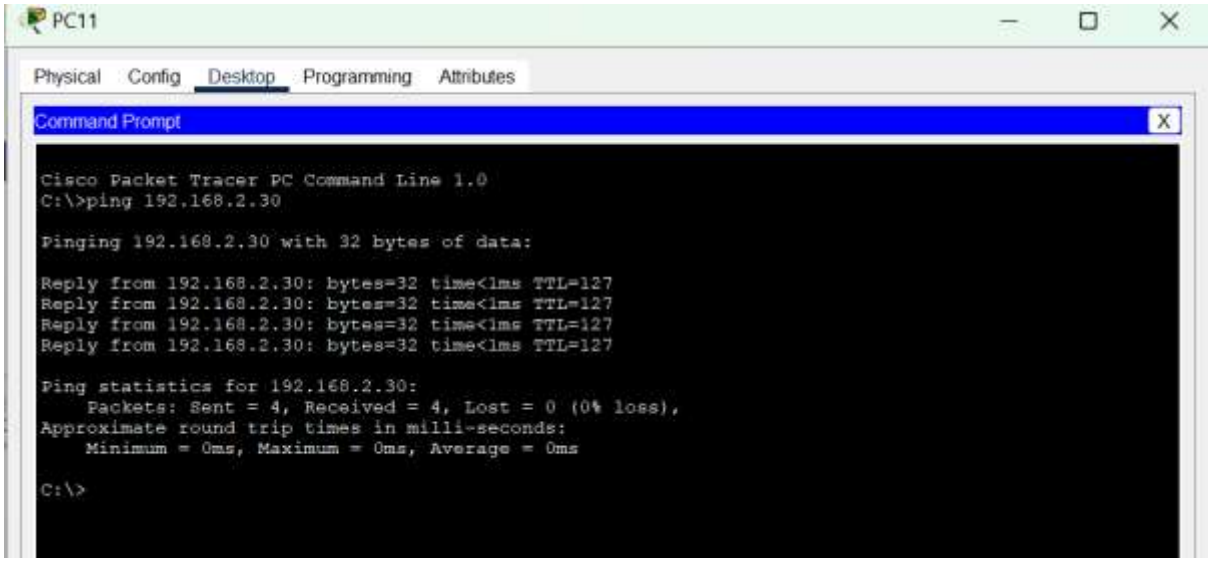
Step 4: Configure router for VLAN creation and routing in CLI

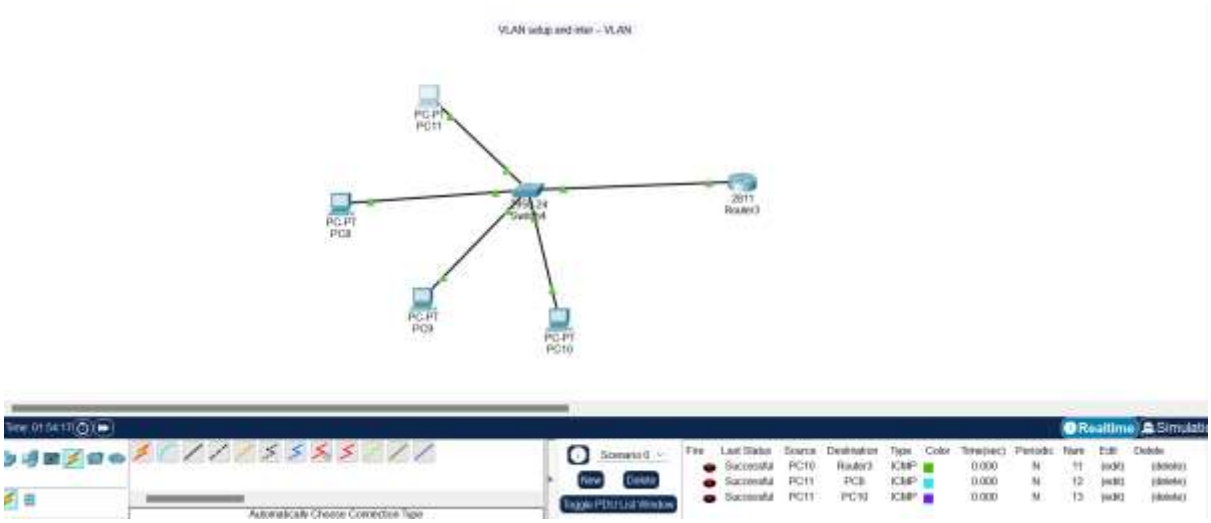
IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#fa0/0
               ^
% Invalid input detected at '^' marker.

Router(config)#int fa0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Router(config-if)#int fa0/0.10
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)#ipadd 192.168.1.1 255.255.255.0
                     ^
% Invalid input detected at '^' marker.

Router(config-subif)#ip add 192.168.1.1 255.255.255.0
Router(config-subif)#int fa0/0.20
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 add 192.168.2.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

Output:

Thus, a PC can communicate with other PC within the VLAN





Conclusion:

In this way, VLAN setup and inter-VLAN routing is carried out using cisco packet tracer.