Department of Computer Science and Engineering

Laboratory Manual

of

CE3004 - Network Laboratory

is submitted to

Ms. Ankita J Desai

Assistant Professor

Asha M. Tarsadia Institute of Computer Science and Technology

Uka Tarsadia University, Maliba Campus Bardoli, Gujarat

Semester – 2

(Summer 2022)

ASHA M. TARSADIA INSTITUTE OF COMPUTER SCIENCE AND TECHNOLOGY

CERTIFICATE

This is to certify that Mr./Ms. Saurabh Yadav Enrolment No: 202103103510362 of B.Tech. Computer Science and Engineering 2nd semester has satisfactorily completed his/her laboratory work of **CE3004 - Network Laboratory** during regular term in academic year 2021-22.

Date of Submission: _____

Ms. Ankita J Desai
Subject Teacher
Assistant Professor
Department of Computer Science and Engineering

Department Authority

Institute Stamp

INDEX

Sr. No.	Name of the Practical	Date	Grade	Signature
1	To create straight ethernet cable.	25/02/22		
2	To create cross ethernet cable.	04/02/22		
3	To configure DHCP protocol to dynamically allocate IP address.	11/03/22		
4	To study basic linux networking utility.	18/03/22		
5	To study HTTP, FTP, TFTP, DNS protocol.	25/03/22		
6	To study Cisco packet tracer and it's interface.	01/04/22 08/04/22		
7	To study and demonstrate LAN topology in Cisco Packet Tracer.	15/04/22		
8	To study and demonstrate dynamic routing in Cisco Packet Tracer.	06/05/22		

Practical 1

Aim: To create straight ethernet cable.

Tools Required:

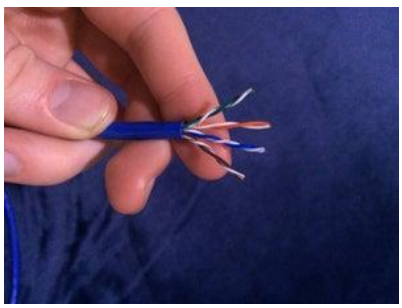
1) CAT 5 Cable CAT 5 Cable - bulk Category 5, cable bulk Category 5, cable
2) RJ45 Ends
3) Crimper for RJ45
4) Wire Cutters – to cut and strip the cable if necessary

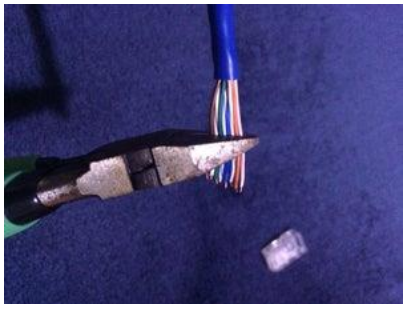
Steps to create straight ethernet cable:

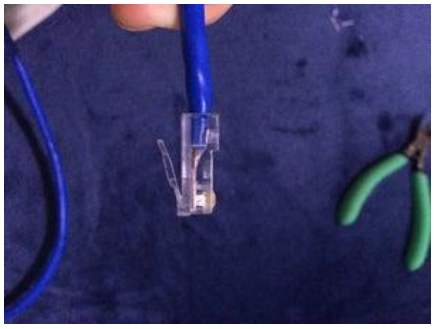
1) Cable Inspection

2) Striping the cable

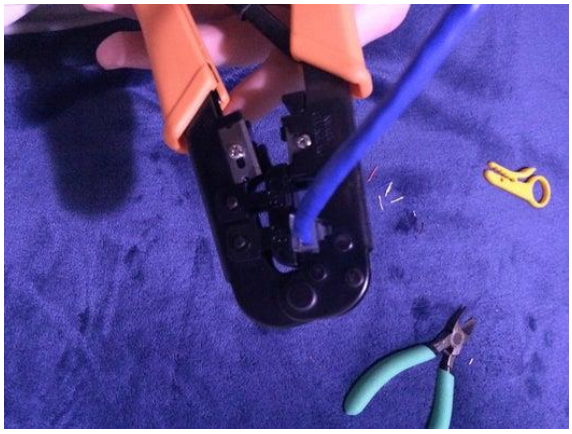
3) Putting the wires in the Connectors



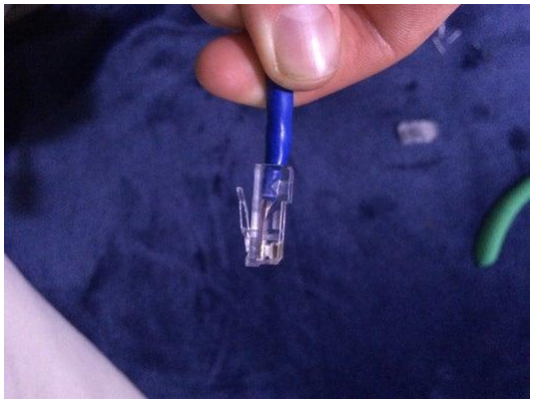


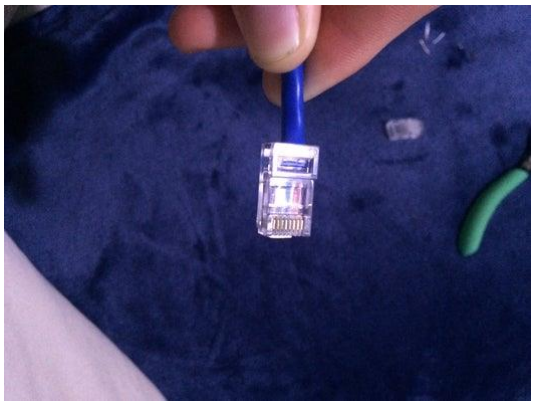


4) Crimping the Connector

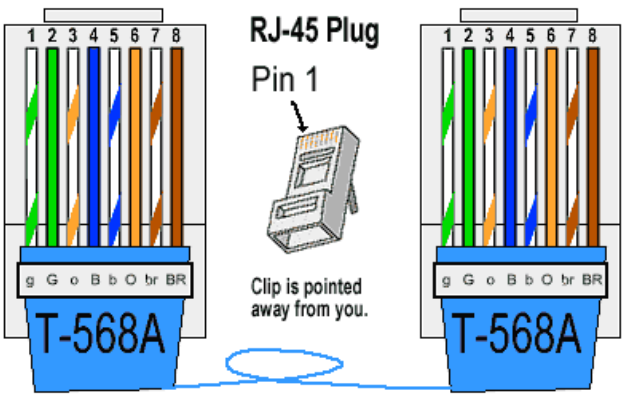


5) Testing the cable





Color-Code for straight through:



Practical 2

Aim: To create cross ethernet cable Tools Required:

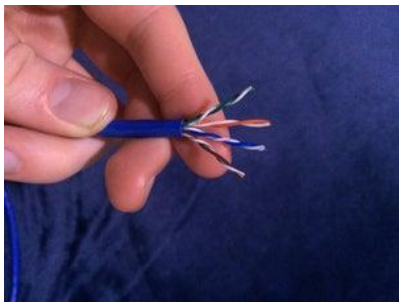
5) CAT 5 Cable CAT 5 Cable - bulk Category 5, cable bulk Category 5, cable
6) RJ45 Ends
7) Crimper for RJ45
8) Wire Cutters – to cut and strip the cable if necessary

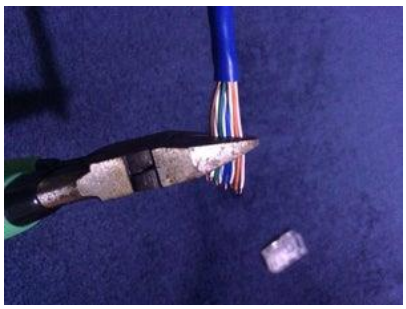
Steps to create straight ethernet cable:

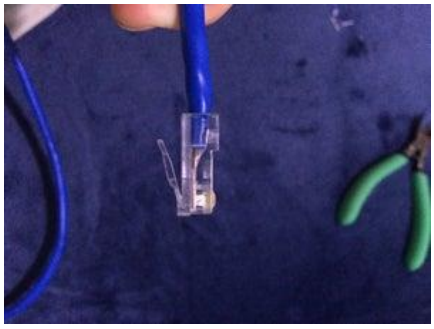
1) Cable Inspection

2) Striping the cable

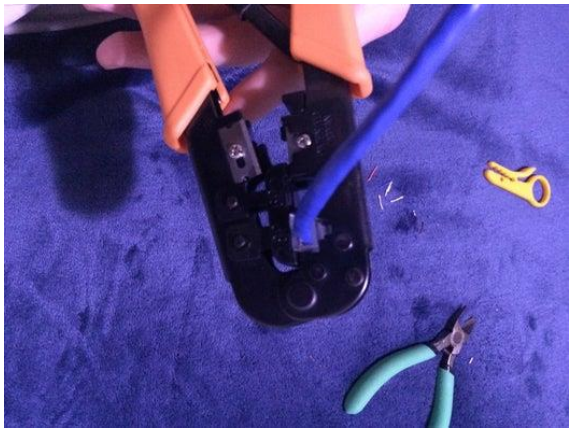
3) Putting the wires in the Connectors



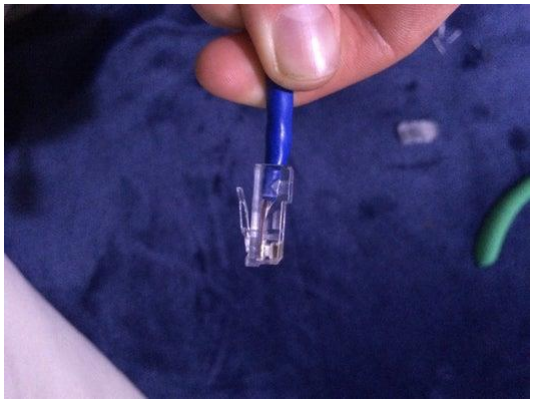


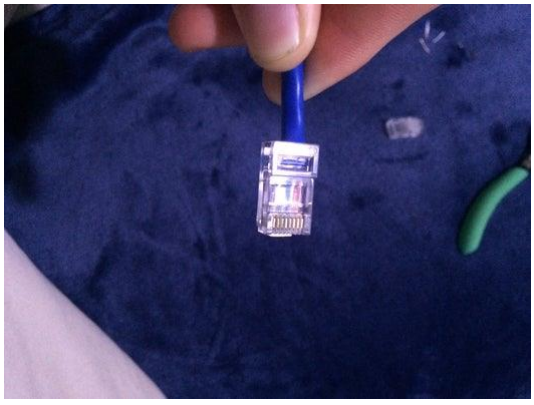


4) Crimping the Connector

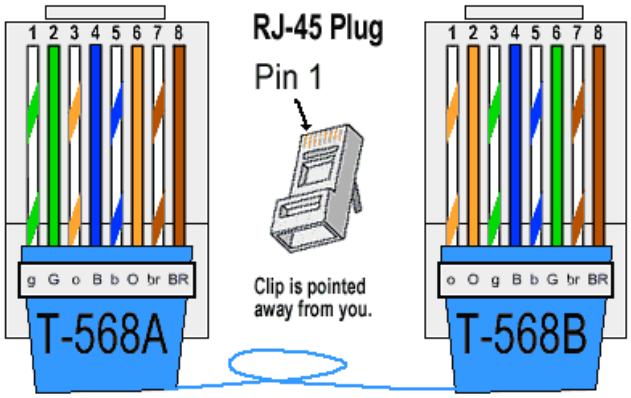


5) Testing the cable





Color-Code for straight through:

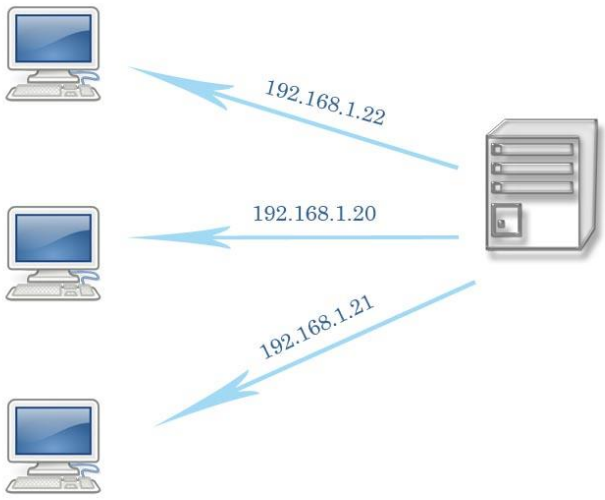


Practical 3

Aim: To configure DHCP protocol to dynamically allocate IP address.

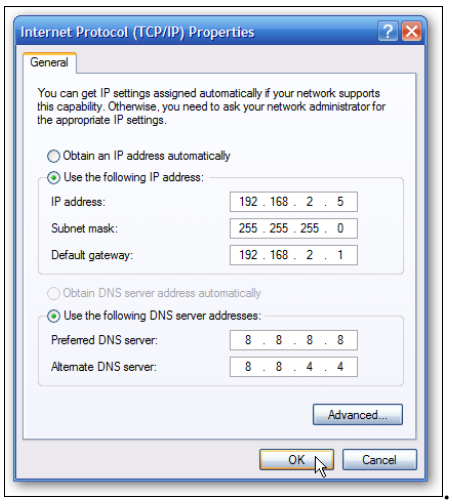
What is DHCP Protocol:

DHCP (Dynamic Host Configuration Protocol) is a network protocol, which assigns IP Address and configures network settings for devices to access internet services using the client-server architecture.

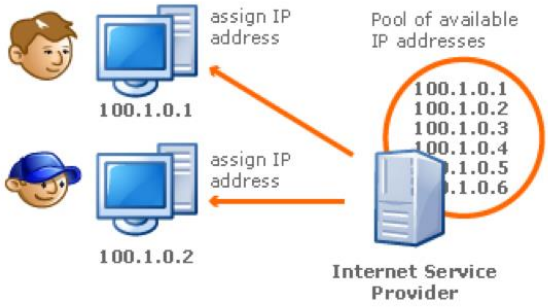


DHCP Allocation Methods

1) **Manual allocation also known as Static IP:**
   a) In this allocation process, the device is assigned the IP address by the user manually.
   b) This is done by operating the system's network configuration settings



2) **Dynamic allocation:**
   a) In this process, the DHCP server reserves an IP address for the client system and assigns dynamically
   b) The assigned IP address is given on lease which is temporarily assigned.



Practical 4

Aim: To study basic linux networking utility.

Ifconfig:

Linux ifconfig stands for interface configurator. It is one of the most basic commands used in network inspection. ifconfig is used to initialize an interface, configure it with an IP address, and enable or disable it. It is also used to display the route and the network interface.

```
cgpit-utu@cgpit-utu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.[redacted]  netmask 255.255.255.0  broadcast 192.168.[redacted]
        inet6 fe80::2b6d:[redacted]  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 3560  bytes 4587238 (4.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1075  bytes 103270 (103.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 111  bytes 9849 (9.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 111  bytes 9849 (9.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ping:

Linux ping is one of the most used network troubleshooting commands. It basically checks for the network connectivity between two nodes.

```
cgpit-utu@cgpit-utu:~$ ping utu.ac.in
PING utu.ac.in (103.241.244.49) 56(84) bytes of data.
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=1 ttl=57 time=72.3 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=2 ttl=57 time=68.1 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=3 ttl=57 time=71.9 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=4 ttl=57 time=158 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=5 ttl=57 time=52.8 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=6 ttl=57 time=56.0 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=7 ttl=57 time=54.2 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=8 ttl=57 time=121 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=9 ttl=57 time=39.1 ms
64 bytes from 103.241.244.49 (103.241.244.49): icmp_seq=10 ttl=57 time=38.7 ms
^C
--- utu.ac.in ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9023ms
rtt min/avg/max/mdev = 38.747/73.292/158.370/36.031 ms
cgpit-utu@cgpit-utu:~$
```

Traceroute:

Linux traceroute is one of the most useful commands in networking. It is used to troubleshoot the network. It detects the delay and determines the pathway to your target. It basically helps in the following ways:

```
cgpit-utu@cgpit-utu:~$ traceroute google.com
traceroute to google.com (142.250.183.174), 64 hops max
  1   192.168[redacted]  45.320ms  61.189ms  1.871ms
  2   106.213.225.1  18.055ms  39.486ms  40.460ms
  3   125.22.222.237  117.585ms  40.146ms  18.474ms
  4   182.79.141.201  44.560ms  38.234ms  49.232ms
  5   72.14.212.48  52.674ms  40.153ms  39.683ms
  6   *  *  *
  7   108.170.248.177  50.090ms  34.545ms  41.788ms
  8   108.170.248.179  40.415ms  32.438ms  39.726ms
  9   108.170.248.209  43.935ms  38.344ms  39.677ms
 10   142.251.64.13  37.156ms  41.863ms  41.088ms
 11   142.250.183.174  36.503ms  35.215ms  39.755ms
cgpit-utu@cgpit-utu:~$
```

Route:

Linux route command displays and manipulates the routing table existing for your system. A router is basically used to find the best way to send the packets across to a destination.

```
cgpit-utu@cgpit-utu:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
192.168[redacted]  0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
cgpit-utu@cgpit-utu:~$
```

Dig:

Linux dig command stands for Domain Information Groper. This command is used in DNS lookup to query the DNS name server. It is also used to troubleshoot DNS related issues. It is mainly used to verify DNS mappings, MX Records, host addresses, and all other DNS records for a better understanding of the DNS topography.

```
cgpit-utu@cgpit-utu:~$ dig utu.ac.in

; <<>> DiG 9.11.3-1ubuntu1.15-Ubuntu <<>> utu.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31792
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;utu.ac.in.                     IN      A

;; ANSWER SECTION:
utu.ac.in.              102     IN      A       103.241.244.49

;; Query time: 5 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun May 15 00:00:15 IST 2022
;; MSG SIZE  rcvd: 54
```

Practical 5

Aim: To study HTTP, FTP, TFTP, DNS protocol.

HTTP:

Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes. HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response. HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests.

FTP:

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.

In an FTP transaction, the end user's computer is typically called the *local host*. The second computer involved in FTP is a *remote host*, which is usually a server. Both computers need to be connected via a network and configured properly to transfer files via FTP. Servers must be set up to run FTP services, and the client must have FTP software installed to access these services.

Although many file transfers can be conducted using Hypertext Transfer Protocol (HTTP) -- another protocol in the TCP/IP suite -- FTP is still commonly used to transfer files behind the scenes for other applications, such as banking services. It is also sometimes used to download new applications via web browsers.

TFTP:

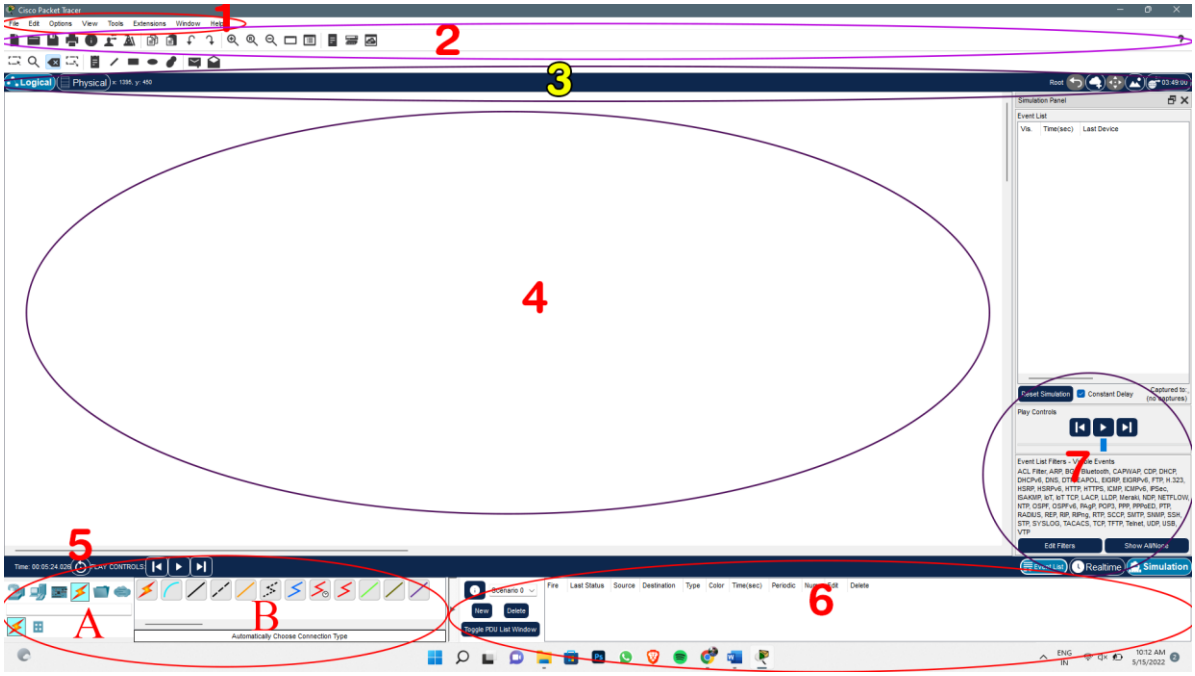
TFTP (Trivial File Transfer Protocol). TFTP is used to transfer a file either from client to server or from server to client without the need of FTP feature. Software of TFTP is smaller than FTP. TFTP works on 69 Port number and its service is provided by UDP.

DNS:

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:cb00:2048:1::c629:d7a2 (in IPv6).

Practical 6

Aim: To study Cisco packet tracer and it's interface.



Area 1: Menu bar – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.

Area 2: Main toolbar – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.

Area 3: Logical/Physical workspace tabs – These tabs allow you to toggle between the Logical and Physical work areas.

Area 4: Workspace – This is the area where topologies are created and simulations are displayed.

Area 5: This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas:

Area 5A: Device-type selection box – This area contains device categories

Area 5B: Device-specific selection box – When a device category is selected, this selection box displays the different device models within that category

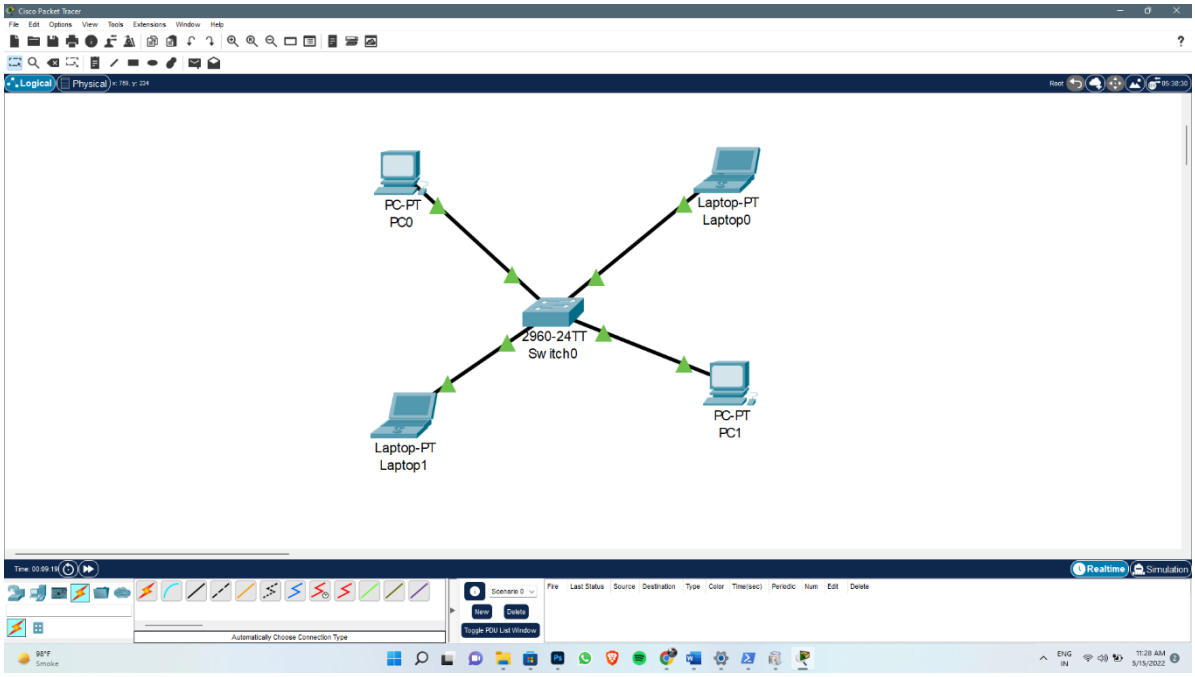
Area 6: User-created packet box – Users can create highly-customized packets to test their topology from this area, and the results are displayed as a list.

Area 7: These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.

Practical 7

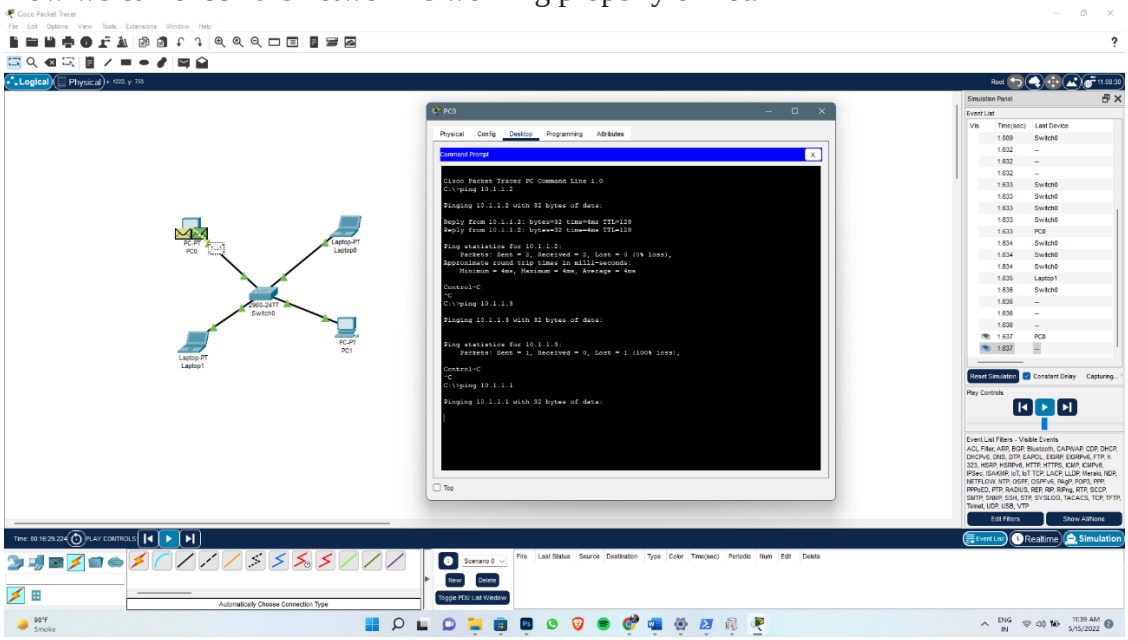
Aim: To study and demonstrate LAN topology in Cisco Packet Tracer.

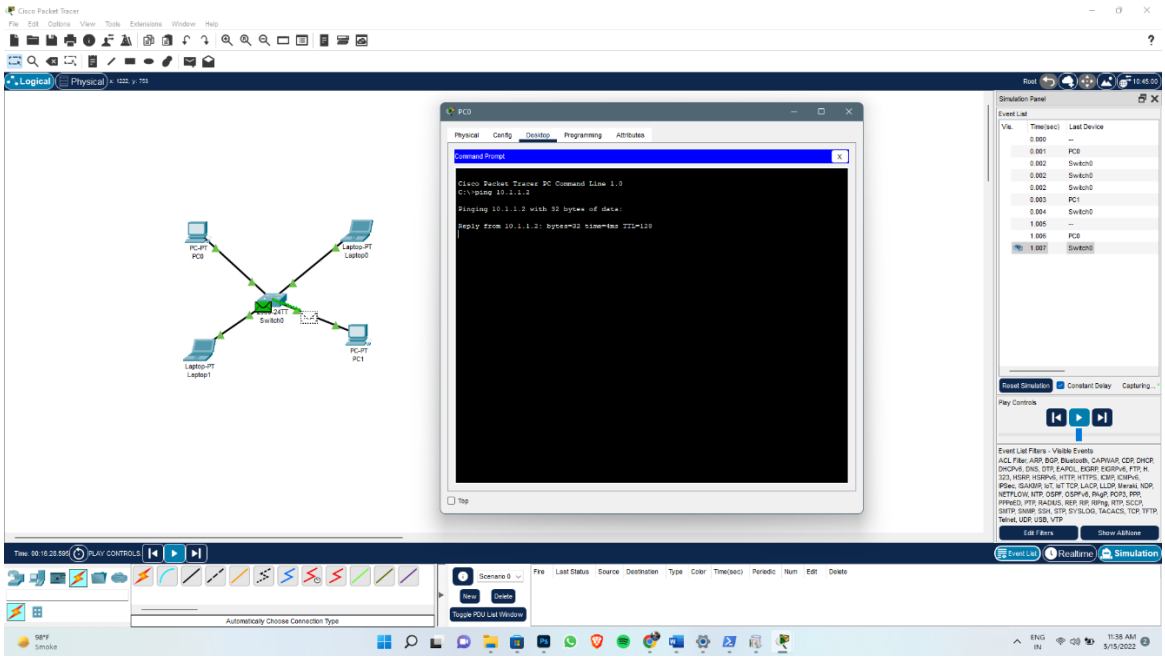
This is a basic LAN network created in Cisco Packet Tracer.

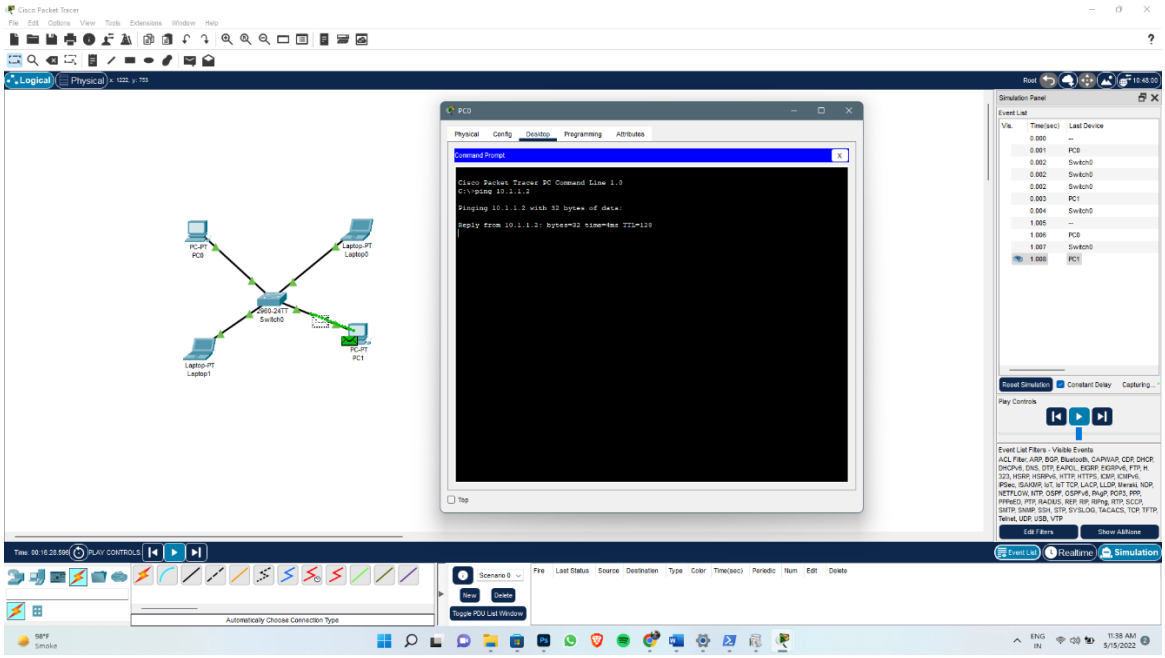


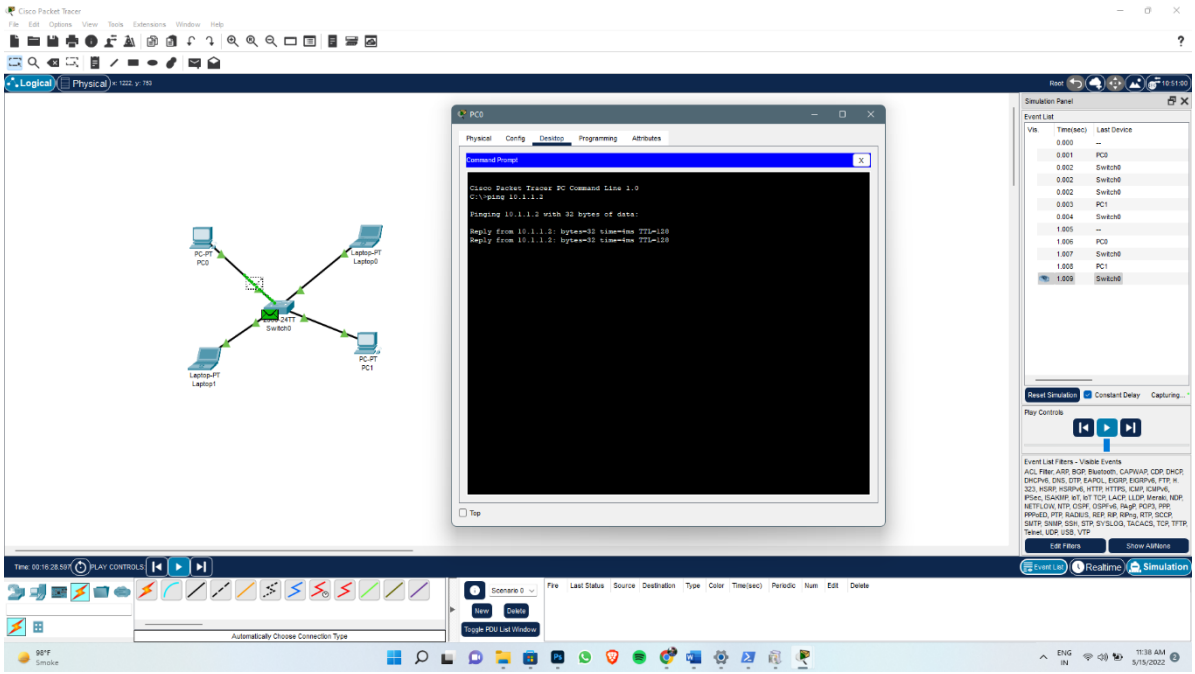
After the connections are done all the devices are allocated unique.
Laptop0: 10.1.1.1
PC1: 10.1.1.2
Laptop1: 10.1.1.3
PC0: 10.1.1.4

Now we can check the network is working properly or not.




Cisco Packet Tracer
Logical
Physical
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.2
Pinging 10.1.1.2 with 32 bytes of data:
Reply from 10.1.1.2: bytes=32 time=4ms TTL=128
PC-PT PC0
Laptop-PT Laptop0
2960-24TT Switch0
PC-PT PC1
Laptop-PT Laptop1
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Event List
Realtime
Simulation
Automatically Choose Connection Type


Cisco Packet Tracer
Logical
Physical
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.2
Pinging 10.1.1.2 with 32 bytes of data:
Reply from 10.1.1.2: bytes=32 time=4ms TTL=128
PC-PT PC0
Laptop-PT Laptop0
2960-24TT Switch0
PC-PT PC1
Laptop-PT Laptop1
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Event List
Realtime
Simulation
Automatically Choose Connection Type



In the above network:
I ping the PC1 from PC0 and as a result we can see that a packet is sent from PC0 to PC1 within the network and then a packet is received back from PC1 to PC0.

The above screenshorts are the demonstration of the basic and simple LAN network in the Cisco Packet Tracer.

Practical 8

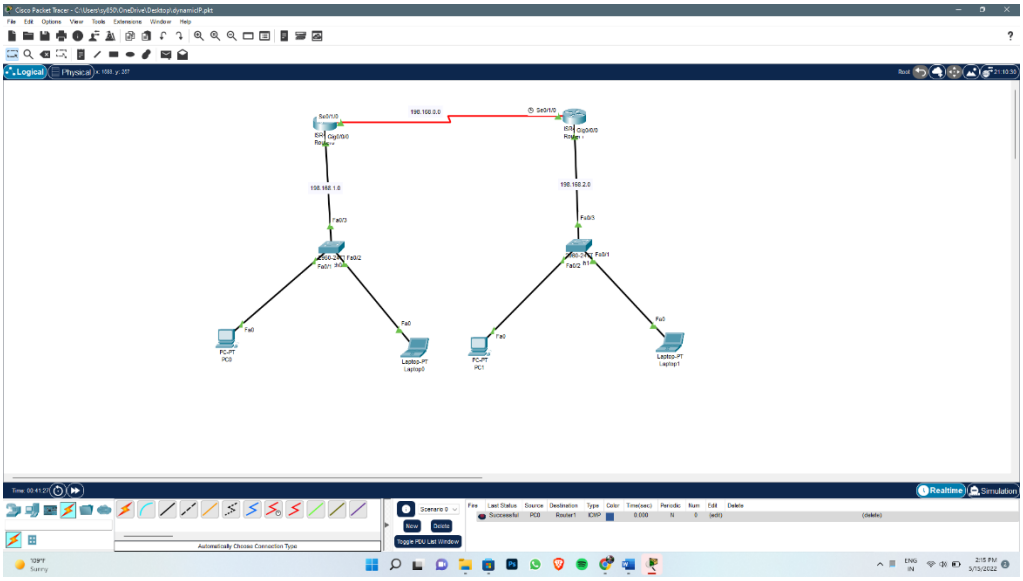
Aim: To study and demonstrate dynamic routing in Cisco Packet Tracer.

What is dynamic routing in Cisco?

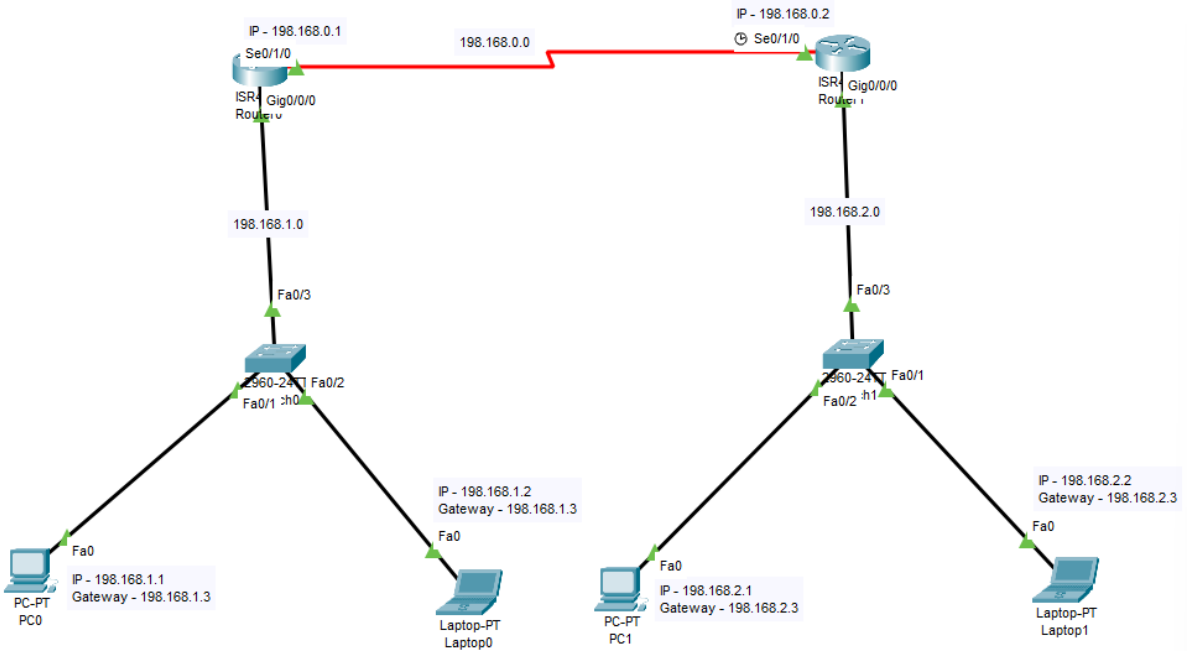
It allows one router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network.

Demonstration:

Below is a simple dynamic routing connection made in Cisco Packet Tracer.



Below Fig. contains the IP Addresses of each device and the default Gateway.



The Configurations for each router is shown below.

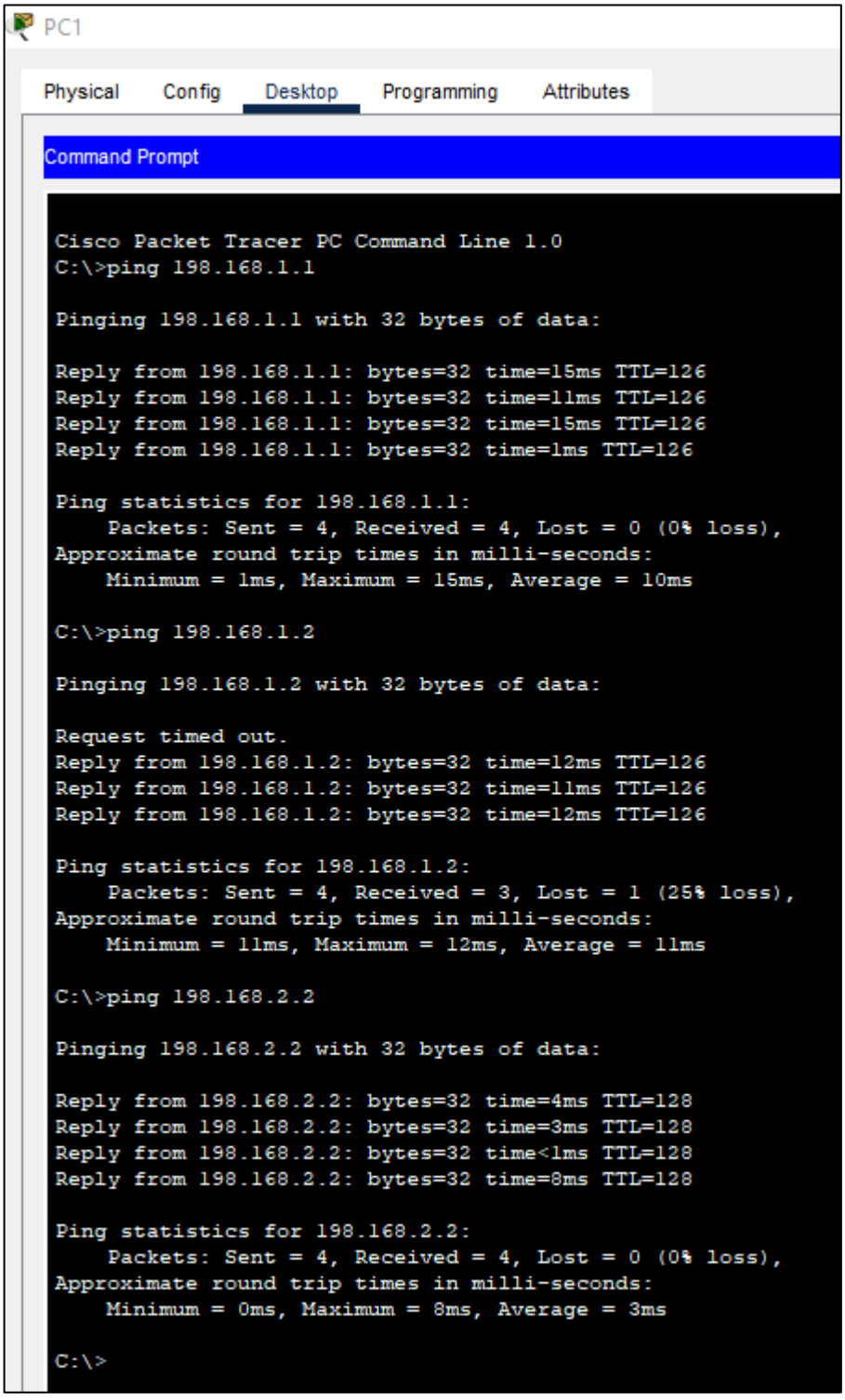
Router0 Configuration:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
ip address 198.168.1.3 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 198.168.1.0
Router(config-router)#network 198.168.0.0
Router(config-router)#network 198.168.2.0
Router(config-router)#
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
ip address 198.168.0.1 255.255.255.0
Router(config-if)#clock rate 4000000
This command applies only to DCE interfaces
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

Router1 Configurations:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
ip address 198.168.2.3 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 198.168.0.0
Router(config-router)#network 198.168.1.0
Router(config-router)#network 198.168.2.0
Router(config-router)#
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
ip address 198.168.0.2 255.255.255.0
Router(config-if)#clock rate 4000000
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

After all the configurations are done let's test the connection. For this we will ping all the other devices from one device within the network.



As we can in the above screenshot all the other devices within the network responds to the packet sent to them.

Thus, this is the demonstration of a simple Dynamic Routing in the Cisco Packet Tracer.

Advantages of dynamic routing:

- It is straightforward to configure.
- It adapts to network topology changes.
- It is suitable in a network where many routers are used.
- Configuring dynamic routing does not require detailed knowledge of the network.

Disadvantages of Dynamic Routing

- Resources. Dynamic routing requires more resources such as CPU, RAM and Bandwidth.
- Communication. Some machines in the network may have problems in communicating with dynamic routing protocol.
- Complex network and it’s configuration.