



KRISHNA ENGINEERING COLLEGE

(Approved by AICTE & Affiliated to Dr. APJ Abdul Kalam Technical University (Formerly UPTU), Lucknow)

Department of CSE – AI

INDEX

Student Roll no :- 2101611520020

Student name :- Harsh Maheshwari

Subject name :- CN Lab

Subject code :- KCS653

Sno	Practical name	Scheduled date	Implementation (10 marks)	Output (5 marks)	Viva (5 marks)	Total (20 marks)	Signature
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							

Faculty Remarks & Signature



KRISHNA ENGINEERING COLLEGE

(Approved by AICTE & Affiliated to Dr. APJ Abdul Kalam Technical University (Formerly UPTU), Lucknow)

INDEX

S.NO	TITLE	DATE	SIGNATURE
1	Study of different types of Network cables and practically implement the cross-wired cable and straight through cable using clapping tool.		
2	Study of Network devices in detail.		
3	Study of network IP and basic networking commands.		
4	Basic networking device configuration and securing TELNET.		
5	Configure switch and router ports and IP route.		
6	Implementation of static routing.		
7	Configure a network using distance vector routing protocol.		
8	Configure network using link state vector routing protocol.		

PRACTICAL: 1

AIM: Study of different types of Network cables and practically implements the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Clipping Tool, Twisted pair Cable

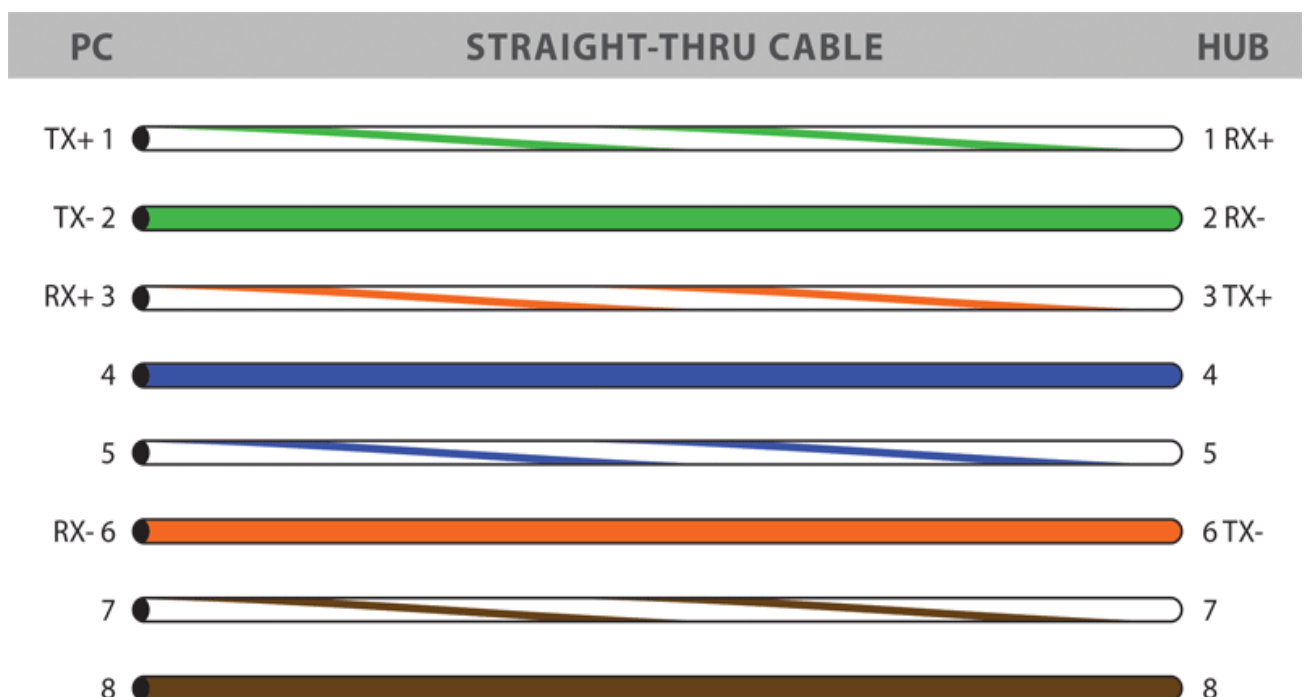
Procedure: To do these practical following steps should be done:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render it useless. Check the wires, **one more time** for nicks or cuts. If there are any, just whack the whole end off, and start over.

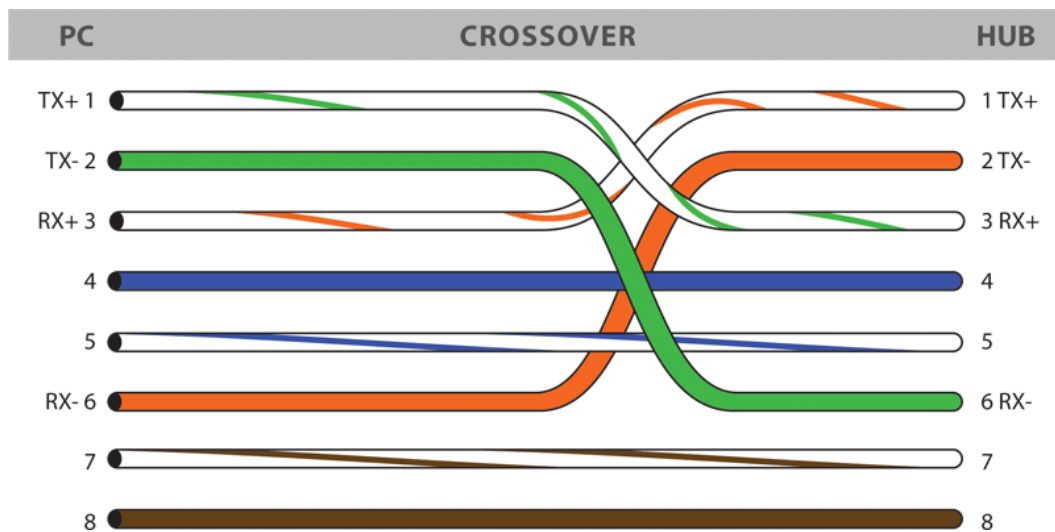
2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

➤ **Diagram shows you how to prepare straight through wired connection.**



➤ **Diagram shows you how to prepare Cross wired connection**



➤ **Ethernet Cable Tips:**

- A straight-thru cable has identical ends.
- A crossover cable has different ends.
- A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- A crossover has one end with the Orange set of wires switched with the Green set.
- Odd numbered pins are always striped; even numbered pins are always solid coloured.
- Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left.
- No more than 1/2" of the Ethernet cable should be untwisted otherwise it will be susceptible to crosstalk.
- Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near noise inducing components.

PRACTICAL: 2

AIM: Study of various network devices in detail

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and requirements for a Network+ candidate. The all network devices are explained below:

Hubs:

The hub or network hub connects computers and devices and sends messages and data from any one device to all the others. If the desktop computer wants to send data to the laptop and it sends a message to the laptop through the hub, the message will get sent by the hub to all the computers and devices on the network. They need to do work to figure out that the message is not for them. The message also uses up bandwidth (room) on the network wires or wireless radio waves and limits how much communication can go on. Hubs are not used often these days.

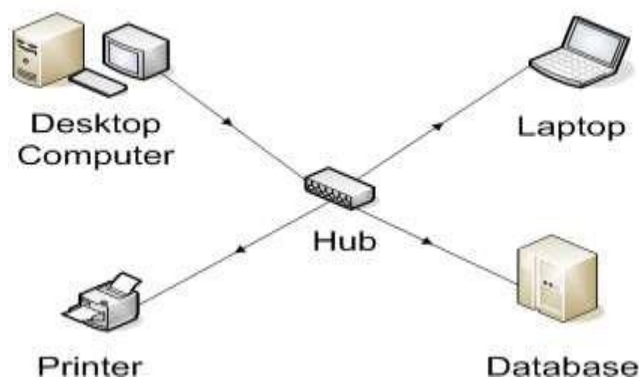


Fig.1 Hub

Switch:

The switch connects the computer network components but it is smart about it. It knows the address of each item and so when the desktop computer wants to talk to the laptop, it only sends the message to the laptop and nothing else. In order to have a small home network that just connects the local equipment all that is really needed is a switch and network cable or the switch can transmit wireless information that is received by wireless receivers that each of the network devices have.

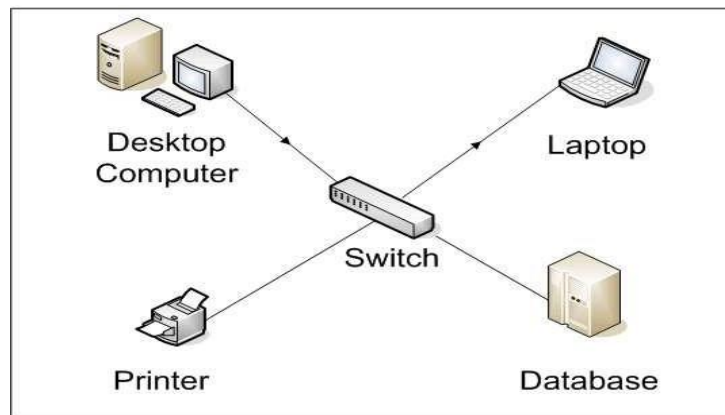


Fig. 2 Switch

Bridges:

Bridges are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came).

A bridge functions by blocking or forwarding data, based on the destination MAC address written into each frame of data. If the bridge believes the destination address is on a network other than that from which the data was received, it can forward the data to the other networks to which it is connected. If the address is not on the other side of the bridge, the data is blocked from passing. Bridges “learn” the MAC addresses of devices on connected networks by “listening” to network traffic and recording the network from which the traffic originates. Figure 3 shows a representation of a bridge.

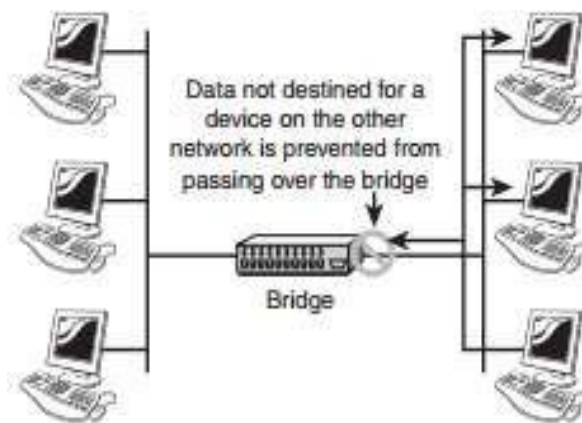


Fig. 3 Bridges

Routers:

In a common configuration, routers are used to create larger networks by joining two network segments. A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router. Figure 4 shows, in basic terms, how a router works.

The routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to be two things. It must be up-to-date, and it must be complete. There are two ways that the router can get the information for the routing table—through static routing or dynamic routing.

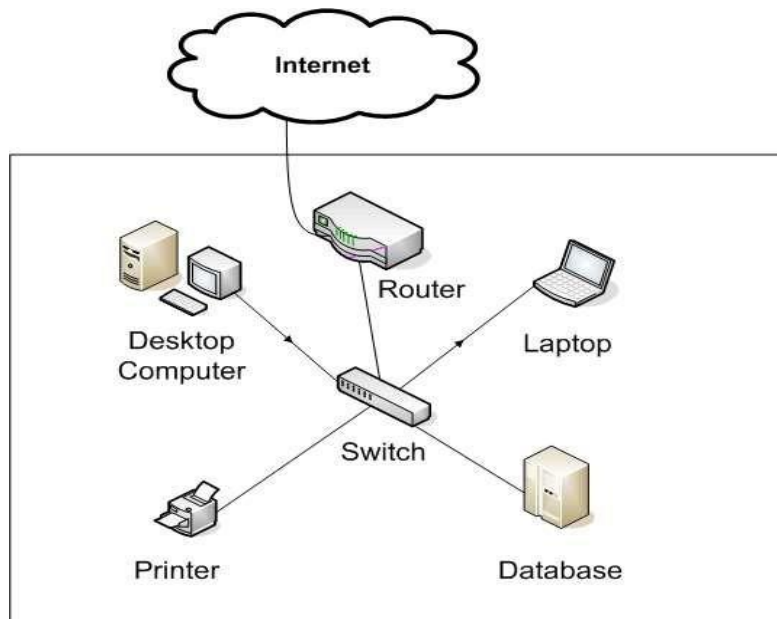


Fig. 4 Router

Gateways:

Any device that translates one data format to another is called a gateway. Some examples of gateways include a router that translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself. In many cases, the gateway functionality is incorporated into another device.

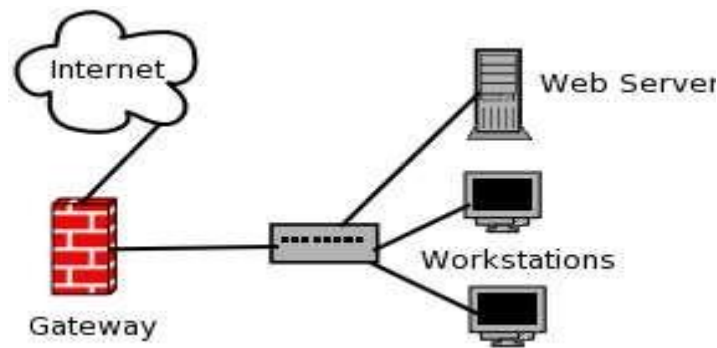


Fig. 5 Gateways

CSU/DSU:

A Channel Service Unit/Digital Service Unit (CSU/DSU), sometimes called Data Service Unit, is a device that converts the digital signal format used on LANs into one used on WANs. Such translation is necessary because the networking technologies used on WANs are different from those used on LANs. The CSU/DSU sits between the LAN and the access point provided by the telecommunications company. Many router manufacturers are now incorporating CSU/DSU functionality into their products.

Network Cards:

Network cards, also called Network Interface Cards, are devices that enable computers to connect to the network. When specifying or installing a NIC, you must consider the following issues:

- **System bus compatibility**—If the network interface you are installing is an internal device, bus compatibility must be verified. The most common bus system in use is the Peripheral Component Interconnect (PCI) bus, but some older systems might still use Industry Standard Architecture (ISA) expansion cards.
- **System resources**—Network cards, like other devices, need IRQ and memory I/O addresses. If the network card does not operate correctly after installation, there might be a device conflict.
- **Media compatibility**—Today, the assumption is that networks use twisted-pair cabling, so if you need a card for coaxial or fiber-optic connections, you must specify this. Wireless network cards are also available.

ISDN Adapters:

Integrated Services Digital Network (ISDN) is a remote access and WAN technology that can be used in place of a Plain Old Telephone Service (POTS) dial-up link if it is available. The availability of ISDN depends on whether your local telecommunications service provider offers the service, the quality of the line to your premises, and your proximity to the provider's location. ISDN offers greater speeds than a modem and can also pick up and drop the line considerably faster. If ISDN is available and you do elect to use it, a special device called an ISDN terminal adapter is needed to connect to the line.

ISDN terminal adapters can be add-in expansion cards, external devices that connect to the serial port of the system, or specialized interfaces built in to routers or other networking equipment. The ISDN terminal adapter is necessary because, although it uses digital signals, the signals are formatted differently from those used on a LAN. In addition, ISDN can create multiple communication channels on a single line. Today, ISDN is not widely deployed and has been replaced by faster and often cheaper technologies.

Wireless Access Points:

Wireless access points (APs) are a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). APs are typically a separate network device with a built-in antenna, transmitter, and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. APs also typically have several ports allowing a way to expand the network to support additional clients.

Modem:

Most everyone wants to connect to the internet. A broadband modem is used to take a high speed Internet connection provided by an ISP (Internet Service Provider) and convert the data into a form that your local network can use. The high speed connection can be DSL (Digital Subscriber Line) from a phone company or cable from a cable television provider.

In order to be reached on the Internet, your computer needs a unique address on the internet. Your ISP will provide this to you as part of your Internet connection package. This address will generally not be fixed which means that they may change your address from time to time. For the vast majority of users, this makes no difference. If you have only one computer and want to connect to the Internet, you strictly speaking don't need a router. You can plug the network cable from the modem directly into the network connection of your computer. However, you are much better off connecting the modem to a router. The ip address your ISP provides will be assigned to the router.

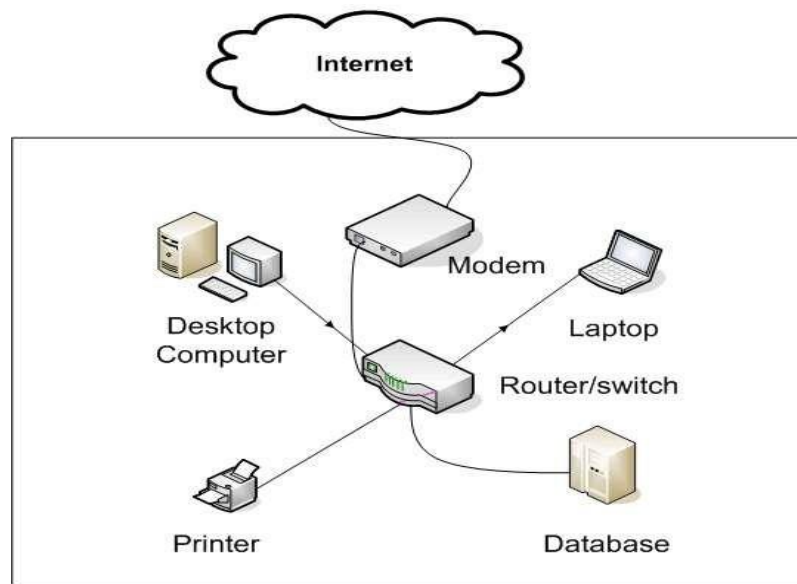


Fig. 6
Modem

The router will assign a hidden address (non routable) to each of the computers on the network. This is strong protection against hackers since they scan ip addresses for computers that are open to being attacked. The router is not a general purpose computer and will not be visible to them.

Transceivers (Media Converters):

The term transceiver does describe a separate network device, but it can also be technology built and embedded in devices such as network cards and modems. In a network environment, a transceiver gets its name from being both a transmitter and a receiver of signals—thus the name transceivers. Technically, on a LAN, the transceiver is responsible for placing signals onto the network media and also detecting incoming signals traveling through the same wire. Given the description of the function of a transceiver, it makes sense that that technology would be found with network cards. Although transceivers are found in network cards, they can be external devices as well.

As far as networking is concerned, transceivers can ship as a module or chip type. Chip transceivers are small and are inserted into a system board or wired directly on a circuit board. Module transceivers are external to the network and are installed and function similarly to other computer peripherals, or they can function as standalone devices.

Firewalls:

A firewall is a networking device, either hardware or software based, that controls access to

your organization's network. This controlled access is designed to protect data and resources from an outside threat. To do this, firewalls are typically placed at entry/exit points of a network—for example, placing a firewall between an internal network and the Internet. Once there, it can control access in and out of that point.

Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network—for example, placing a firewall between the Accounts and the Sales departments.

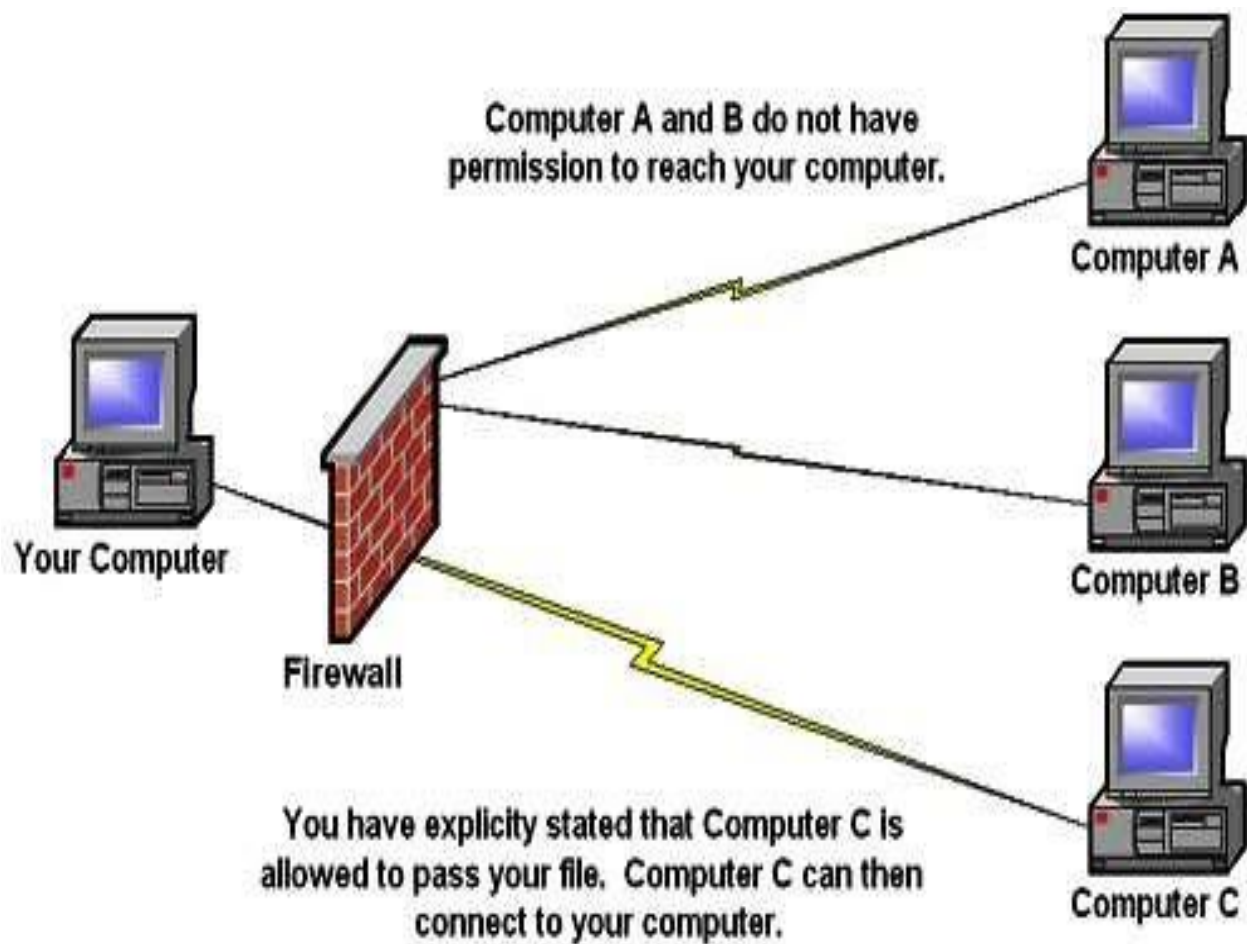


Fig. 7 Firewall

MAC Addresses:

A MAC address is a unique 6-byte address that is burned into each network interface or more specifically, directly into the PROM chip on the NIC. The number must be unique, as the MAC address is the basis by which almost all network communication takes place. No matter which networking protocol is being used, the MAC address is still the means by which the network interface is identified on the network. Notice that I say network interface. That's very important, as a system that has more than one network card in it will have more than one MAC address.

MAC addresses are expressed in six hexadecimal values. In some instances, the six values are separated by colons (:); in others, hyphens (-) are used; and in still others, a space is simply inserted between the values. In any case, because the six values are hexadecimal, they can only be numbers 0–9 and the letters A–F.

PRACTICAL: 3

AIM: Study of Different Commands: Ping, Ip Config, Tcpdump and Traceroute.

The study of these essential networking commands, understanding their functionalities, and how they are used in troubleshooting and analyzing network-related issues.

1. Ping

Description:

- **Ping** (Packet Internet Groper) is a networking utility used to test the reachability of a host on an Internet Protocol (IP) network.
- It sends ICMP (Internet Control Message Protocol) Echo Request messages to the target host and waits for ICMP Echo Reply messages to verify the network connectivity.

Usage:

- `ping [hostname or IP address]`

Features:

- **Reachability Testing:** Determines if a remote host is reachable over the network.
- **Round-Trip Time (RTT):** Measures the time taken for a packet to travel from the source to the destination and back.
- **Packet Loss:** Indicates the percentage of packets lost during transmission.

Applications:

- Network diagnostics
- Troubleshooting connectivity issues
- Monitoring network performance

2. IpConfig (Windows) / IfConfig (Unix/Linux)

Description:

- **IpConfig** (Windows) and **IfConfig** (Unix/Linux) are command-line utilities that display the current configuration and status of network interfaces on a system.
- They provide detailed information about IP addresses, subnet masks, default gateways, and other network settings.

Usage:

- `ipconfig` (Windows)
- `ifconfig` (Unix/Linux)

Features:

- **IP Address:** Displays the IPv4 and/or IPv6 addresses assigned to network interfaces.
- **Subnet Mask:** Shows the subnet mask used to identify the network portion of an IP address.

- **Default Gateway:** Indicates the IP address of the default gateway used for routing traffic.
- **DNS Servers:** Lists the IP addresses of DNS servers configured on the system.

Applications:

- Network configuration
- Troubleshooting network connectivity
- Diagnosing network-related issues

3. Tcpdump

Description:

- **Tcpdump** is a powerful command-line packet analyzer that captures and displays network traffic on a system.
- It supports filtering and analyzing packets based on various criteria, such as protocol type, source/destination IP addresses, port numbers, and more.

Usage:

- `tcpdump [options] [filter expression]`

Features:

- **Packet Capture:** Captures network packets in real-time or from a saved capture file.
- **Protocol Analysis:** Filters and analyzes packets based on specific protocols (e.g., TCP, UDP, ICMP).
- **Packet Filtering:** Uses BPF (Berkeley Packet Filter) syntax to filter packets based on custom criteria.
- **Verbose Output:** Provides detailed information about captured packets, including headers, payload, and timestamp.

Applications:

- Network monitoring and analysis
- Troubleshooting network issues
- Security analysis and intrusion detection

4. Traceroute (Tracert on Windows)

Description:

- **Traceroute** (or **Tracert** on Windows) is a network diagnostic tool used to trace the path that packets take from the source to the destination host.
- It sends ICMP or UDP packets with increasing TTL (Time-To-Live) values to identify the routers or hops along the route to the target host.

Usage: `traceroute [hostname or IP address]` (Unix/Linux)

- `tracert [hostname or IP address]` (Windows)

Features:

- **Hop-by-Hop Analysis:** Identifies each router or hop along the path to the destination host.
- **Round-Trip Time (RTT):** Measures the time taken for packets to reach each hop and return to the source.
- **Packet Loss:** Indicates if any routers are dropping packets along the route.
- **DNS Resolution:** Resolves IP addresses and hostnames for each hop.

Applications:

- Network path analysis
- Identifying network bottlenecks
- Troubleshooting latency and routing issues

Conclusion

Understanding the functionalities and usage of these essential networking commands is crucial for network administrators, IT professionals, and anyone involved in managing or troubleshooting computer networks. Whether you're diagnosing connectivity problems, analyzing network traffic, or optimizing network performance, these commands provide valuable insights and tools to ensure reliable and efficient network operations. Mastery of these commands will empower you to effectively manage, monitor, and troubleshoot networks, enhancing your skills and expertise in the field of networking.

PRACTICAL: 4

AIM: Configure and secure a basic networking device for telnet access

To secure Telnet, it is essential to understand the basics of networking devices and their configuration. Here's a summary of the key points:

Networking Devices:

Switches: Connect multiple devices within a network, allowing them to communicate with each other. They operate at the data link layer of the OSI model.

Routers: Connect multiple networks together, routing data packets between them. They operate at the network layer of the OSI model.

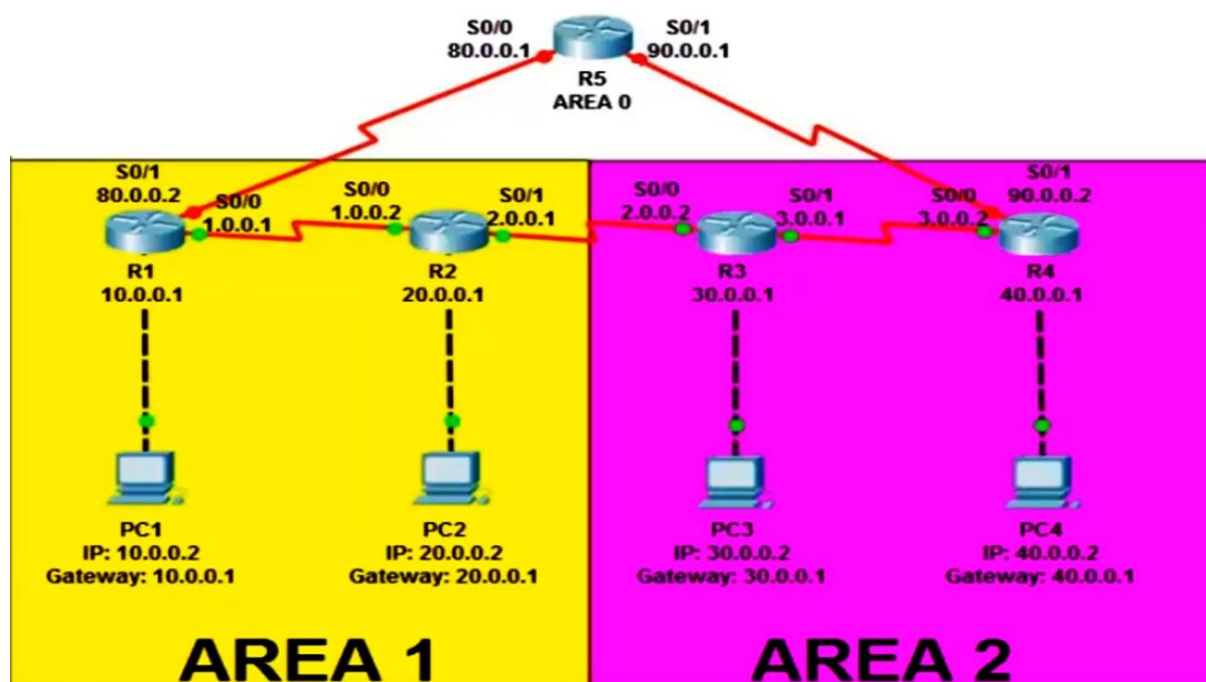
Access Points: Allow devices to connect to a wireless network without cables.

Securing Telnet:

Disable Unencrypted Remote Admin Protocols: Disable Telnet and other unencrypted remote admin protocols (e.g., FTP) to prevent unauthorized access to your network infrastructure.

Implement Role-Based Access Control: Assign access rights based on role, location, and other factors to ensure the right level of access is given to the right people and devices.

Use Secure Protocols: Use secure protocols like SSH (Secure Shell) instead of Telnet for remote access to your network devices.



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty ?
    <0-15>  First Line number
Router(config)#line vty 0 15
Router(config-line)#password ccna
Router(config-line)#login
Router(config-line)#enable secret cisco
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
C:\>telnet 3.0.0.2
Trying 3.0.0.2 ...Open

User Access Verification

Password:
Router>en
Password:
Router#show protocol
Global values:
    Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
    Internet address is 40.0.0.1/8
Serial10/0 is up, line protocol is up
    Internet address is 3.0.0.2/8
Serial10/1 is up, line protocol is up
    Internet address is 90.0.0.2/8
```

Additional Tips:

Regularly Update Firmware and Software: Keep your networking devices' firmware and software up-to-date to ensure you have the latest security patches and features.

Monitor Network Traffic: Monitor network traffic to detect and respond to potential security threats.

Implement Firewalls and VPNs: Use firewalls and VPNs to protect your network from unauthorized access and data breaches.

PRACTICAL: 5

AIM: Configure switch and router ports and IP route.

To configure a switch and router for IP routing, you'll need to follow these steps:

Step 1: Enable IP routing on the router:

To enable IP routing on the router, you'll need to access the router's configuration mode and enter the command `ip routing`. This will allow the router to forward IP packets between different networks.

Step 2: Create the SVI interface or navigate to configuration mode for the interface:

To create a Switched Virtual Interface (SVI) or navigate to configuration mode for the interface, you'll need to enter the command `switch #no switchport`. This will allow you to configure the interface as a routed port.

Step 3: Assign an IP address to the SVI for the VLAN:

To assign an IP address to the SVI for the VLAN, you'll need to enter the command `switch #ip address n.n.n.n subnet-mask`. Replace `n.n.n.n` with the desired IP address and `subnet-mask` with the subnet mask.

Step 4: Specify an IP routing protocol:

To specify an IP routing protocol, you'll need to enter the command `switch #router ip routing_protocol <options>`. This will allow the router to exchange dynamic routing updates with other routing devices. The routing protocol specified may require additional options. Refer to the documentation for the routing protocol for further details.

Step 5: Configure the switch management interface:

To configure the switch management interface, you'll need to enter the command `S1(config)# interface vlan 99`. This will allow you to configure the interface as a management interface.

Step 6: Save the running config to the startup config:

To save the running config to the startup config, you'll need to enter the command `S1# copy running-config startup-config`. This will save the current configuration to the startup configuration file.

Step 7: Configure password for console, Telnet, and aux ports:

To configure the password for console, Telnet, and aux ports, you'll need to enter the command `switch(config)# enable secret password`. Replace `password` with the desired password.

Step 8: Verify the IP route:

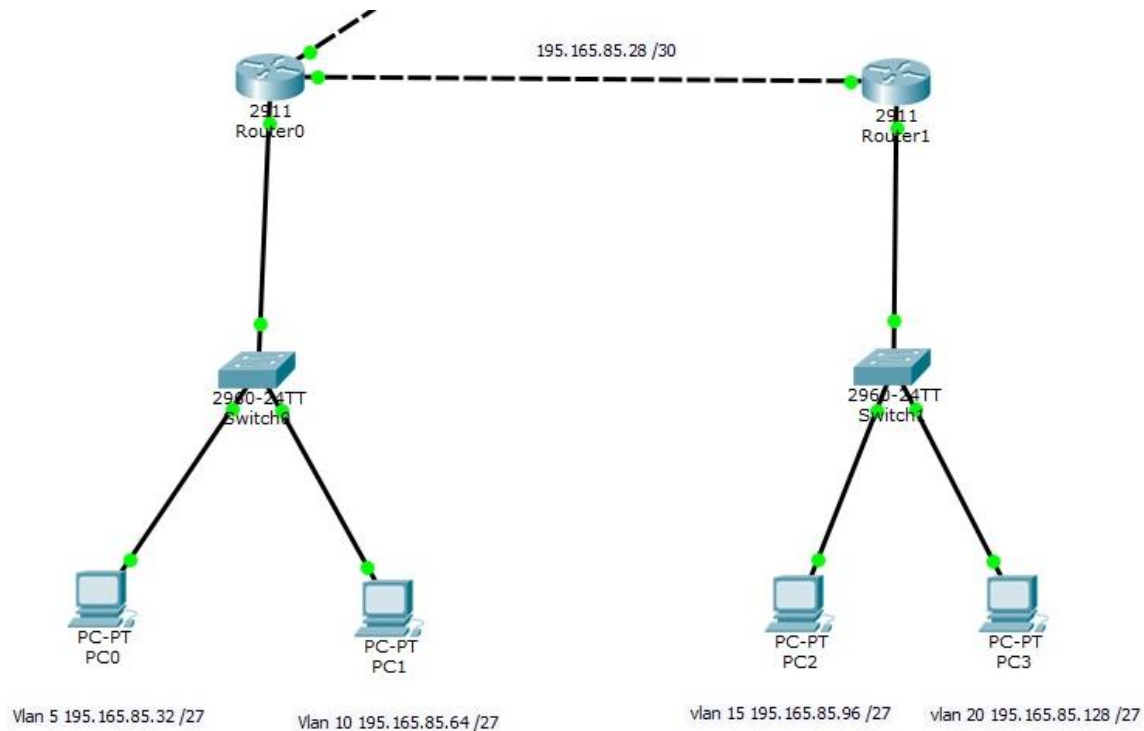
To verify the IP route, you'll need to enter the command `switch# show ip route`. This will display the current IP routing table.

Step 9: Configure the router's default gateway:

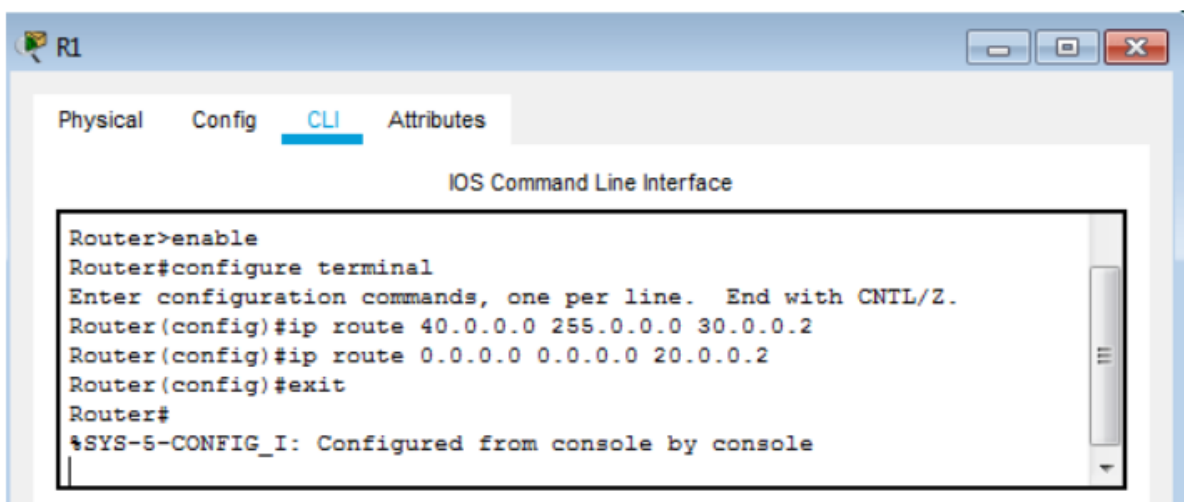
To configure the router's default gateway, you'll need to enter the command `switch(config)# ip default-gateway 172.16.29.1`. Replace 172.16.29.1 with the desired default gateway IP address.

Step 10: Verify the default gateway:

To verify the default gateway, you'll need to enter the command `switch# show ip route`. This will display the current IP routing table and the default gateway.



```
Router(config)#ip route 40.0.0.0 255.0.0.0 30.0.0.2
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
```



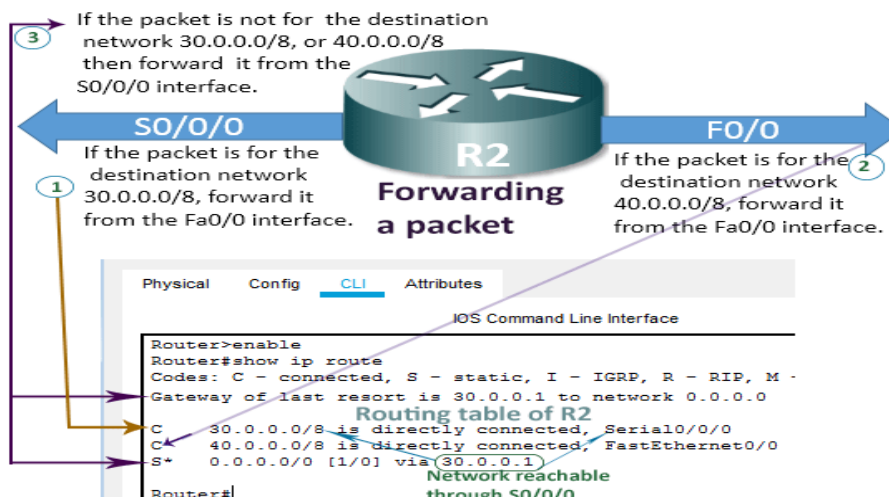
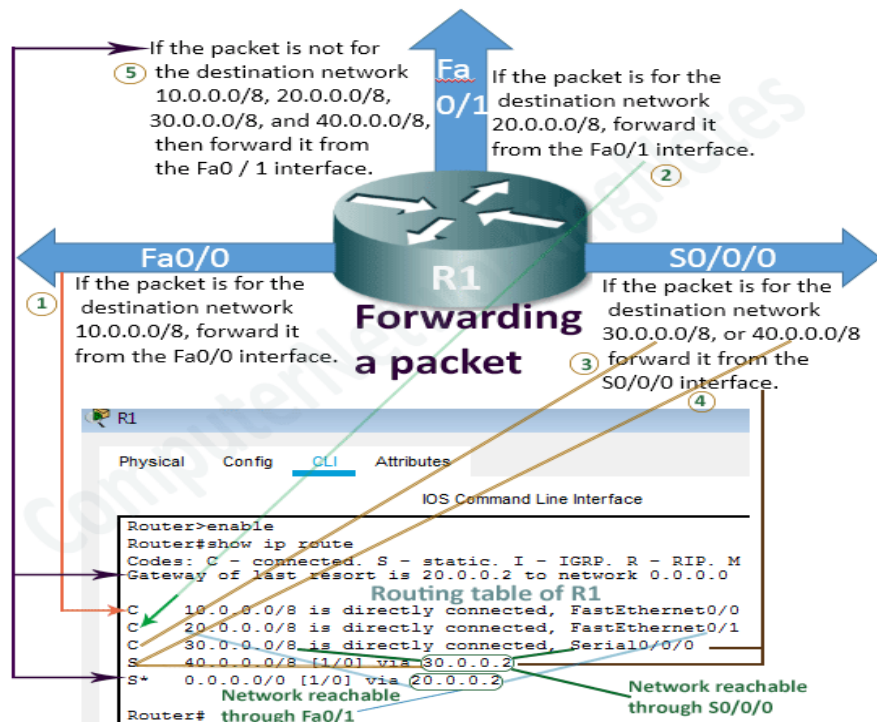
```
Router(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1
```

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```



PC0 IP configuration 10.0.0.2
of the PC0 is 255.0.0.0

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 40.0.0.2

Pinging 40.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 40.0.0.2: bytes=32 time=6ms TTL=126
Reply from 40.0.0.2: bytes=32 time=11ms TTL=126
Reply from 40.0.0.2: bytes=32 time=13ms TTL=126
Verifies that the network 40.0.0.0/8 is accessible
Ping statistics for 40.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 13ms, Average = 10ms

C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time=1ms TTL=127
Verifies that the network 20.0.0.0/8 is accessible
Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

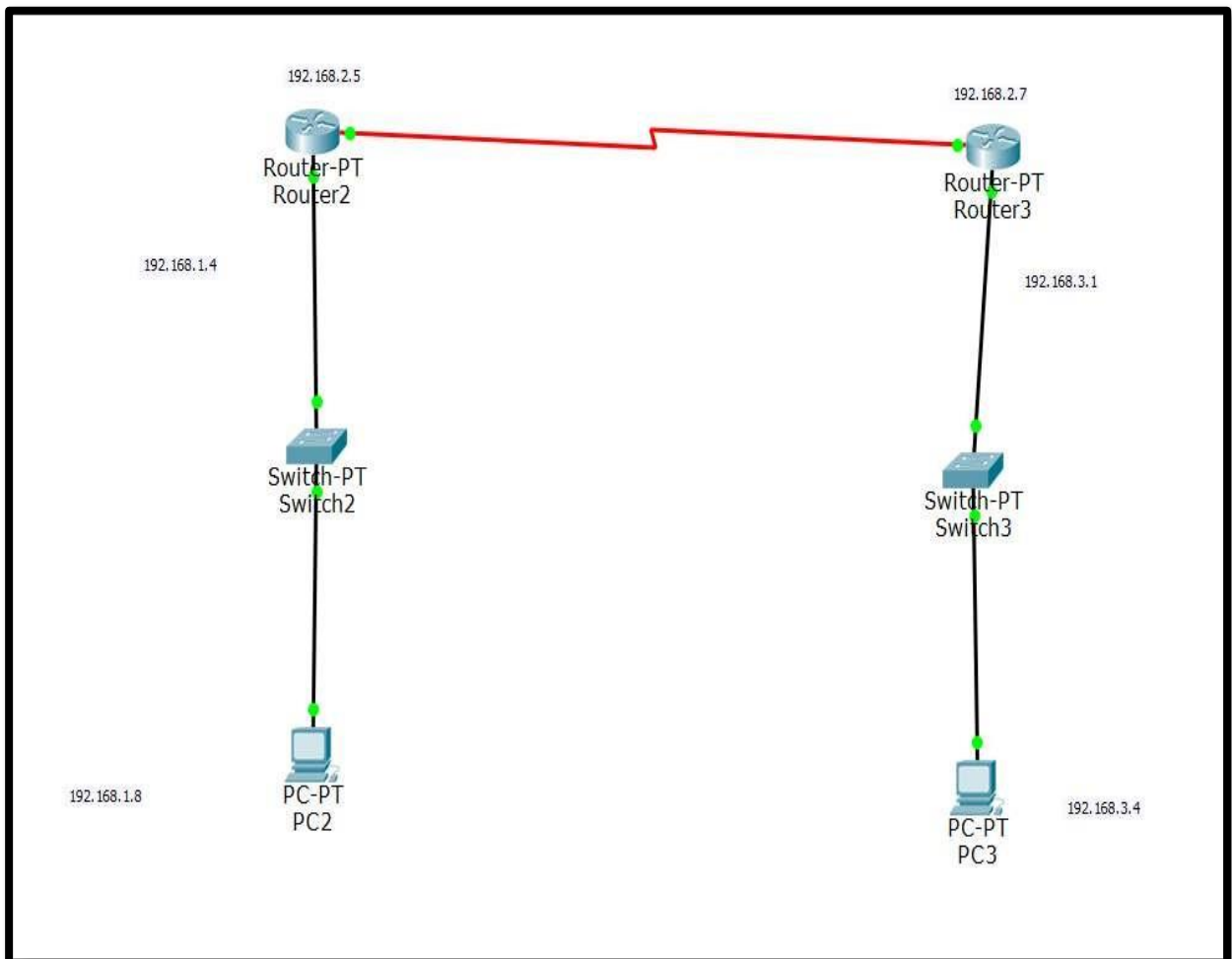
PRACTICAL: 6

AIM: Implement the concept of static routing.

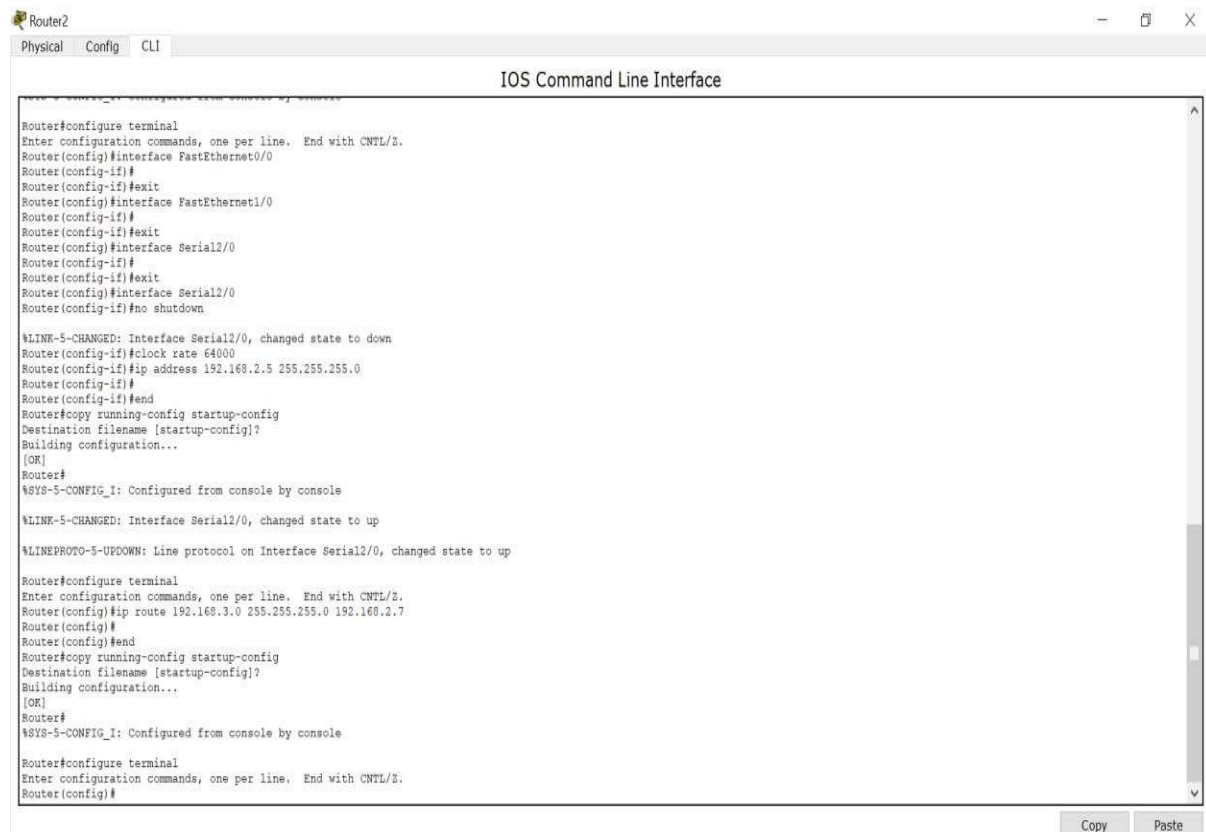
Static routing: -

Static routing is a form of routing that occurs when a router uses a manually- configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table , though this may not always be the case. Unlike dynamic routing , static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks or to provide a gateway of last resort.

Practical Implementation in Cisco Student.



Routing Configuration (Static)



Router2

Physical Config CLI

IOS Command Line Interface

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#no shutdown

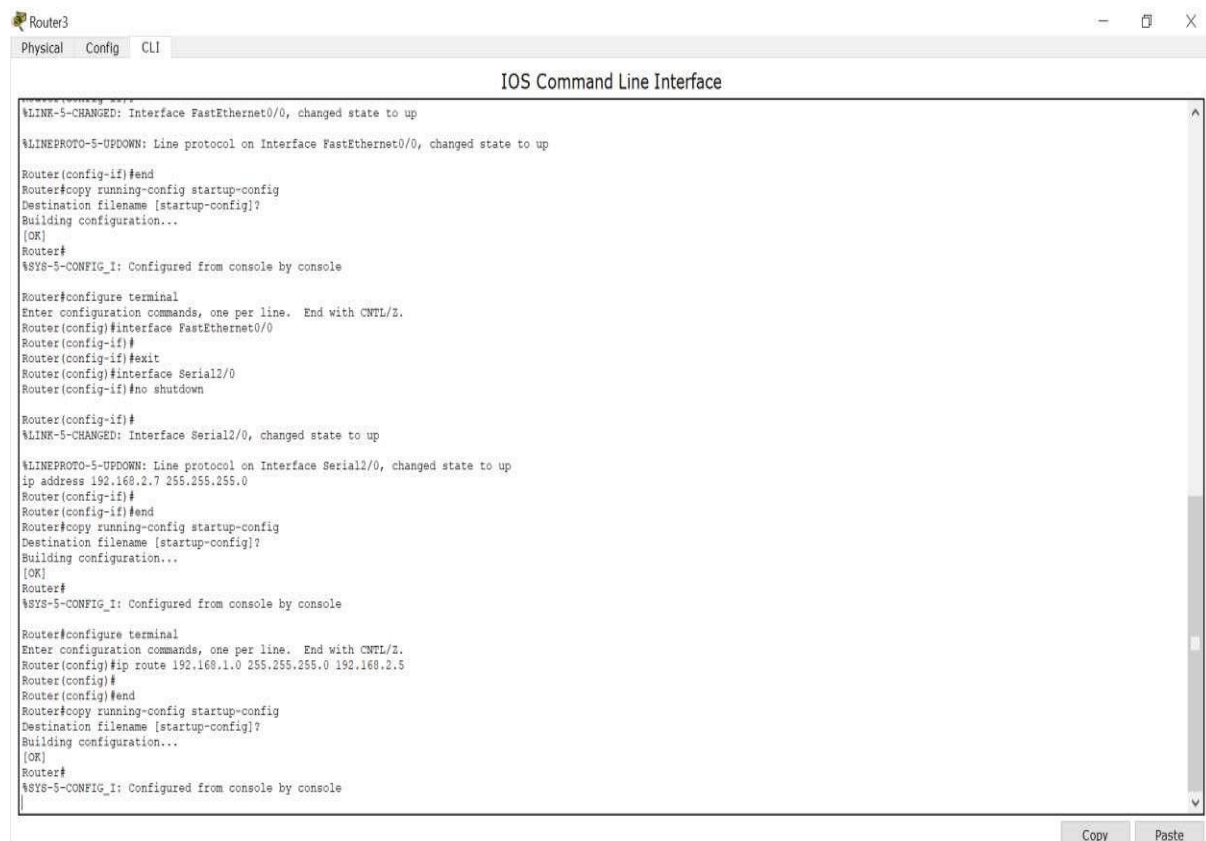
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Router(config-if)#clock rate 64000
Router(config-if)#ip address 192.168.2.5 255.255.255.0
Router(config-if)#
Router(config-if)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.7
Router(config)#
Router(config)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Copy Paste



Router3

Physical Config CLI

IOS Command Line Interface

```
%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)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

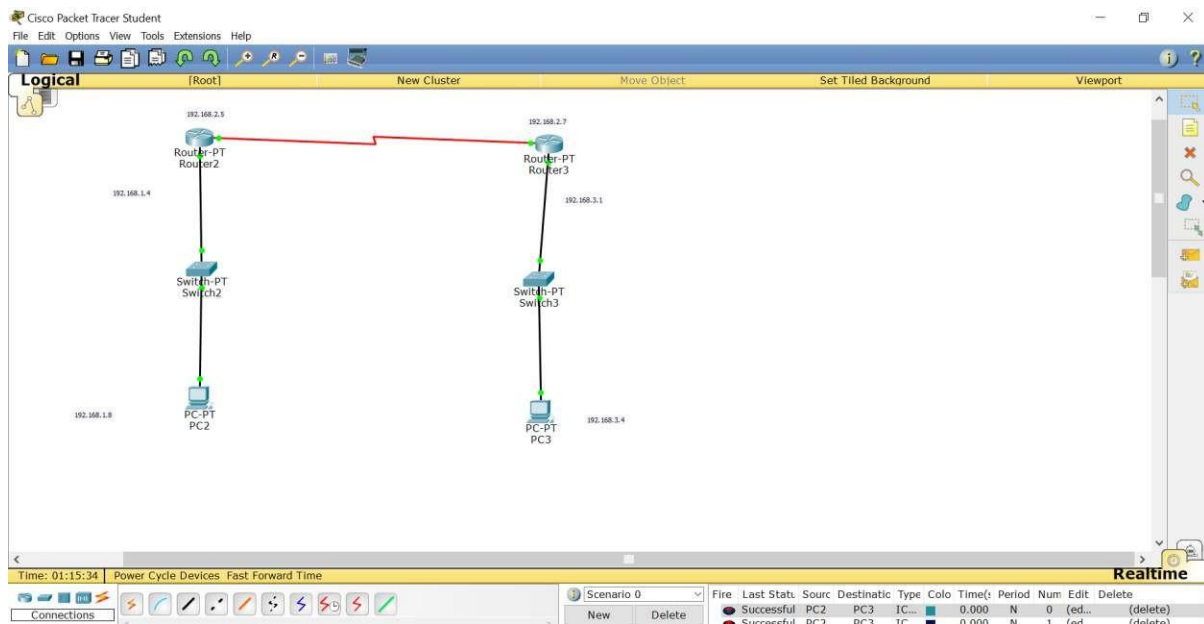
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
ip address 192.168.2.7 255.255.255.0
Router(config-if)#
Router(config-if)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.5
Router(config)#
Router(config)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

Packet transfer: -



Here we can see that packet is successfully transfer from PC2 to PC3.

PRACTICAL: 7

AIM: Configure a network using distance vector routing protocol.

To configure a network using a distance vector routing protocol using Cisco packet computer network practical, you will need to follow these steps:

Step 1: Configure the routers:

Configure the routers with the necessary information, such as IP addresses, subnet masks, and default gateways. You can use the Cisco packet computer network practical to configure the routers.

Step 2: Configure the distance vector routing protocol:

Configure the distance vector routing protocol on each router. For example, you can use the RIP (Routing Information Protocol) or IGRP (Interior Gateway Routing Protocol) protocol.

Step 3: Set the update interval:

Set the update interval for the distance vector routing protocol. This determines how often the routers will send routing updates to each other.

Step 4: Configure the metric:

Configure the metric for the distance vector routing protocol. This determines how the routers will calculate the best path to a destination network.

Step 5: Verify the configuration:

Verify the configuration by checking the routing tables on each router to ensure that the routers are advertising the correct routes and that the best path to each destination network is being used.

Here is an example of how you might configure a network using RIP and IGRP:

Router 1:

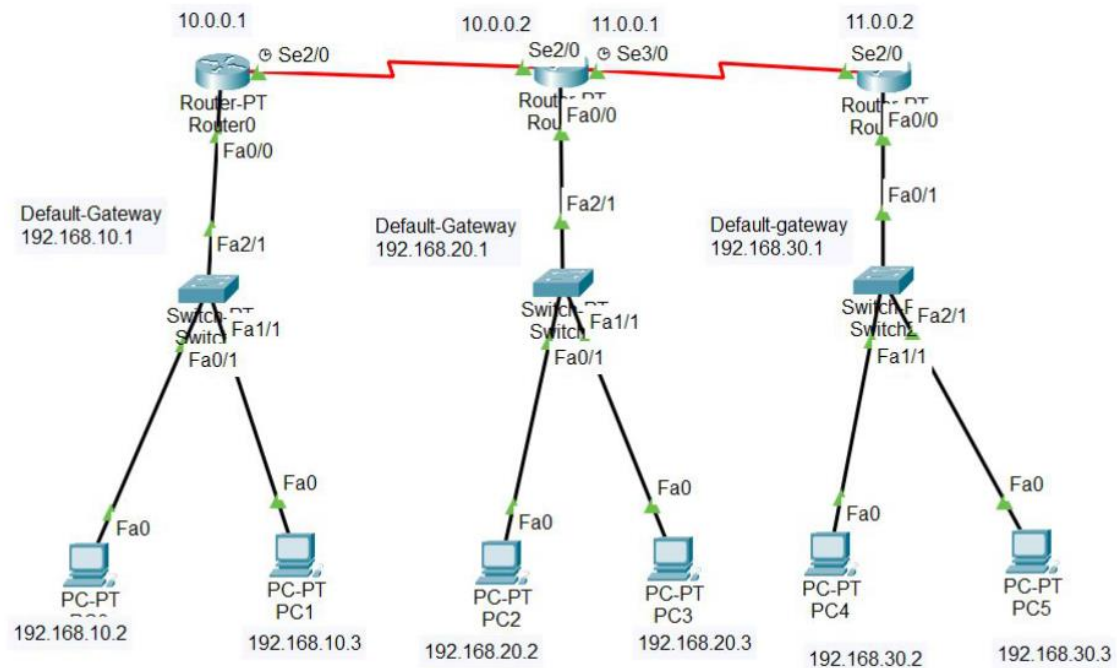
```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# metric 1
Router(config-router)# update-interval 30
```

Router 2:

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# metric 1
Router(config-router)# update-interval 30
```

Router 3:

```
Router(config)# router igrp 100
Router(config-router)# network 10.0.0.0
Router(config-router)# metric 1
Router(config-router)# update-interval 90
```



In this example, Router 1 and Router 2 are configured to use RIP, and Router 3 is configured to use IGRP. The update interval for RIP is set to 30 seconds, and the metric is set to 1. The update interval for IGRP is set to 90 seconds, and the metric is also set to 1.

PRACTICAL: 8

AIM: Configure a link-state vector routing protocol.

To configure a network using Link State Vector (LSV) routing protocol on a Cisco packet computer network, you can follow these steps:

Step 1: Enable OSPF (Open Shortest Path First) protocol

On the Cisco router, enter the configuration mode by typing `enable` and then `config t`.

Type `router ospf <process-id>` to enable OSPF, replacing `<process-id>` with a unique identifier for the OSPF process.

Set the router ID by typing `router-id <router-id>`.

Step 2: Define the network

Define the network by typing `network <network-id> <wildcard-mask>`.

Step 3: Configure the interface

Configure the interface by typing `interface <interface-name>` and then `ip address <ip-address> <subnet-mask>`.

Enable OSPF on the interface by typing `ip ospf <process-id> area <area-id>`.

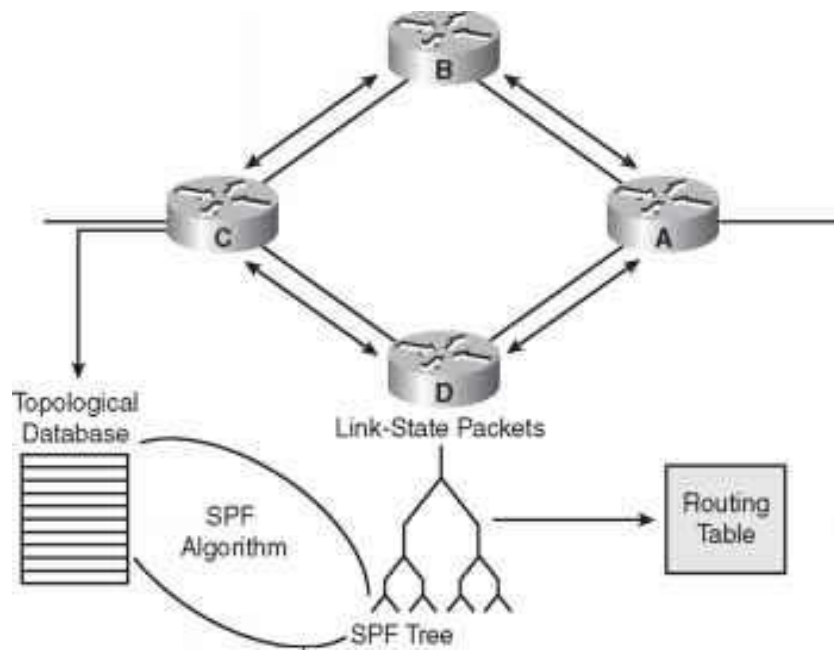
Step 4: Verify the configuration

Verify the configuration by typing `show ip ospf` to display the OSPF process information.

Verify the network topology by typing `show ip route` to display the routing table.

Here is an example configuration:

```
Router# enable
Router(config)# router ospf 1
Router(config-router)# router-id 192.168.1.1
Router(config-router)# network 10.10.1.0 0.0.0.255 area 0
Router(config-router)# interface FastEthernet0/0
Router(config-if)# ip address 10.10.1.1 255.255.255.0
Router(config-if)# ip ospf 1 area 0
Router(config-if)# end
Router# show ip ospf
Router# show ip route
```



Additional Information:

Link State Vector (LSV) routing protocol is a type of link-state routing protocol that uses a link-state database to build the routing table.

OSPF is a popular link-state routing protocol used in many networks.

The `show ip ospf` command displays information about the OSPF process, including the router ID, process ID, and area ID.

The `show ip route` command displays the routing table, including the routing information learned through OSPF.