

Practical No. 1:

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

Solution:

Apparatus (Components):

RJ-45 connector, Crimping Tool, Twisted pair Cable

Procedure:

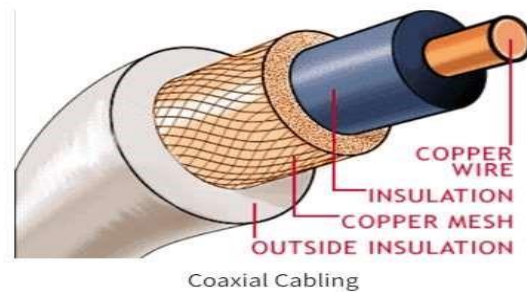
To do these practical following steps should be done:

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.

Description:

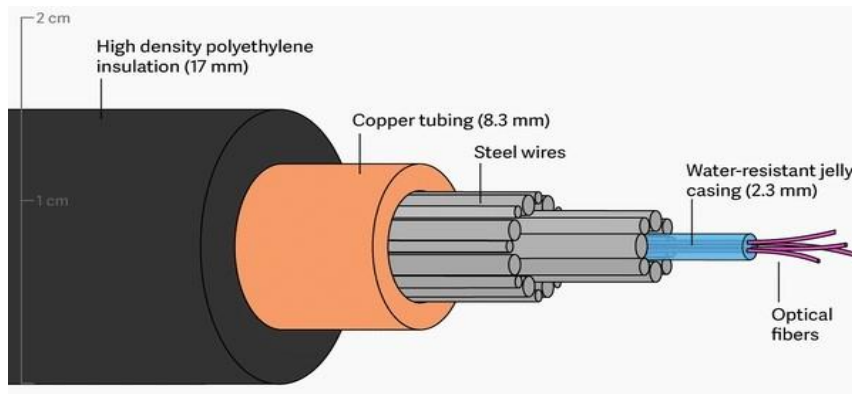
Coaxial cabling:

- Coaxial Cable is a standard for 10 Mbps Ethernet cables.
- These types of cables consist of an inner copper wire cover with insulation and another shielding.
- It has a plastic layer that offers insulation between the braided metal shield and center conductor.
- Coaxial cabling has a single copper conductor in its center.
- Types of Coaxial Cable are 1) RG58 2) RG8 3) RG6 4) RG59



Fiber-optic cabling:

- Fiber optic cables mostly consist of a center glass, and different layers of protective materials surround it.
- Fiber-optic cabling transmits light in place of electronic signals, which removes the issue of electrical interference.
- This makes it an ideal selection for the environments that contain a large amount of electrical interference.
- This type of network cable offers an ability to transmit signals over longer distances.
- It also provides the ability to carry information at faster space.

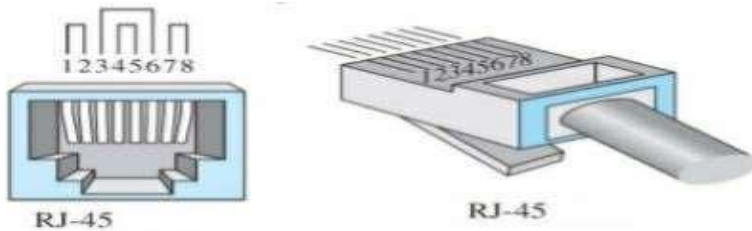


Two types of fiber-optic cables are:

- Single-mode fiber (SMF)–This type of fiber optic cable uses only a single ray of light to carry data. Used for larger distance wiring.
- Multi-mode fiber (MMF)–This type of fiber-optic uses multiple rays of light to carry data. Less expensive than SMF.
- Four types of connectors in network that are mostly used for fiber optic cable are:
 1. ST (Straight-tip Connector)
 2. SC (Subscriber Connector)
 3. FC (Fiber Channel)
 4. LC (Lucent Connector) Crimping Tool:



RJ-45:



Ethernet Cables & Types:

Ethernet Cables:

- Ethernet cables are forms of network cables that are utilized on connected networks.
- They were created to link network devices.
- These cables come in all sizes. Based on your need you can get whatever length you want.
- Ethernet cables are mostly used to connect devices located on LAN systems, such as routers, PCs, and switches.

Ethernet Cable Categories:

- There are many Ethernet cable options available, and each one of them has its unique purpose and use.
- You need to choose the higher quality cable, which will be stronger, faster, and a better fit for your specific needs.
- However, depending on your hardware, you can select your below-given Ethernet cabling category.

Category-3:

- Cat3 cable is an earlier generation of cable, which supports a maximum frequency of 16 MHz
- This cable may have 2, 3, or 4 copper pairs.

- Cat3 type of Ethernet cable is still used for two-line telephone systems and 10BASE-T networks.
- It is also used for alarm system installation or similar kinds of applications.

Category-5:

- These cables are slower compared to modern-day hardware requirements.
- You should use this type of Cable only if you have older hardware that demands outdated hardware.

Category-5e:

- Cat5e is one of the most popular cabling types of an Ethernet cable used for deployments because of its ability to support Gigabit speeds at a cost-effective price.
- Cat 5e can support up to 1000 Mbps speeds, which is flexible enough for small space installations. Therefore, it is widely used in residential areas. Cat5e is one of the least expensive cabling options available in the market.

Category-6:

- Cat6 cabling support up to 10 Gbps and frequencies of up to 250 MHz
- These types of cables are more tightly twisted and feature two or more twists per centimeter.
- It only supports 37-55 meters when transmitting 10 Gbps speeds.

Category-6a:

- Cat6a Ethernet cable supports bandwidth frequencies of up to 500 MHz
- Cat6a cabling is thicker compared to Cat6, making it less flexible. That is why it is more suited for industrial environments at a lower price point.

Category Cable Wiring



Ethernet cable Categories and pinouts

Category-7:

- Cat7 has the ability to transmit up to 40 GB at 50 meters and 100 GB at 15 meters.
- This type of Ethernet cable offers extensive shielding to decrease signal attenuation.
- It is relatively stiff in comparison to previous generations of cabling.
- Cat7 type of Cable is suited for use in Datacenters and large enterprise networks.
- However, Cat7 has not been approved as a cable standard for telecommunications.

Category-8:

- Category 8 cable is designed for operations of up to 2000 MHz
- CAT8 cables work with 25/40GBASE-T Gigabit Ethernet; this reduces power consumption and is designed for bandwidth-intensive data center applications.
- This type of Cable is ideal to use where the distances between units are short.
- CAT8 cables are backward compatible with previous Categories of Ethernet cables.

Practical No. 2

Study of various network devices in detail

Solution:

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.

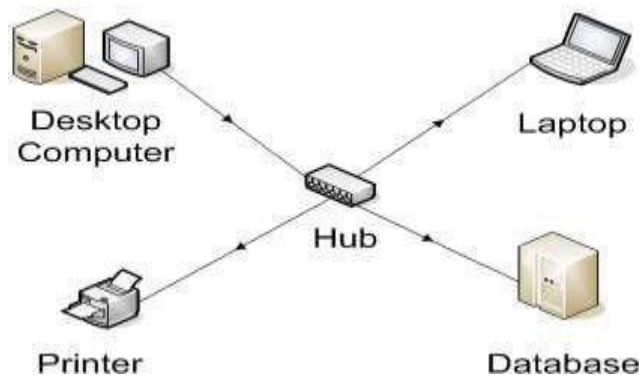


Fig.1 Hub

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.

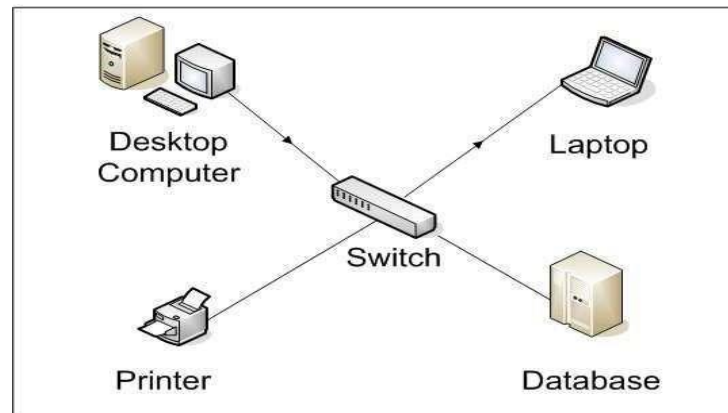


Fig. 2 Switch

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.

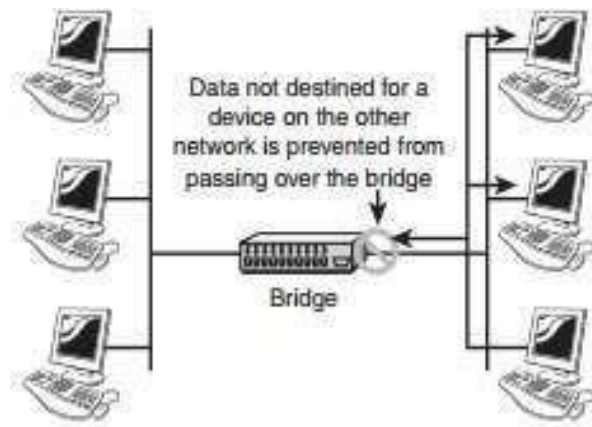


Fig 3 Bridges

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.

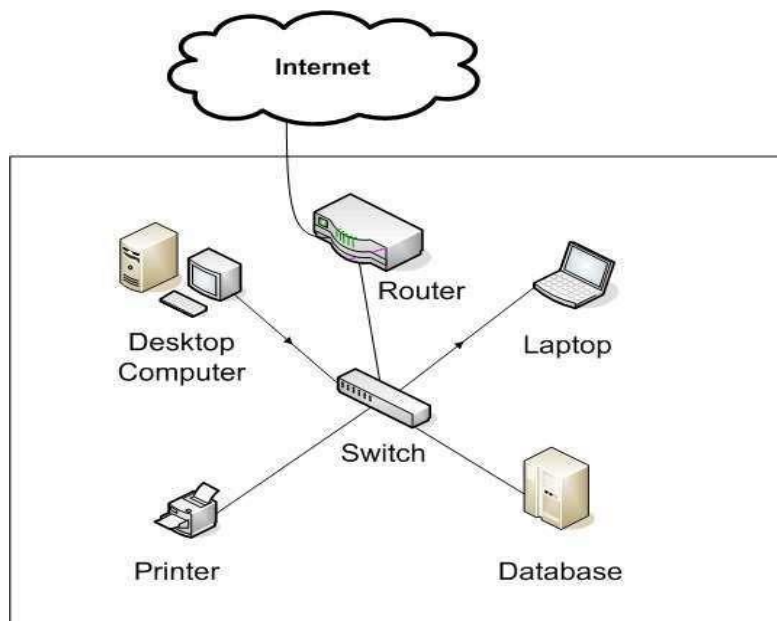


Fig. 4 Router

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.

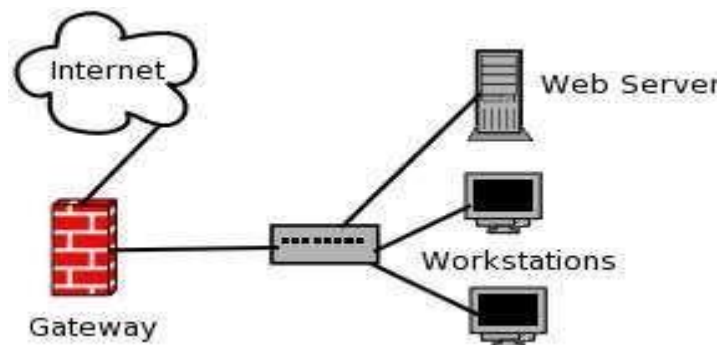


Fig. 5 Gateways

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.

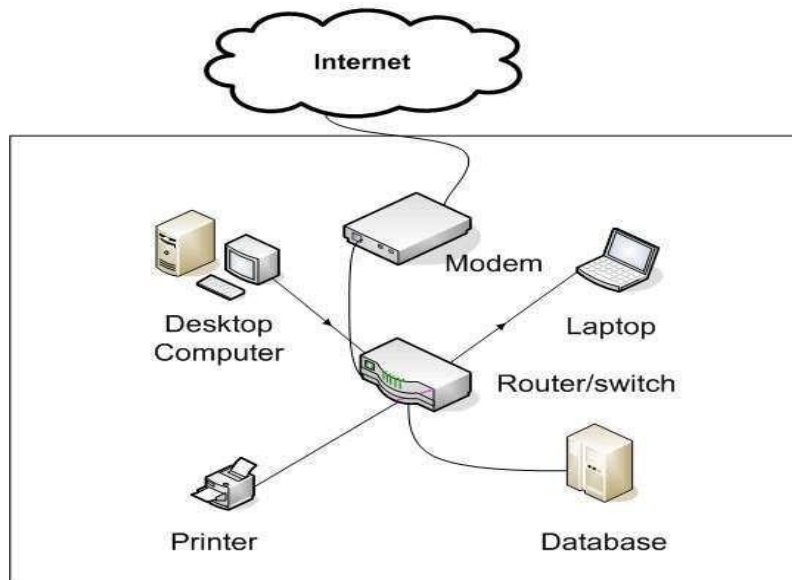


Fig. 6 Modem

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.

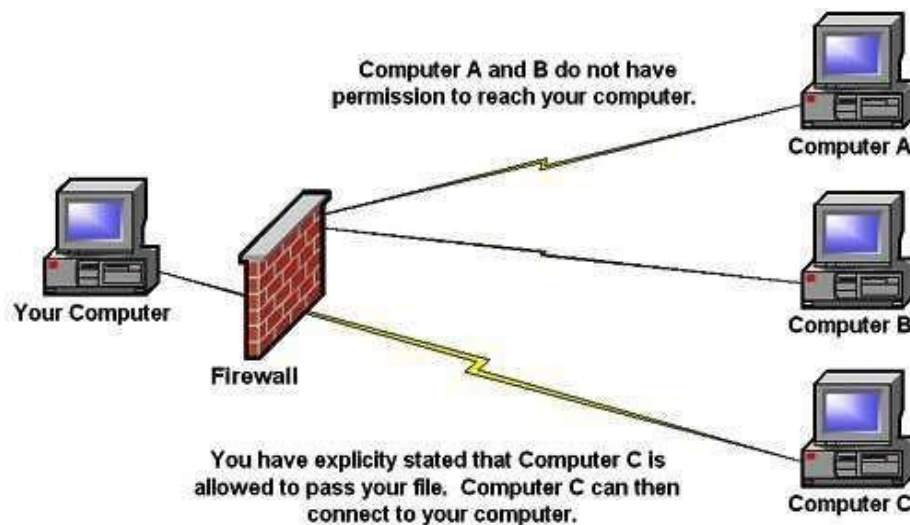


Fig. 7 Firewall

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 No. 3:

Configuration and connection of two LANs.

Solution:

Study of network IP

- Classification of IP address
- Sub netting
- Super netting

Apparatus (Software): NA

Procedure: Following is required to be study under this practical.

- Classification of IP address

As show in figure we teach how the ip addresses are classified and when they are used.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

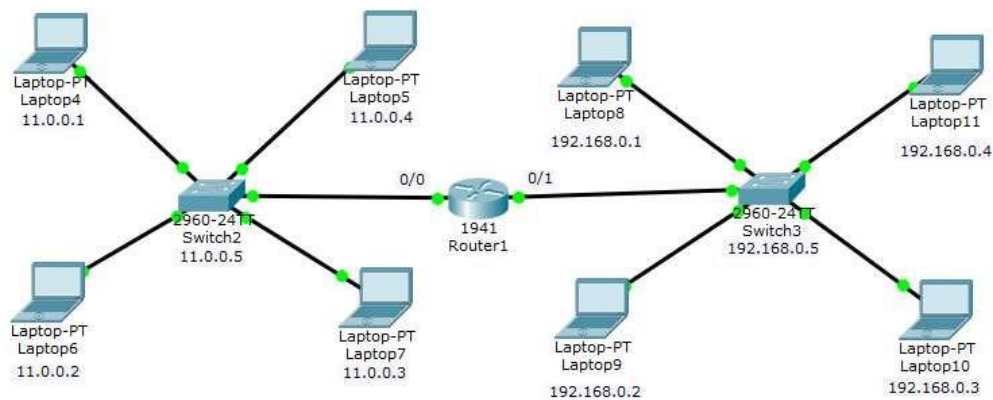
- Sub netting

Why we Develop sub netting and How to calculate subnet mask and how to identify subnet address.

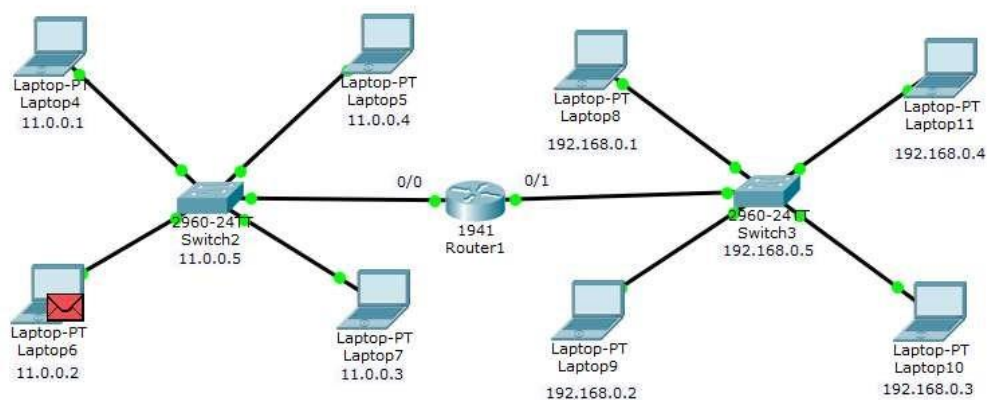
- Super netting

Why we develop super netting and How to calculate supernet mask and how to identify supernet address.

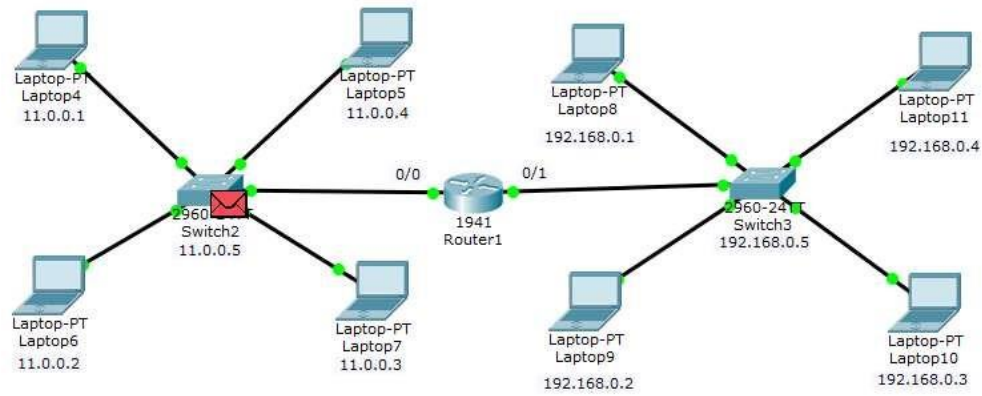
Snapshots:



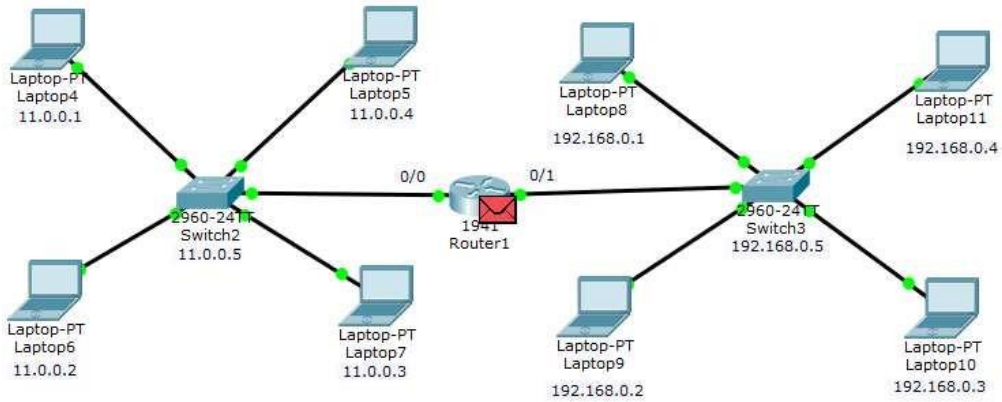
Router connecting two LANs



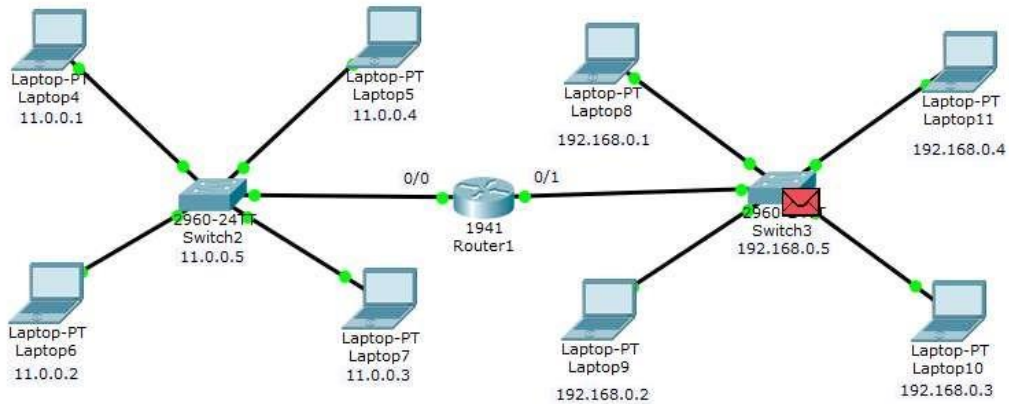
Message to be sent from Laptop-6 to Laptop-11



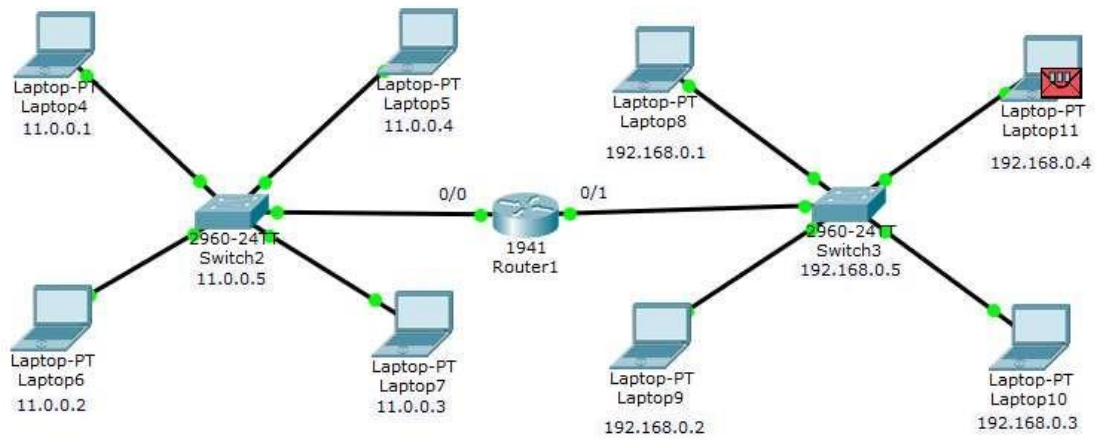
Message_sent from Laptop-6 to switch of that LAN



Message sent from switch to router as destination PC is in another LAN



Message sent from router to switch of second LAN



Message sent from switch to Laptop-11 (destination PC)

Practical No. 4

Configuration of a simple network topology using switch.

Solution: Steps to be followed on Cisco Packet Tracer

Step 1. Adding end devices for topology from bottom left corner:

- Click on End devices and select Generic PC (PC0) from second menu to immediate right. Add it to the sandbox screen.
- Similarly add one more Generic PC (PC1).
- Select Generic Laptop (Laptop0) to add laptop to your topology.
- Similarly add one more Generic Laptop (Laptop1).
- Now select a Switch (2960) from the same menu and add it to the sandbox screen.

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
Wireless Router	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

Step 2. Adding Connections between the devices:

- Click on Connections (bottom-left corner menu) and select Copper cross-over cable for wired connection.
- Now click on PC0 and select FastEthernet0 type from dropdown menu.
- Now click on Switch0 and select FastEthernet0/1 type from dropdown menu.
- Similarly create connections between PC1 and Switch0, Laptop0 and Switch0, and Laptop1 and Switch0. Use separate FastEthernet (FastEthernet 0/ 1-24) on switch for each connection.
- Fast forward time so that all connections to the router get activated (green dots) by clicking on Fast Forward Time option above menu at bottom-left corner.

Step 3. Configuring the IP settings:

- Double-Click on PC0 for configuration menu. Click on Desktop tab and select IP configuration.
- Select static option for IP settings and assign IP address to the device, for example: 10.1.1.1
- Hit Enter (Return), the subnet mask will appear automatically. Otherwise fill appropriate mask manually.
- Close the PC0 window.
- Similarly assign IP addresses to other device (PC1, Laptop0, Laptop1).
- Ensure that the devices have IP address of same class and same subnet mask.

Step 4. Sending data among the nodes:

- Click the packet icon on the right menu.
- Click on PC0 and then click PC1.
- Notification will appear at bottom-right corner for Successful transmission.

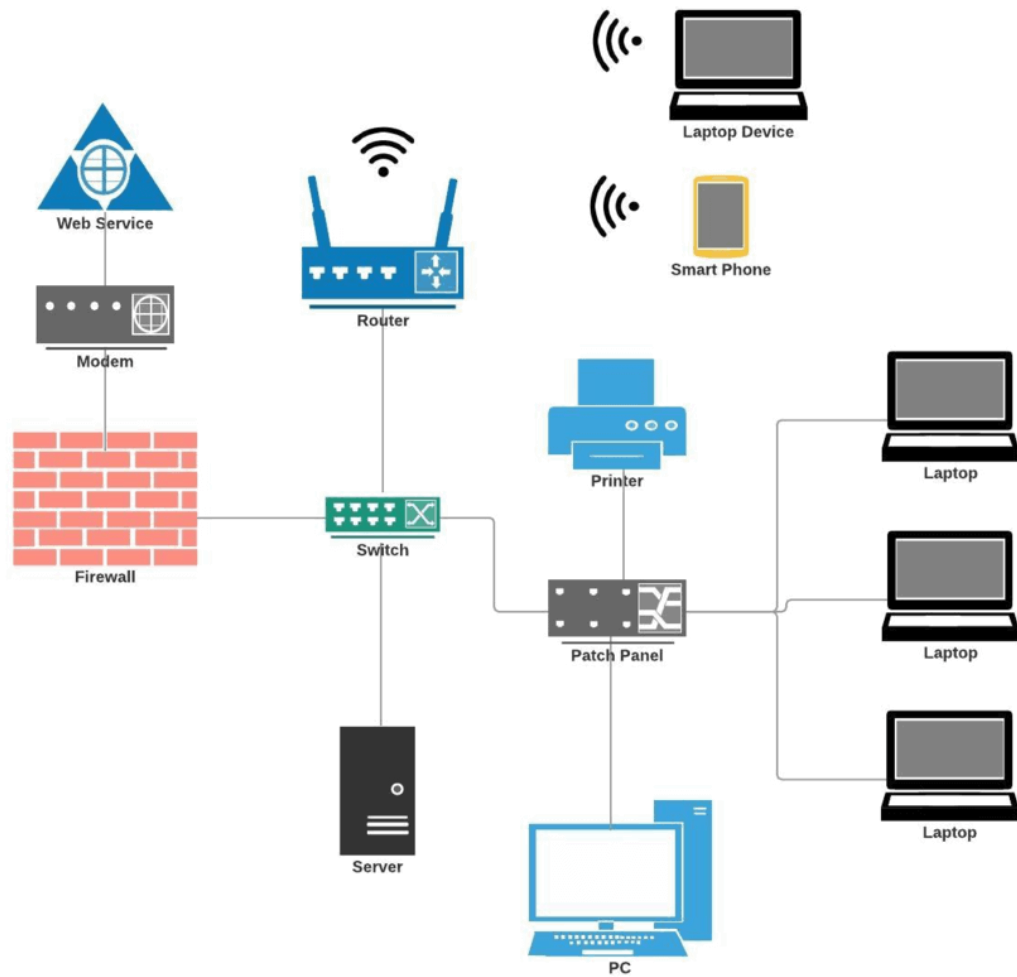


Fig. Configuration of a simple network topology using switch

Practical No. 5

Static Routing Configuration using two Routers

Solution: Steps to be followed on Cisco Packet

Tracer

Step 1: Creating topology:

- Add 2 Switches (Switch0-1).

S.NO	Device	Model Name	Qty.
1.	PC	PC	4
2.	Switch	PT-Switch	2
3.	Router	PT-Router	2

- Add 2 Routers-1841 (Router0-1).
- Connect them using Copper Straight cable.
- Add 4 Generic PCs (PC0-3). Connect PC0 and PC1 to Switch0 using Copper Straight cable and connect PC2 and PC3 to Switch1.

S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway
1.	pc0	192.168.1.2	255.255.255.0	192.168.1.1
2.	pc1	192.168.1.3	255.255.255.0	192.168.1.1
3.	pc2	192.168.2.2	255.255.255.0	192.168.2.1
4.	pc3	192.168.2.3	255.255.255.0	192.168.2.1

- Connect Switch0 to Router0 (FastEthernet0/0) and Switch1 to Router1 (FastEthernet0/0) using Copper Straight cable.
- Connect two Routers (FastEthernet0/1) using Copper crossover cable

Step 2: In PC0, go to its Desktop panel and select IP configuration. Give IP address, Subnet Mask, and Gateway. Give IP address, mask and Gateway to PC1. Do the same with another two (PC2-PC3).

- PC0-PC1: 1.0.0.1 and 1.0.0.2 resp. Mask: 255.0.0.0 Gateway: 1.0.0.5
- PC2-PC3: 3.0.0.1 and 3.0.0.2 resp. Mask: 255.0.0.0 Gateway: 3.0.0.5

Step 3: Now for Router Configuration, Click on Router1 and go to CLI tab. Press Enter and type following commands:

- Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 3.0.0.5 255.0.0.0
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)#exit

Router(config)#interface fa0/1Router(config-if)#ip address 2.0.0.1 255.0.0.0

Router(config-if)#no shutdownRouter(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state

to up □ Router(config-if)#exit

Step 4: Similarly to configure other router (Router0), type these commands:

- Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fa0/0

Router(config-if)#ip address 1.0.0.5 255.0.0.0

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)#exit

Router(config)#interface fa0/1

Router(config-if)#ip address 2.0.0.2 255.0.0.0

Router(config-if)#no shutdown

Router(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

Router(config-if)#exit

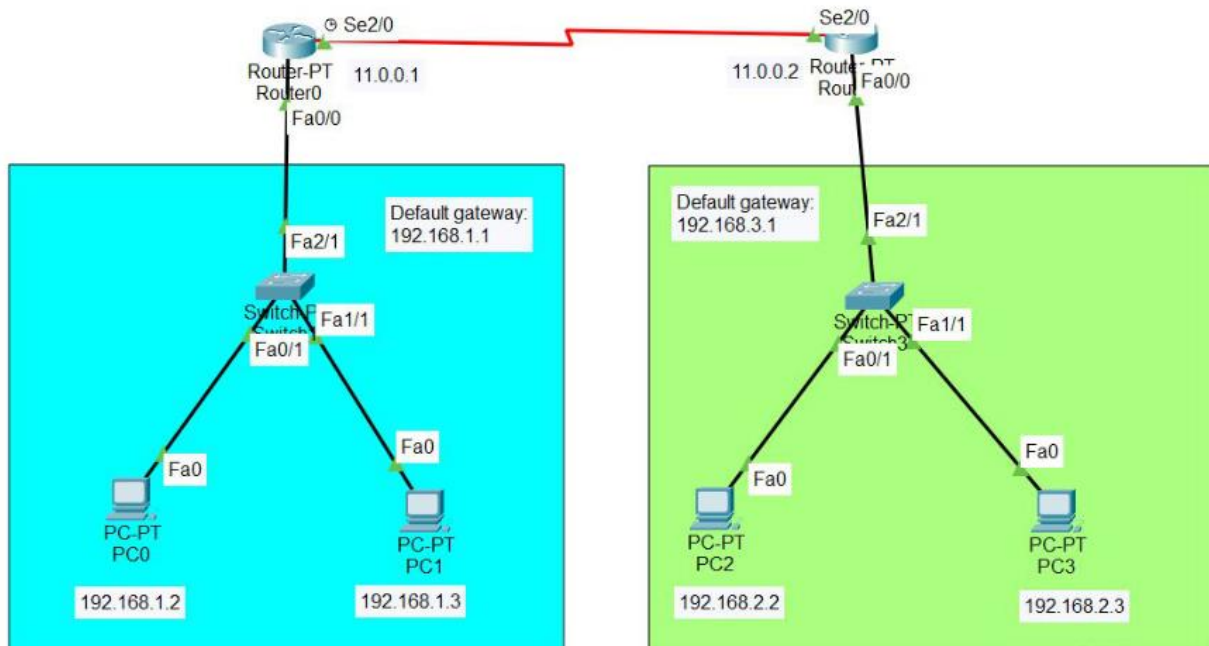
Step 6: Now go to Router1 and type

Router(config)#ip route 3.0.0.0 255.0.0.0 2.0.0.2

Step 7: Now go to other router (Router0) and type

Router(config)#ip route 1.0.0.0 255.0.0.0 2.0.0.1

Step 8: Verify connections by ping command. Select one of the devices, go to its command prompt and type ping ip-address.



Practical No. 6:

Configuration of dynamic routing.

Solution:

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) that is commonly used in internal networks. It allows the Cisco RV180/RV180W 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.

NOTE RIP is disabled by default on the Cisco RV180/RV180W.

To configure dynamic routing:

1. Choose Networking > Routing > Dynamic Routing.
2. To configure how the router sends and receives RIP packets, choose the RIP direction:
 - None—The router neither broadcasts its route table nor does it accept any RIP packets from other routers. This option disables RIP.
 - In Only—The router accepts RIP information from other router, but does not broadcast its routing table.
 - Out Only—The router broadcasts its routing table periodically but does not accept RIP information from other routers.
 - Both—The router both broadcasts its routing table and also processes RIP information received from other routers.
3. Choose the RIP version:
 - Disabled.
 - RIP-1—This is a class-based routing version that does not include subnet information. RIP-1 is the most commonly supported version.
 - RIP-2B—This version broadcasts data in the entire subnet. ☐ RIP-2M—This version sends data to multicast addresses.

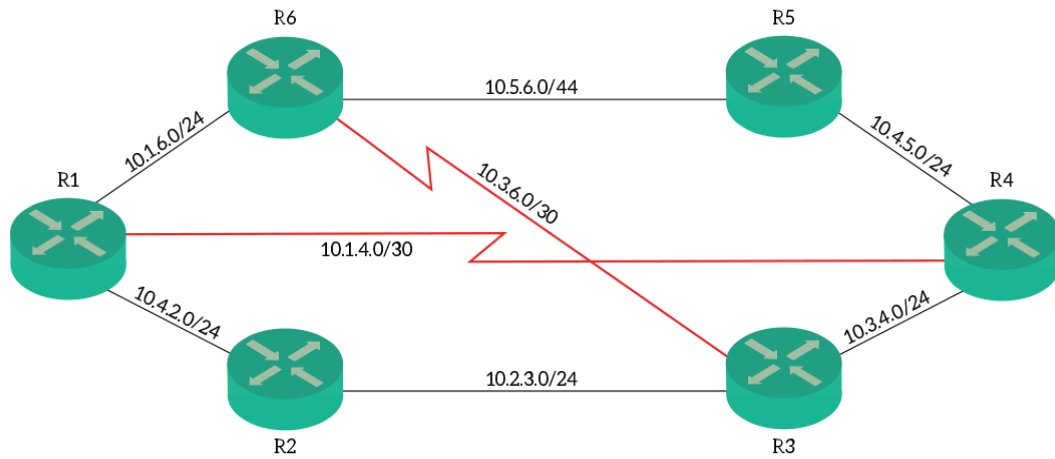
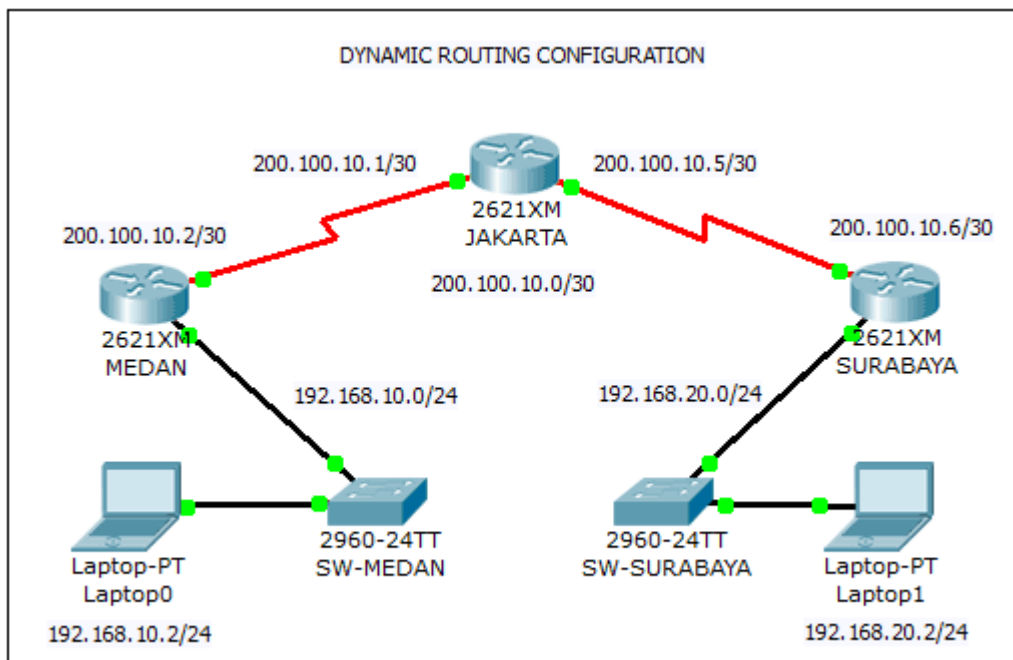


Fig. RIP Dynamic routing

4. RIP v2 authentication forces authentication of RIP packets before routes are exchanged with other routers. It acts as a security feature because routes are exchanged only with trusted routers in the network. RIP authentication is disabled by default. You can enter two key parameters so that routes can be exchanged with multiple routers present in the network. The second key also acts as a failsafe when authorization with first key fails. To enable authentication for RIP-2B or RIP- 2M, check the Enable box. (You must also choose the direction as explained in Step 2.)
5. If you enabled RIP v2 authentication, enter the following first and second key parameters:
 - MD5 Key ID—Input the unique MD-5 key ID used to create the Authentication Data for this RIP v2 message.
 - MD5 Auth Key—Input the auth key for this MD5 key, the auth key that is encrypted and sent along with the RIP-V2 message.
 - Not Valid Before—Enter the start date when the auth key is valid for authentication.
 - Not Valid After—Enter the end date when the auth key is valid for authentication.
6. Click Save.



Practical No 7:

Configuration of Wireless router.

Solution:

1. Open a web browser. Your router's configuration page can be accessed by any computer that is connected to the same network. When configuring your router, you will have the best results if you connect with a computer that is wired to the router with an Ethernet cable.

*You can use Google Chrome, Mozilla Firefox, or another web browser.

2. Enter in your router's address. Routers are accessed through your web browser by entering the IP address into the address bar. The IP address varies a bit by manufacturer, but most are the same or very close. These are some of the more popular manufacturers and the associated addresses:

- a. Linksys: <http://192.168.1.1>
- b. Xfinity: <http://10.0.0.1/>
- c. 3Com: <http://192.168.1.1>
- d. D-Link: <http://192.168.0.1>
- e. Belkin - <http://192.168.2.1>
- f. Netgear - <http://192.168.1.1>
- g. Arris - <http://10.0.0.1>
- h. Most routers have their default address printed in the documentation or on a sticker on the router itself. You can also look it up online on the manufacturer's website or if the given router's address doesn't work for you then you can simply reset your router to its default state.

The image shows a web login interface. At the top, there is a blue header bar with the text "Web login". Below this, there are three input fields: "Username:", "Password:", and "VerificationCode:". Each field has a corresponding text input box. Below the "VerificationCode:" field, there is a small image of a captcha that reads "jc0nn". At the bottom of the form, there are two buttons: "Login" and "Rewrite".

3. Enter in your username and password. Before you access the configuration page, you'll be asked for a username and password. Most routers will come with a default username/password combo, while some allow you to proceed without entering anything.
 - i. Your router's documentation will tell you the default username and password required. They may also be printed on the router itself.
 - ii. "admin" is one of the most common default usernames.
 - iii. "admin" or "password" are two of the most common passwords.
- b. Reset your router if you can't access it. If you've looked up your default address and username/password combo and you still can't access your router, you can reset it to factory defaults to clear out any changes that may have been made. This is useful for secondhand routers or old changes that you can't remember.
 - i. You can reset your router by pressing the Reset button on it. This button is usually small and recessed, and can only be reached by a paper clip. Some routers have a button that can be pressed more easily.
 - ii. You'll know the router is reset once you see the lights flashing. After pressing the reset button, wait 30-60 seconds and then try entering the router's address and username/password combination again.

Web login

Username:

Password:

VerificationCode:

4. Assign the router a new username and password. Leaving your router with the default username and password is very insecure, and you should change it immediately after setting it up. You can usually find this in the Administration section of the router configuration.
 - i. Choose a username and password that can't be easily guessed. Include numbers and symbols to create a secure password.
 - ii. Routers connected to services, such as Xfinity, may require you to log into a mobile app to manage more settings. If you don't see more options, head to your internet provider's main website to download their mobile app.

Practical No. 8:

Configuration of WLAN.

Solution:

1. How to Configure WAN Interfaces:

By default, ports p2 and p3 are preconfigured. In the event that you need to design a WAN interface for both of these ports, you may need to evacuate the default configurations:

- Port p2 – Initially, the system interface for port p2 is designed as a powerful system interface named DHCP. On the off chance that you need to design either a static or other unique association other than DHCP (PPTP or PPPoE) on port p2, erase the default DHCP interface.
- Port p3 – Initially, port p3 is connected to port p1. The two interfaces are likewise designed as the executive's ports in the LAN. To utilize port p3 for another association, erase the P1-P3 connect. Anyway, you may lose availability to the system from your regulatory PC.

After removing the default setups for ports p2 and p3, you can reconfigure them as WAN interfaces. For some other ports, simply start arranging the WAN interface. You can arrange the WAN interface with either static or dynamic IP address assignment.

Make certain to add the entryway to make the default course over the WAN interface, either when you include or alter a static system interface, or on the NETWORK > Routing page.

Choose whether the WLAN SSID should broadcast on all APs associated to the managed device or Mobility Master configuration, or whether the WLAN should broadcast on APs in a selected AP group. If you choose the Select AP Groups option, you are prompted to select one or more AP groups.

General

Advanced

Interface 'X1' Settings

Zone:	WAN
IP Assignment:	Static
IP Address:	10.203.15.82
Subnet Mask:	255.255.255.0
Default Gateway:	10.203.15.1
DNS Server 1:	10.50.129.148
DNS Server 2:	0.0.0.0
DNS Server 3:	0.0.0.0
Comment:	Default WAN
Management:	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input type="checkbox"/> SNMP <input type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
	<input type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS

2. Remove the default configurations for port p2 and port p3:

On the off chance that you need to utilize port p2 or p3, first evacuate their default designs.

1. If you need to use port p2:

- Go to the NETWORK > IP Configuration page.
- Delete the default DHCP interface from the Dynamic Interface Configuration section.

2. If you need to utilize port p3:

- Go the NETWORK > Bridging page and delete the P1-P3 bridge.
- Go the FIREWALL > Firewall Rules page. Delete the P1-P3-BRIDGE firewall rule.

3. Configure a WAN interface:

To configure a WAN interface:

1. Go to the NETWORK > IP Configuration page.
2. If your WAN interface has a static IP address:
 - a. In the Static Interface Configuration section, click Add Static Network Interface.
 - b. Configure the static interface settings, including the gateway address.
 - c. Click Add.
3. If you have a dynamic connection, for example, PPTP or PPPoE:
 - a. In the Dynamic Interface Configuration segment, click Add Dynamic Network Interface.
 - b. Configure the dynamic interface settings.
 - c. Click Add.
4. At the top of the page, click on the warning message to execute the new network configuration.

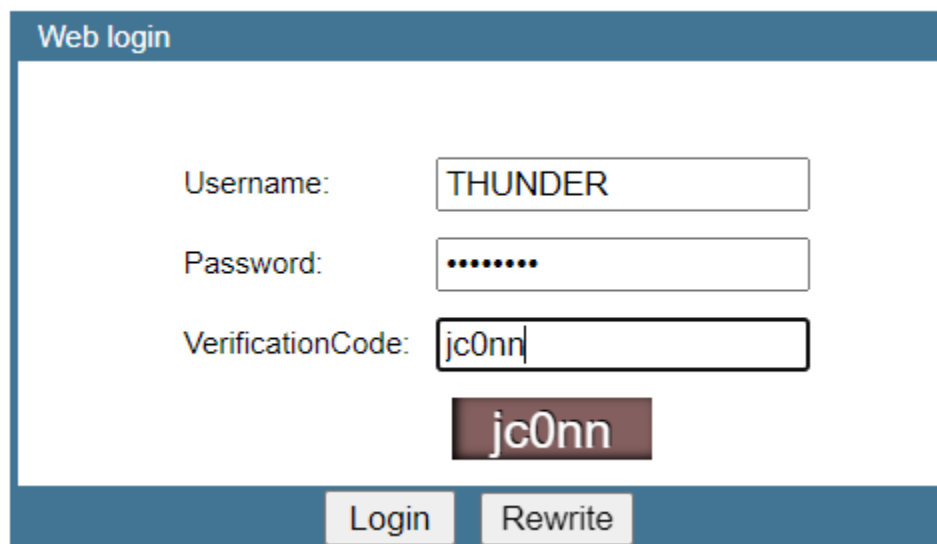
Practical No 9:

Connection of wired with wireless LAN.

Solution:

For Netlink router for BSNL broadband:

1. Login to Netlink ONU in any browser with URL 192.168.1.1
2. Enter username and password. Username is admin and default password is stdONU101



The image shows a web login interface for a Netlink ONU. The title is "Web login". It contains three input fields: "Username:" with the value "THUNDER", "Password:" with masked characters ".....", and "VerificationCode:" with the value "jc0nn". Below the verification code field is a button labeled "jc0nn". At the bottom of the form are two buttons: "Login" and "Rewrite".

3. Go to Management > Device Management > Restore default > Restore Factory default
4. Click Network > Internet > Delete
5. Check Status > Wan Connection info > WAN info status enabled means you are ready to browse the internet.
6. Click Network > Internet (Add New Connection for Internet)

Mode : Route,

IP Protocol Mode : Ipv4, and select PPPoE,

Enable NAT : Select radio button

Enable Vlan : Enable by select,

Vlan id : Submit the ID provided by BSNL,

Username : Enter BSNL allocated FTTH username followed by @ftth.bsnl.in

Password : password (default)

Service Name : BSNL or which you want,

IP Address: Provide your BSNL allocated IP address,

Port binding : Enable Port 1, Port2 and WLAN (SSID1) by selecting in each box Click Save

7. Again Click Network > Internet for Voice Configuration

Connection name : Add new wan connection,

Mode : Route,

IP Protocol Mode : Ipv4, and select Static,

Enable Vlan : Enable by select,

Vlan id : 1830,

Provide your BSNL allocated IP address, Subnet Mask, Default Gateway, DNS1, DNS2, provided by BSNL

Service Mode : Voice

Click Save

8. Click Application

Enable all the services(ftp, h323, rtsp, ipsec, sip, pptp) in ALG configuration

Save/Apply

9. Click Application > VOIP

SIP registered address : xx.ftthvoip.bsnl.in (first 5 to be filled as xx.ftth.bsnlvoip.bsnl.in)

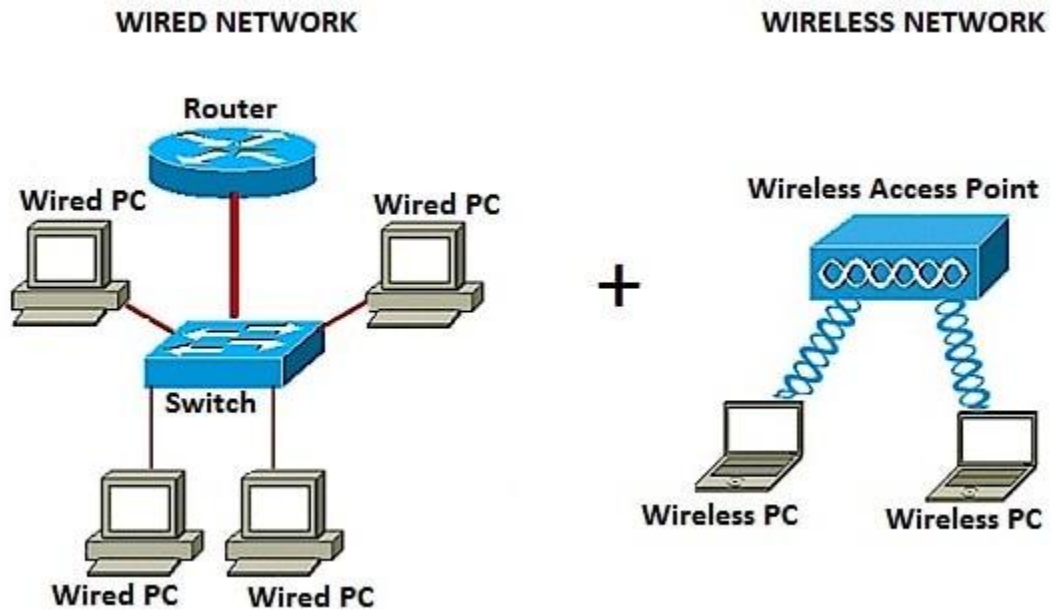
Select and Enable Outbound Proxy,

Enable Line 1 and enter Account name, Account number, Account password with allotted BSNL FTTH phone number starting with 91 starting by removing 0

Click Save/Apply

10. Click Status

WAN Information info for both Voice and Internet facilities are enabled or not.



Practical No. 10

Configuration of DHCP server in a network.

Solution:

Steps to be followed on Cisco Packet Tracer

Step 1: Creating a LAN and server:

- Add a Switch (Switch0).
- Add a Server PT (Server0).
- Connect them using Copper Straight cable.
- Add 3 Generic PCs and connect them to Switch0 using Copper Straight cable.

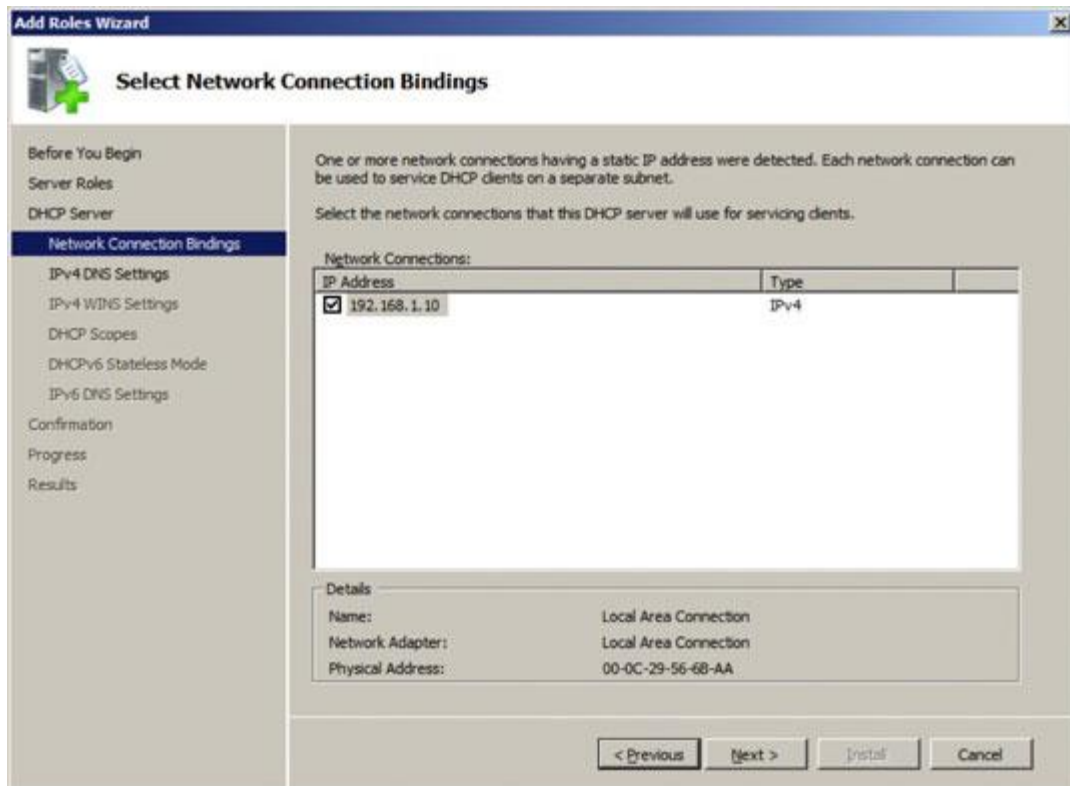
Step 2: Click on Server for configuration menu, then go to Services tab.

Step 3: Turn the Service On by choosing On radio option.

Step 4: Go to Services tab and click on DHCP.

Step 5: Then edit Start IP address and assign IP and Subnet Mask:

IP: 10.0.0.10 and Subnet mask 255.0.0.0



Step 6: In Maximum Number of Users assign number if required (512 default).

Step 7: Click on Save.

Step 8: Go to Config tab and select FastEthernet0 from left side menu.

Step 9: Assign IP address and Subnet Mask. In this case assign IP: 10.0.0.1 and subnet mask 255.0.0.0 and close the window.

Step 10: Now, Click on any of the PC-> then click on Desktop->IP configuration, and Choose 'DHCP' wait for some time, if your DHCP request failed then try few more times.

- ☐ You can also add any new PC or Laptop to Switch0 and assign IP using DHCP.

