TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

Computer Networks a computer network is interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communication data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as nodes.

Types of Networks

There are many different types of networks. However, from an end user's point of view there are three basic types:

- Local Area Network (LAN)
- Metropolitan Area Network (WAN)
- Wide Area Network (WAN)

Local-Area Network (LAN) The computers are geographically close together (that is, in the same room or building).

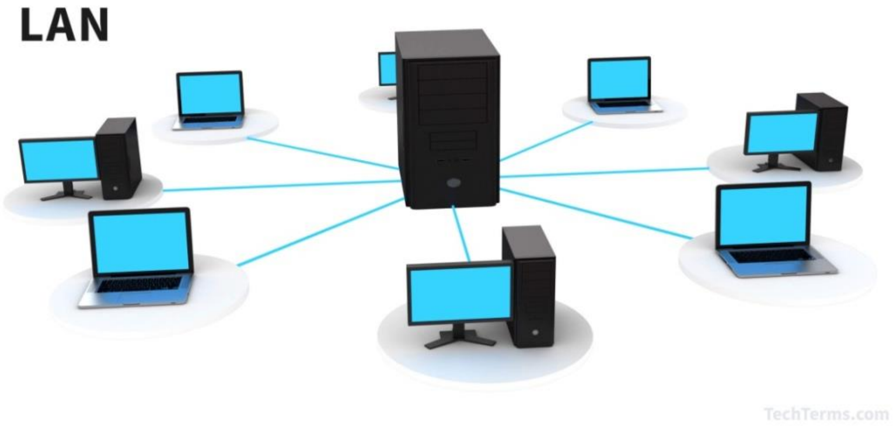


FIG 1.1 Local Area Network

METROPOLITAN AREA NETWORK MAN

A Metropolitan Area Network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN.

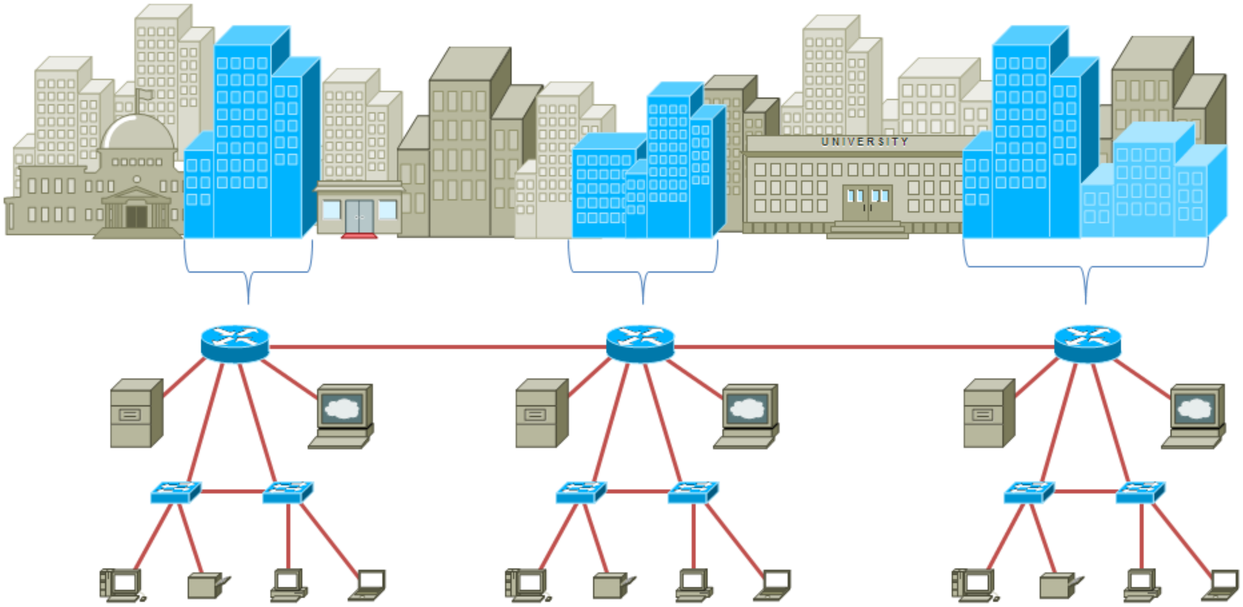


FIG 1.2Metropolitan Area Network

Wide-Area Network (WAN)

A Wide Area Network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports. WAN is a computer network spanning regions, countries, or even the world.

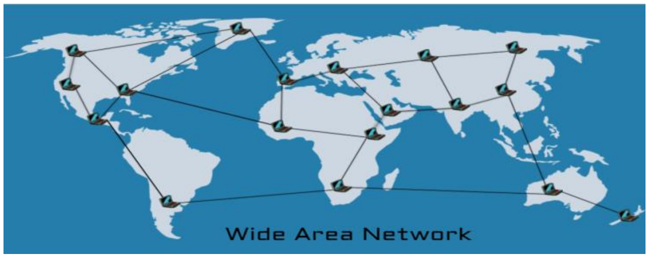


FIG 1.3 Wide Area Network

Bus Topology

In Bus Networks the ends are not connected. All communications are carried on a common cable or bus and are available to each device on the network.

Access and control of bus networks are typically maintained by a method called contention, whereby if a line is unused, a terminal or device can transmit its message at will, but if two or more terminals initiate messages simultaneously, they must stop and transmit again at different intervals.

Star Topology

The Star Network is frequently used to connect one or more small computers or peripheral devices to a large host computer or CPU. Many organizations use the star network or a variation of it in a time-sharing system, in which several users are able to share a central processor.

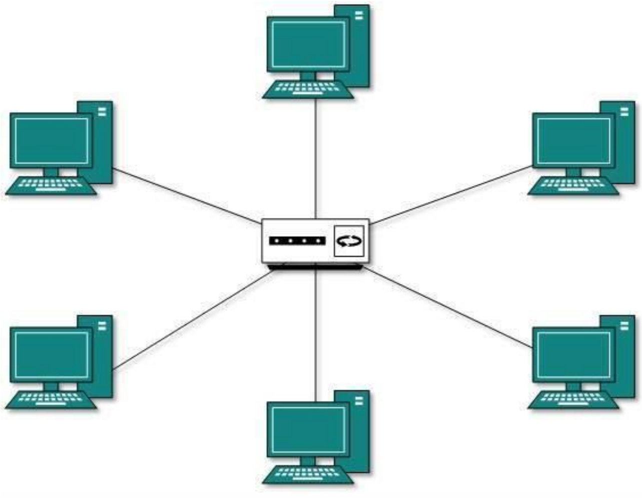


FIG 1.4 Star Topology

In a time-sharing setup, each terminal receives a fixed amount of the CPU's time, called a time slice. If you are sitting at a terminal and cannot complete your task during the time slice, the computer will come back to you to allow you to do so. If the user of one microcomputer wants to send a document or message to a user at another computer, the message is routed through the central communications controller commonly called as HUB. Another common use of the star network is the feasibility of connecting several microcomputers to a mainframe computer that allows access to an organization's database. Access and control of star network typically is maintained by a polling system. Polling means that the central computer or communications controller "polls" or asks each device in the network if it has a message to send and then allows each in turn to transmit data.

Mesh Topology

Or Mesh network, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a true mesh topology every node has a connection to every other node in the network.

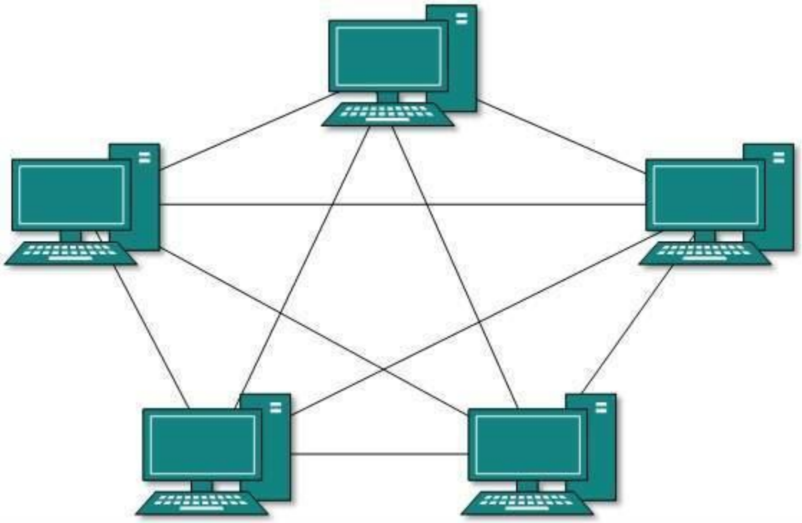


FIG 1.5 Mesh Topology

Ring Topology

The Ring Network is a Local Area Network (LAN) whose topology is a ring - can be as simple as a circle or point-to-point connections of computers at dispersed locations, with no central host computer or communications controller. That is, all of the nodes are connected in a closed loop. Messages travel around the ring, with each node reading those messages addressed to it. One of the advantages of ring networks is that they can span larger distance than other types of networks, such as bus networks, because each node regenerates messages as they pass through it.

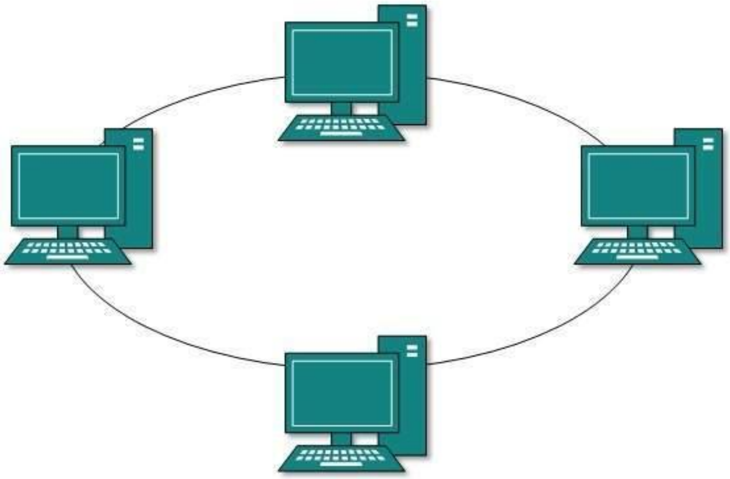


FIG 1.6 Ring Topology

Access and control of ring networks are typically maintained by a "token-passing" system. IBM's Token-Ring network is thought by some observers to be a watershed event comparable to the development of the IBM PCV itself, because the Token-Ring network is designed to link all types of computers together, including not only personal computers but also possible mini computes and mainframes.

Hybrid Topology

The combination of two or more of the above mentioned topologies is called a Hybrid Network. For example the below shown network is the combination of Bus, Star and Ring topology.

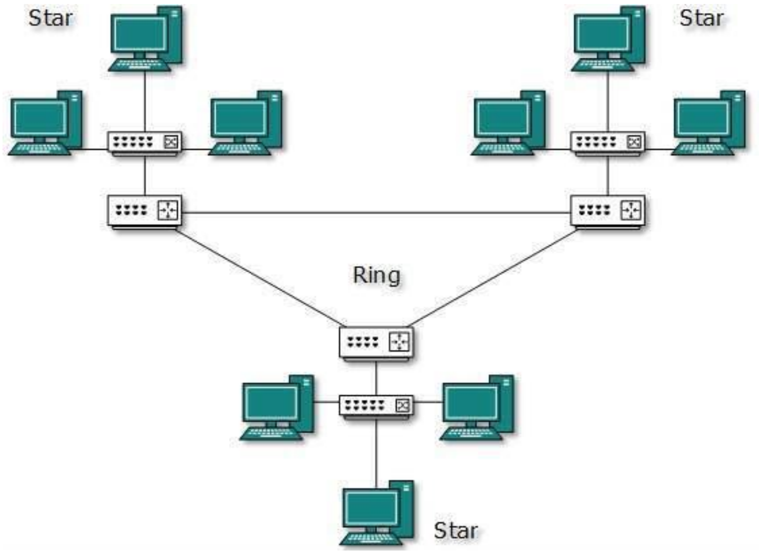


FIG 1.7 Hybrid Topology

1.1 <u>NEED OF STUDY</u>

- **Get connected to the most connected people**

  There is a worldwide community of people just like you. More than 4.75 million students in 165 countries have participated in Cisco Networking Academy courses since 1997. That's a lot of friends to find and connect with on LinkedIn or the Cisco Networking Academy Facebook page, which has over 530,000 student and instructor members who use it to stay in touch, ask questions, and learn about new learning opportunities. Most academies have their own Facebook sites and many have LinkedIn communities.

- **Every workplace needs a few friendly geeks**

Networking skills give you an edge and an opportunity to make a career in almost any sector you can imagine: financial services, education, transportation, manufacturing, oil and gas, mining and minerals, technology, government, hospitality, health care, retail... you name it. If you have an interest in a particular field, technology is probably part of it. For example, health care clinicians study networking technology to better understand how to use it in their practice. At Effat University in Saudi Arabia, women have dramatically expanded their career opportunities by adding networking to their skills set. Veteran Matt Hefler became a virtual systems engineer with several job offers after his networking studies. Whether you see yourself with your own business, as part of a small company or inside a global corporation, networking basics open the door to help advance your career.

Computer networks help users on the network to share the resources and in communication. Can you imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet?

- **File sharing**: Networking of computers helps the network users to share data files.

- **Hardware sharing**: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.

- **Application sharing**: Applications can be shared over the network, and this allows to implement client/server applications

- **User communication**: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

CHAPTER 2
IMPLEMENTATION OF PROPOSED METHOD

2.1 SYSTEM REQUIREMENT

Simulation Software

Simulation is the imitation of the operation of a real-world process or system over time.[1] The act of simulating something first requires that a model be developed; this model represents the key characteristics, behaviors and functions of the selected physical or abstract system or process. The model represents the system itself, whereas the simulation represents the operation of the system over time.

Packet Tracer

It is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students they had enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.[1] Since August 2017 with version 7.1 is free to everyone.

2.2 CABLES USED

Twisted-pair

This wire comes in several ―standards.‖ Unshielded twisted pair (UTP) Category 3 wire (also called 10BaseT) is often used for your phone lines, and UTP Category 5 (also called 10Base2) wire is the current networking standards. Coaxial resembles round cable TV wiring.

Fiber-optic

Usually reserved for connections between backbone‖ devices in larger networks, though in some very demanding environments, highly fault resistant cable is used to connect desktop workstations to the network and to link adjacent buildings.

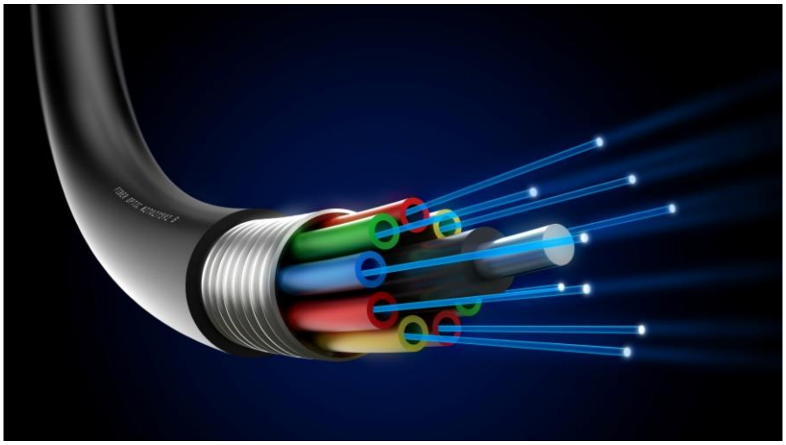


FIG 2.1 Fiber Optic Cable

Fiber-optic cable is the most reliable wiring but also the most expensive. For instance, Ethernet can useUTP Category 3 wiring. However, Fast Ethernet requires at least the higher-grade UTP Category 5 wiring. As a result, all new wiring installations should be Category 5.

Coaxial

Coaxial cable or coax is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outersheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis.

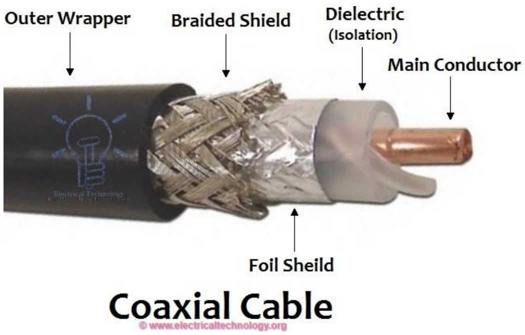


FIG 2.2 Coaxial Cable

SERIAL CABLE

A serial cable is a cable used to transfer information between two devices using a serial communication protocol. The form of connectors depends on the particular serial port used. A cable wired for connecting two DTEs directly is known as a null modem cable.

FIG 2.3 Serial Cable

CROSS OVER CABLE

A crossover cable connects two devices of the same type, for example DTE-DTE or DCE-DCE, usually connected asymmetrically (DTE-DCE), by a modified cable called a crosslink.[1] Such distinction of devices was introduced by IBM.

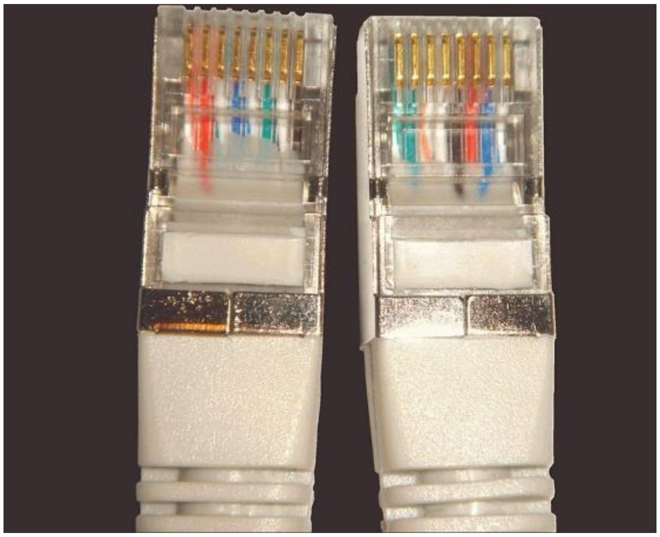


FIG 2.4 Cross Over Cable

2.3HARDWARE USED

Repeater

A device which amplifies or regenerates digital signals received while sending them from one part of a network into another. It works on OSI layer 1.

FIG 2.5 Repeater

Hubs

Hubs, or repeaters, are simple devices that interconnect groups of users. Hubs forward any data packets they receive over one port from one workstation—including e-mail, word processing documents, spread-sheets, graphics, or print requests—to all of their remaining ports. All users connected to a single hub or stack of connected hubs are in the same segment, sharing the hub's bandwidth or data-carrying capacity.

As more users are added to a segment, they compete for a finite amount of bandwidth devoted to that segment. : a device that connects multiple Ethernet segments, making them act as a single segment. When using a hub, every attached device shares the same broadcast domain and the same collision. Therefore, only one computer connected to the hub is able to transmit at a time. Depending on the network topology, the hub provides a basic level 1 OSI model connection among the network objects (workstations, servers, etc.). It provides bandwidth which is shared among all the objects, in contrast to switches, which provide Aconnection between individual nodes. It works on OSI layer 1.

Switches

Switches are smarter than hubs and offer more bandwidth. A switch forwards data packets only to the appropriate port for the intended recipient, based on information in each packet's header. To insulate the transmission from the other ports, the switch establishes a temporary connection between the source and destination then terminates the connection when the conversation is done

FIG 2.6 Cisco Switch

. As such, a switch can support multiple ―conversations‖ and move much more traffic through the network than a hub. A single eight-port Ethernet hub provides a total of 10 megabits per second (Mbps) of data- carrying capacity shared among all users on the hub. A ―full-duplex, eight-port Ethernet switch can support eight 10-Mbps conversations at once, for a total data-carrying capacity of 160 Mbps. ―Full-duplex‖ refers to simultaneous two-way communications, such as telephone communication. With half-duplex communications, data can move across the cable or transmission medium in just one direction at a time. : a device that allocates traffic from one network segment to certain lines (intended destination(s)) which connect the segment to another network segment. Unlike a hub, a switch splits the network traffic and sends it to different destinations rather than to all systems on the network. It works on OSI layer 2.

Routers

Compared to switches and bridges, routers are smarter still. Routers use a more complete packet ―address‖ to which router or workstation should receive each packet. Based on a network roadmap called a ―routing table,‖ routers can help ensure that packets are travelling the most efficient paths to their destinations. If a link between two routers goes down, the sending router can determine an alternate route to keep traffic moving. Routers also provide links between networks that speak different languages—or, in computer speak—networks that use different

FIG 2.7 Cisco Router

―protocols.‖ Examples include IP (Internet Protocol), the IPX® (Internet Packet Exchange Protocol), and AppleTalk. Routers not only connect networks in a single location or set of buildings, but they provide interfaces— or ―sockets‖—for connecting to wide-area network (WAN) services. These WAN services, which are offered by telecommunications companies to connect geographically, dispersed networks. : a specialized network device that determines the next network point to which it can forward a data packet towards the ultimate destination of the packet. Unlike a gateway, it cannot interface different protocols. It works on OSI layer 3

2.4 Command Line Interface (CLI)

Cisco IOS has three command modes, each with access to different command sets:

User mode—This is the first mode a user has access to after logging into the router. The user mode can be identified by the > prompt following the router name. This mode allows the user to execute only the basic commands, such as those that show the system's status. The system cannot be configured or restarted from this mode.

Privileged mode—This mode allows users to view the system configuration, restart the system, and enter configuration mode. It also allows all the commands that are available in user mode. Privileged mode can be identified by the # prompt following the router name. The user mode enable command tells IOS that the user wants to enter privileged mode. If an enable password or enable secret password has been set, the user needs to enter the correct password or secret to be granted access to privileged mode. An enable secret password uses stronger encryption when it is stored in the configuration and, therefore, is safer. Privileged mode allows the user to do anything on the router, so it should be used with caution. To exit privileged mode, the user executes the disable command.

Configuration mode—This mode allows users to modify the running system configuration. To enter configuration mode, enter the command configure terminal from privileged mode. Configuration mode has various submodes, starting with global configuration mode, which can be identified by the (config)# prompt following the router name. As the configuration mode submodes change depending on what is being configured, the words inside the parentheses change. For example, when you enter interface configuration submode, the prompt changes to (config-if)# following the router name. To exit configuration mode, the user can enter end or press Ctrl-Z.

Note that in these modes, entering the context-sensitive command ?at any point shows the available commands at that level. The ?can also be used in the middle of a command to show possible completion options. Example 4-2 shows the use of the ?command to display the commands available within a given command mode.

Example 4-2 Using Context-Sensitive Help

```
Router>?
Exec commands:
 access-enable  Create a temporary Access-List entry
 access-profile  Apply user-profile to interface
clear      Reset functions
...
```

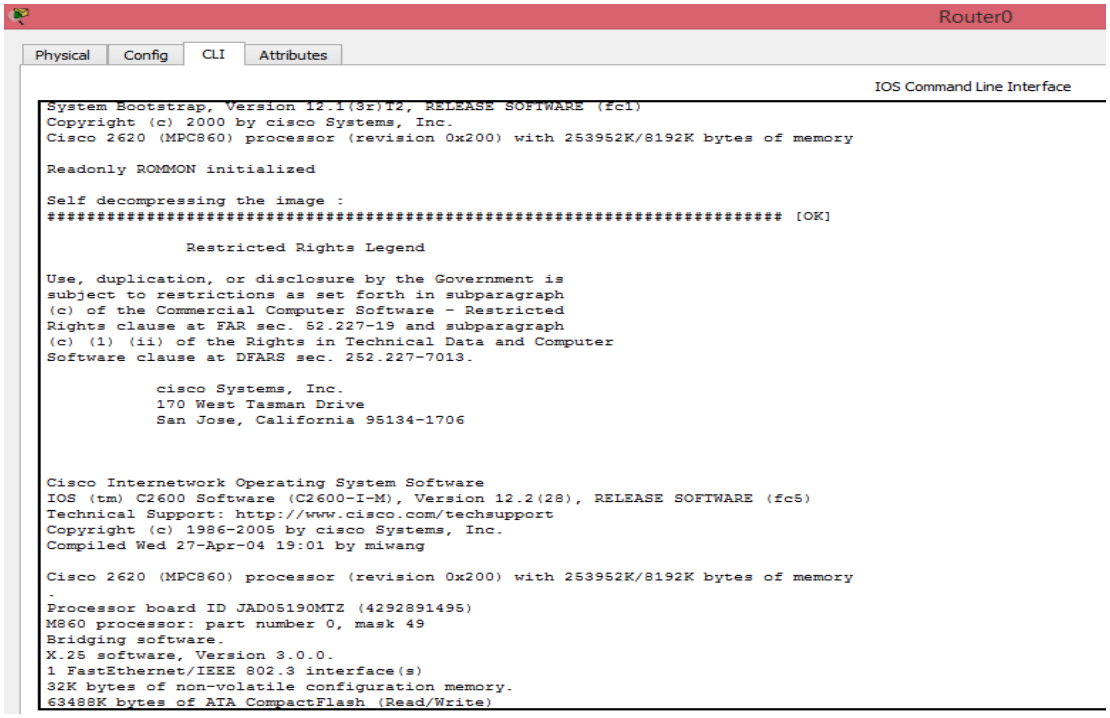
The following steps introduce you to the commands used to change command mode, view system information, and configure a password. Real CLI output from a Cisco 3640 router running Cisco IOS software is shown.

Step 1 Enter enabled mode by entering enable and pressing Enter:

```
Router> enable
Router#
```

Step 2 To see which version of IOS is running on the system, enter the show version command:

```
Router# show version
```



```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Cisco 2620 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memory

Readonly ROMMON initialized

Self decompressing the image :
########################################################################### [OK]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2620 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
```

FIG 2.8 Cisco Router Version

Step 3 Next, configure the router name to be "IOS." To enter configuration mode, use the command configure terminal:

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

Notice that the prompt changes to "IOS" immediately after you enter the hostname command. All configuration changes in Cisco IOS take place immediately.

Step 4 Next, you need to set the enable password and the enable secret pass- word. The enable secret password is stored using stronger encryption and overrides the enable password if it is configured. To set both passwords, you enter the following:

```
IOS(config)# enable password cisco
IOS(config)# enable secret san-fran
IOS(config)# exit
IOS#
```

To get into enabled mode, you need to enter the password san-fran. The exit command takes you up one level in the configuration, or out of the current submode.

Step 5 After configuring the router name and setting the enable and enable secret passwords, you can examine the running configuration:

```
IOS# show running-config
Building configuration...

Current configuration : 743 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname IOS
!
enable secret 5 $1$IP7a$HClNetI.hpRdox84d.FYU.
enable password cisco
!
ip subnet-zero
!
call rsvp-sync
!
interface Ethernet0/0
noip address
shutdown
half-duplex
```

```
!
interface Serial0/0
noip address
shutdown
no fair-queue
!
interface Ethernet2/0
noip address
shutdown
half-duplex
!
interface Ethernet2/1
noip address
shutdown
half-duplex
!
interface Ethernet2/2
noip address
shutdown
half-duplex
!
interface Ethernet2/3
noip address
shutdown
half-duplex
!
ip classless
ip http server
ippimbidir-enable
!
dial-peercor custom
```

```
!
line con 0
line aux 0
linevty 0 4
!
end
```

Step 6 The show running-config output shows the configuration that is currently active in the system; however, this configuration is lost if the system is restarted. To save this configuration to NVRAM, you must issue the following command:

```
IOS# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 7 To view the startup configuration saved in NVRAM, use the command show startup-config.

In the preceding step sequence, notice the Ethernet and serial interfaces that show up in the configuration file. Each interface requires that certain parameters such as encapsulation and address be set before the interface can be used properly. In addition, IP routing or bridging might need to be configured. Refer to the Cisco IOS installation and configuration guides available at http://www.cisco.com for your version of software to learn about all possible configuration options and recommended guidelines.

2.5 SERVICES

The Dynamic Host Configuration Protocol (DHCP)

DHCP is a network management protocol used on TCP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.[1] A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.[1] In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.

DHCP can be implemented on networks ranging in size from home networks to large campus networks and regional Internet service provider networks small local networks as well as large enterprise networks.[2] A router or a residential gateway can be enabled to act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.

1) Client makes a UDP Broadcast to the server about the DHCP discovery.
2) DHCP offers to the client.
3) In response to the offer Client requests the server.
4)Server responds all the Ip Add/mask/gty/dns/wins info along with the acknowledgement packet.

Secure Shell

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.[1] The best known example application is for remote login to computer systems by users.

SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.[2] Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, and hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989. Standards development of HTTP was coordinated by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), culminating in the publication of a series of Requests for Comments (RFCs). The first definition of HTTP/1.1, the version of HTTP in common use, occurred in RFC 2068 in 1997, although this was obsoleted by RFC 2616 in 1999 and then again by the RFC 7230 family of RFCs in 2014.

Domain Name System

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985.

Telnet

Telnet is a protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Voice over IP(VOiP)

Voice over Internet Protocol (also voice over IP, VoIP or IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet.

The Cisco ASA 5500 series is Cisco's follow up of the Cisco PIX 500 series firewall. However, the ASA is not just a pure hardware firewall. In brief, the Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defense that stops attacks before they spread through the network. Indeed, Cisco ASA firewall is the whole package, so to speak.

Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include backup links to provide fault tolerance if an active link fails.

As the name suggests, STP creates a spanning tree within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. STP is based on an algorithm that was invented by Radia Perlman while she was working for Digital Equipment Corporation.

Cisco Configuration Professional

Itoffers smart wizards and advanced configuration support for LAN and WAN interfaces, Network Address Translation (NAT), stateful and application firewall policy, IPS, IPSec and SSL VPN, QoS, and Cisco Network Admission Control policy features. The firewall wizard allows a single-step deployment of high, medium, or low firewall policy settings. IT managers can easily organize and manage multiple routers at a single site.

Cisco Configuration Professional Offers:

- One-click router lockdown
- Innovative voice and security auditing capabilities to check and recommend changes to router configurations
- Monitoring of router status
- Troubleshooting of WAN and VPN connectivity issues
- Cisco Configuration Professional Express is a GUI-based embedded device management tool for Cisco Integrated Services Routers (ISRs). It is available on the flash of the router and used for bootstrapping and basic configurations.

2.6 CONFIGURATION

VLAN CONFIGURATION

```
king#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
king(config)#int
king(config)#interface range fastEthernet 0/3 - 6
king(config-if-range)#sw
king(config-if-range)#switchport mode access
king(config-if-range)#switchport access vlan 3
king(config-if-range)#^Z
king#
%SYS-5-CONFIG_I: Configured from console by console
king#showvlan
VLAN Name                          Status    Ports
---- ------------------------------ --------- -------------------------------
1    default                     active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                        Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                        Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                        Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                        Fa0/23, Fa0/24
2    sales                       active    Fa0/1, Fa0/2
3    Accounts                    active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
1002 fddi-default                 act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default               act/unsup
1005 trnet-default                 act/unsup

VLAN Type  SAID       MTU   Parent RingNoBridgeNoStpBrdgMode Trans1 Trans2
```

```
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------



Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to up
king con0 is now available
Press RETURN to get started.

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
king>en
king#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
king(config)#intfa
king(config)#intfastEthernet 0/24
king(config-if)#sw
king(config-if)#switchport m
king(config-if)#switchport mode t
king(config-if)#switchport mode trunk
king(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
king con0 is now available
Press RETURN to get started
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down

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

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
```

VTP CONFIGURATION

```
Switch#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain ?
WORD  Theascii name for the VTP administrative domain.
Switch(config)#int
Switch(config)#interface f0/1
Switch(config-if)#switchport mode a
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode t
Switch(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

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

Switch(config-if)#exit
Switch(config)#spanning-tree
% Incomplete command.
Switch(config)#spanning-tree ?
mode      Spanning tree operating mode
```

```
portfast  Spanning tree portfast options
vlan      VLAN Switch Spanning Tree
Switch(config)#vt
Switch(config)#vtp d
Switch(config)#vtp domain ?
WORD  Theascii name for the VTP administrative domain.
Switch(config)#vtp domain jetking
Changing VTP domain name from NULL to jetking
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#shvtp status
VTP Version                    : 2
Configuration Revision         : 0
Maximum VLANs supported locally : 255
Number of existing VLANs       : 5
VTP Operating Mode             : Server
VTP Domain Name                : jetking
VTP Pruning Mode               : Disabled
VTP V2 Mode                    : Disabled
VTP Traps Generation           : Disabled
MD5 digest                     : 0x96 0xDB 0xDC 0x3A 0xBC 0x50 0x09 0x65
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#confi
Switch#configure
Configuring from terminal, memory,
or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vl
Switch(config)#vlan 2
Switch(config-vlan)#sa
Switch(config-vlan)#name sales
Switch(config-vlan)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#shvl
Switch#shvlan

VLAN Name                          Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
2    sales                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNoBridgeNoStpBrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

```
Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#wr
Building configuration...
[OK]
```

BACKUP FROM TFTP TO FLASH CONFIGURATION

```
Press RETURN to get started!

Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#int
Router(config)#int f0/0
Router(config-if)#ipaddres
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shut

%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)#^Z
```

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy ?
flash:          Copy from flash: file system
ftp:            Copy from ftp: file system
  running-config  Copy from current system configuration
  startup-config  Copy from startup configuration
tftp:           Copy from tftp: file system
Router#sh version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
```

```
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
Router#show flash

System flash directory:
File  Length   Name/status
  3   5571584  c2600-i-mz.122-28.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[5827403 bytes used, 58188981 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)


Router#copy flash tftp
Source filename []?c2600-i-mz.122-28.bin
Address or name of remote host []?
?Host name or address not specified

Router#copy flash tftp
Source filename []?c2600-i-mz.122-28.bin
Address or name of remote host []? 10.0.0.2
Destination filename [c2600-i-mz.122-28.bin]?

Writing c2600-i-mz.122-28.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
[OK - 5571584 bytes]
```

```
5571584 bytes copied in 3.375 secs (1650000 bytes/sec)
Router#copytftp ?
flash:          Copy to flash: file system
  running-config  Copy configuration from system
  startup-config  Copy startup configuration from system
Router#copytftp flash
Address or name of remote host []?c2600-i-mz.122-28.bin
Source filename []?
?File name not specified
%Error parsing filename (Unknown error 0)

Router#copytftp flash
Address or name of remote host []? 10.0.0.1
Source filename []?c2600-i-mz.122-28.bin
Destination filename [c2600-i-mz.122-28.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing                                                                   device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: complete
Accessing tftp://10.0.0.1/c2600-i-mz.122-28.bin........
%Error opening tftp://10.0.0.1/c2600-i-mz.122-28.bin (Timed out).
```

CHAPTER 3: EXPERIMENTAL RESULT

3.1 MERITES

- **Easily make the blueprints**

  Whenever we have to make any network architecture or any network topology then first of all we have to make the blueprints of the network rather then directly start implementing it on real devices.

- **Time saver**

  This technology is too much time saving we don't have to wait for anything to load or anything all work goes with the smooth flow.

- **Easy to implement**

  This is very easy to implement when we do this on simulation software. Its easy on the real devices too but then you have to do a lot of physical work too like powering on the device put cables to different locations etc.

- **Easy to find errors**

  in this it is easy to find the errors, we can easily capture the error by transmitting packet from source to destination, if the packet sent successfully then its good and if it fails means there is some error.

- **Hands on to the devices you don't have**

  we can easily use the latest routers/switches etc. any network component if we need . we don't have to purchase it in order to use it

CHAPTER4
IMPLEMENTATION OF WAN TECHNOLOGY

- **4.1 <u>WAN TECHNOLOGY</u>**

.A **wide area network** (**WAN**) is a telecommunications network or computer network that extends over a large geographical distance. Wide area networks are often established with leased telecommunication circuits.

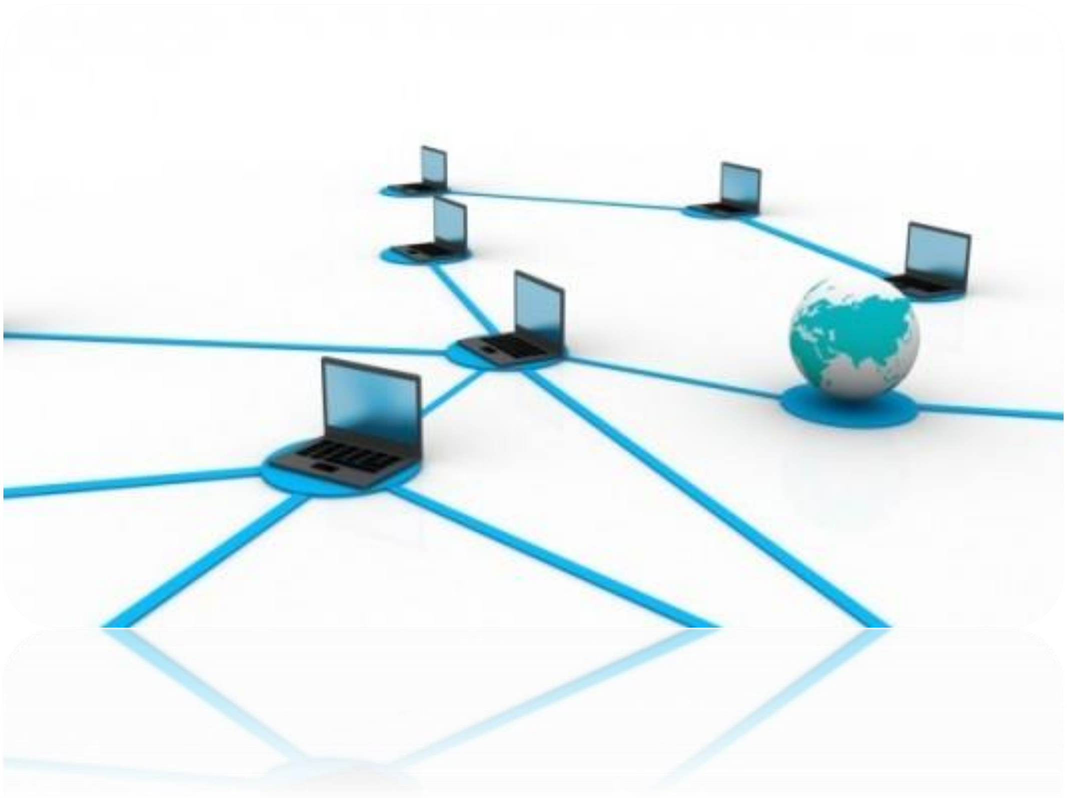


FIG 4.1 WAN Technology

4.2 Circuit Switching

Circuit switching involves creating a direct physical connection between sender and receiver, a connection that lasts as long as the two parties need to communicate. In order for this to happen, of course, the connection must be set up before any communication can occur. Once the connection is made, however, the sender and receiver can count on "owning" the bandwidth allotted to them for as long as they remain connected.

Although both the sender and receiver must abide by the same data transfer speed, circuit switching does allow for a fixed (and rapid) rate of transmission. The primary drawback to circuit switching is the fact that any unused bandwidth remains exactly that: unused. Because the connection is reserved only for the two communicating parties, that unused bandwidth cannot be "borrowed" for any other transmission.

4.3 Message Switching

Unlike circuit switching, message switching does not involve a direct physical connection between sender and receiver. When a network relies on message switching, the sender can fire off a transmission—after addressing it appropriately—whenever it wants. That message is then routed through intermediate stations or, possibly, to a central network computer. Along the way, each intermediary accepts the entire message, scrutinizes the address, and then forwards the message to the next party, which can be another intermediary or the destination node.

What's especially notable about message-switching networks, and indeed happens to be one of their defining features, is that the intermediaries aren't required to forward messages immediately. Instead, they can hold messages before sending them on to their next destination. This is one of the advantages of message switching. Because the intermediate stations can wait for an opportunity to transmit, the network can avoid, or at least reduce, heavy traffic periods, and it has some control over the efficient use of communication lines.

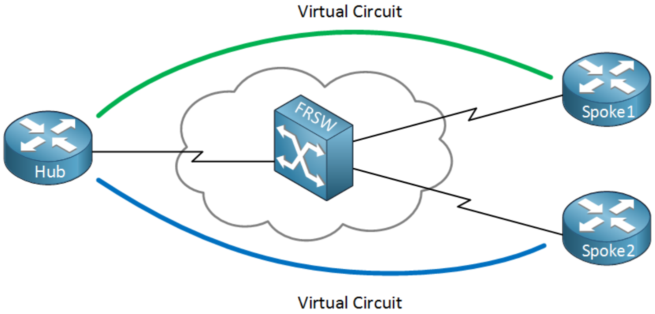
4.4 Packet Switching

Packet switching, although it is also involved in routing data within and between LANs such as Ethernet and Token Ring, is also the backbone of WAN routing. It's not the highway on which the data packets travel, but it *is* the dispatching system and to some extent the cargo containers that carry the data from place to place. In a sense, packet switching is the Federal Express or United Parcel Service of a WAN.

In packet switching, all transmissions are broken into units called packets, each of which contains addressing information that identifies both the source and destination nodes. These packets are then routed through various intermediaries, known as *Packet Switching Exchanges* (*PSE*s), until they reach their destination. At each stop along the way, the intermediary inspects the packet's destination address, consults a routing table, and forwards the packet at the highest possible speed to the next link in the chain leading to the recipient.

Frame relay

Frame relay is a newer, faster, and less cumbersome form of packet switching than X.25. Often referred to as a *fast packet switching* technology, frame relay transfers variable-length packets up to 4 KB in size at 56 Kbps or T1 (1.544 or 2 Mbps) speeds over permanent virtual circuits



Operating only at the data link layer, frame relay outpaces the X.25 protocol by stripping away much of the "accounting" overhead, such as error correction and network flow control, that is needed in an X.25 environment. Why is this? Because frame relay, unlike X.25 with its early reliance on often unreliable telephone connections, was designed to take advantage of newer digital transmission capabilities, such as fiber optic cable and ISDN.

HSRP

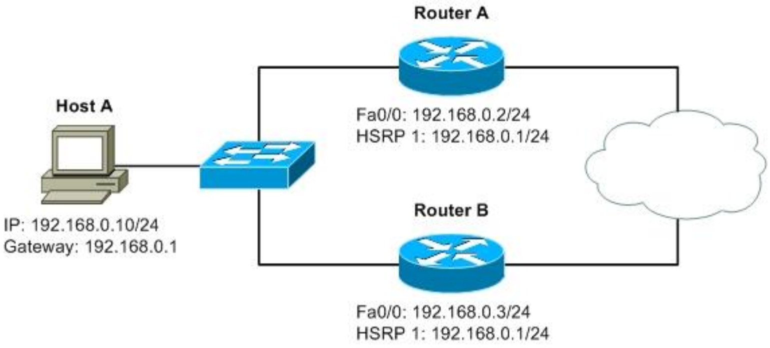


Fig4.2- Hot state Routing Protocol

In computer networking, the **Hot Standby Router Protocol** (**HSRP**) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. Version 1 of the protocol was described in RFC 2281. There is no RFC for version 2 of the protocol.

4.6 **VPN**

A **virtual private network** (**VPN**) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.

VPNs may allow employees to securely access a corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location in order to stay anonymous on the internet.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

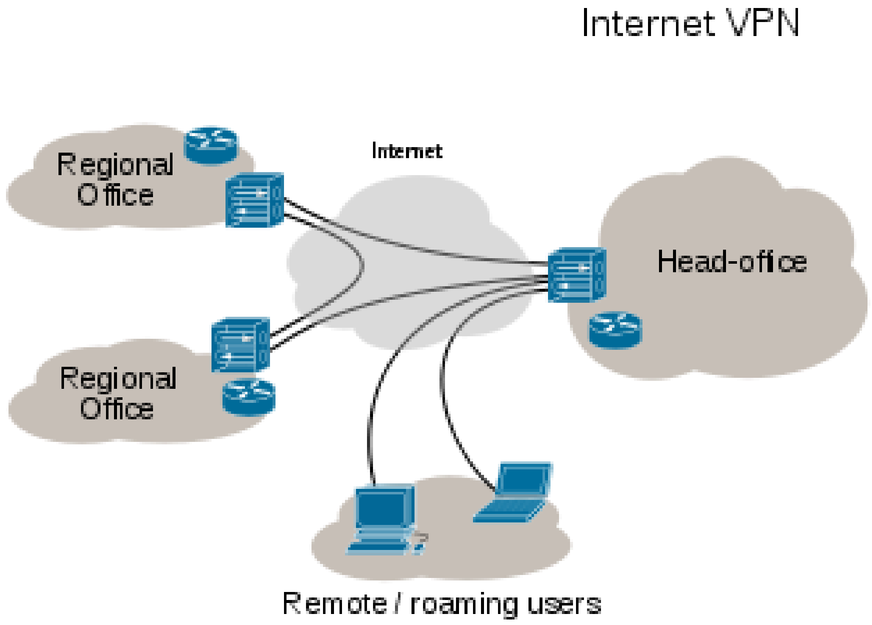
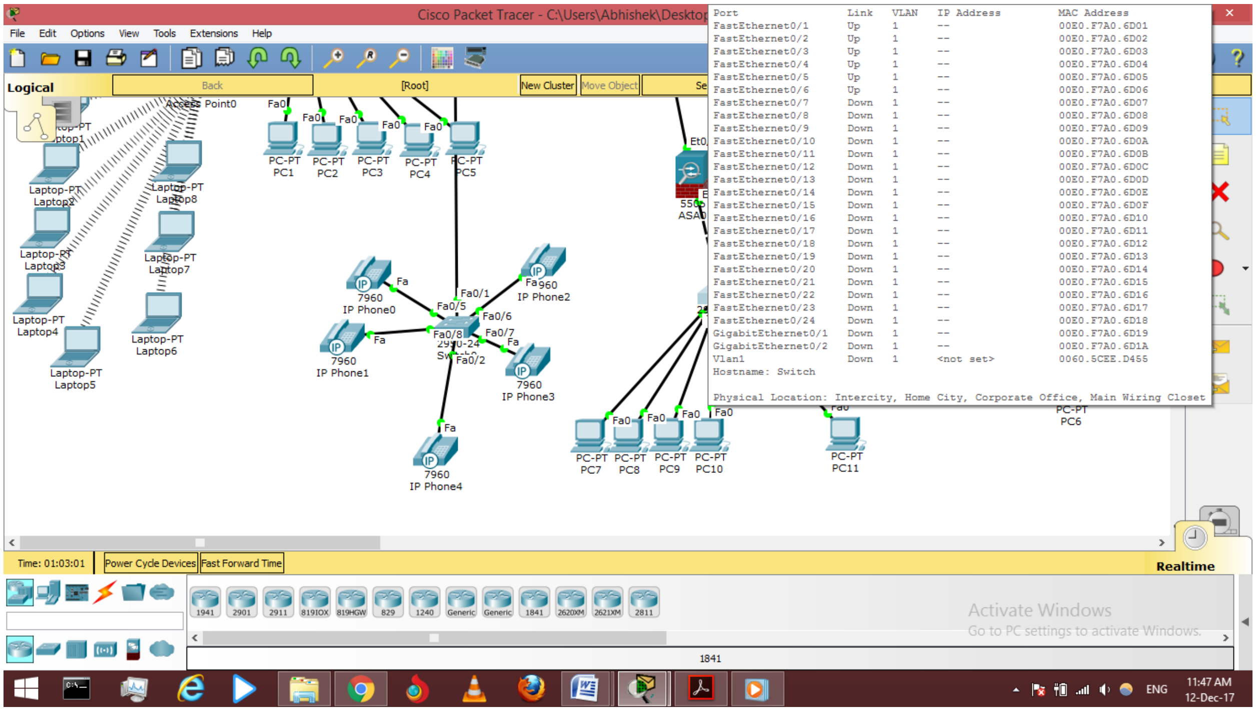


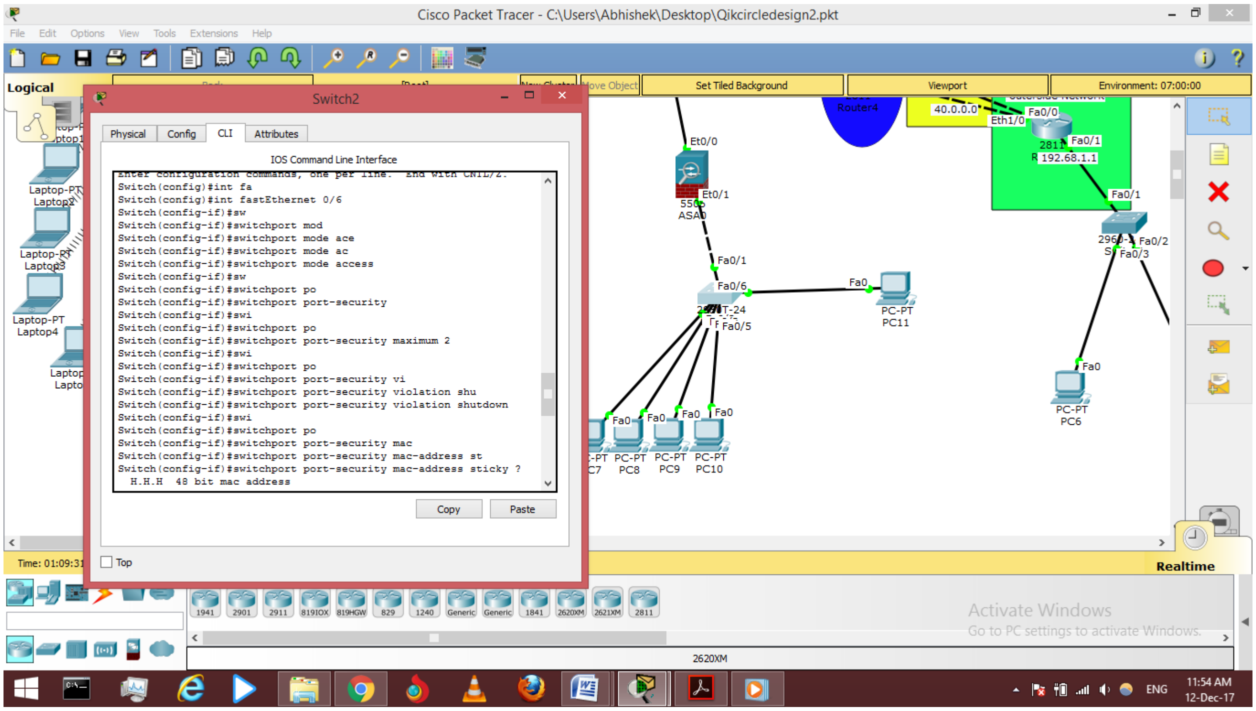
Fig4.3- virtual private network

OUTPUT PAGES



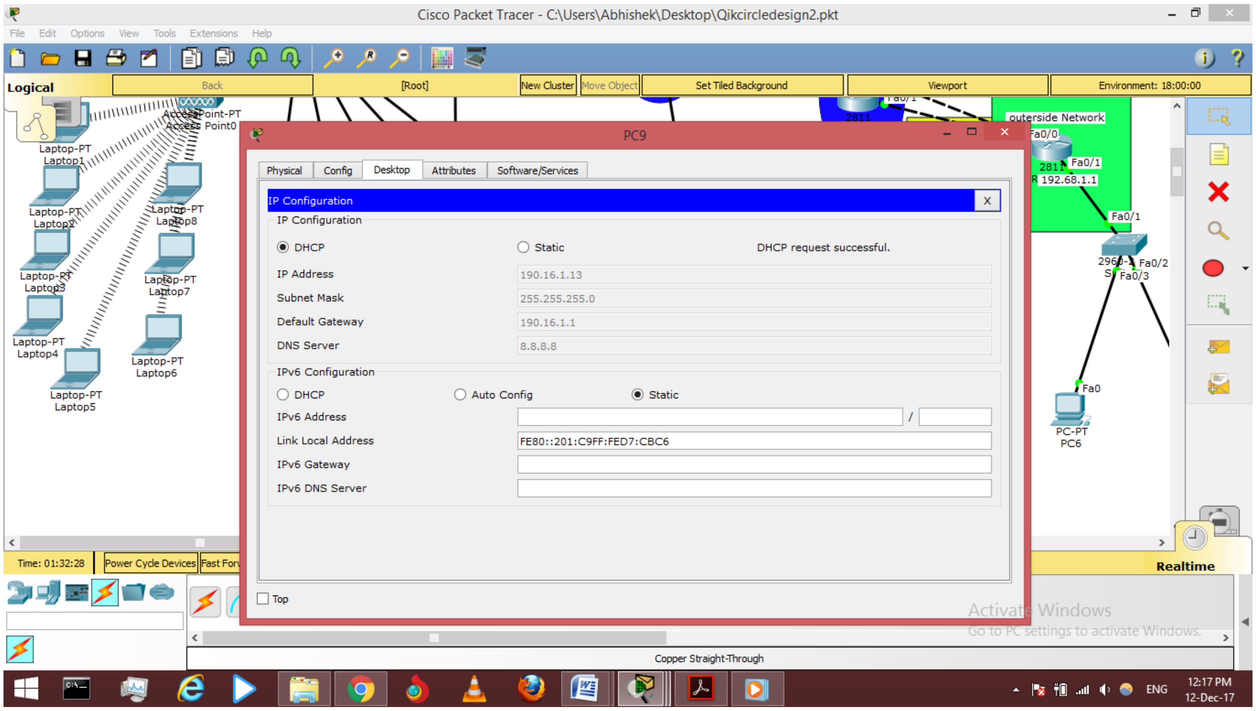
```
Port                 Link   VLAN  IP Address         MAC Address
FastEthernet0/1      Up     1     --                 00E0.F7A0.6D01
FastEthernet0/2      Up     1     --                 00E0.F7A0.6D02
FastEthernet0/3      Up     1     --                 00E0.F7A0.6D03
FastEthernet0/4      Up     1     --                 00E0.F7A0.6D04
FastEthernet0/5      Up     1     --                 00E0.F7A0.6D05
FastEthernet0/6      Up     1     --                 00E0.F7A0.6D06
FastEthernet0/7      Down   1     --                 00E0.F7A0.6D07
FastEthernet0/8      Down   1     --                 00E0.F7A0.6D08
FastEthernet0/9      Down   1     --                 00E0.F7A0.6D09
FastEthernet0/10     Down   1     --                 00E0.F7A0.6D0A
FastEthernet0/11     Down   1     --                 00E0.F7A0.6D0B
FastEthernet0/12     Down   1     --                 00E0.F7A0.6D0C
FastEthernet0/13     Down   1     --                 00E0.F7A0.6D0D
FastEthernet0/14     Down   1     --                 00E0.F7A0.6D0E
FastEthernet0/15     Down   1     --                 00E0.F7A0.6D0F
FastEthernet0/16     Down   1     --                 00E0.F7A0.6D10
FastEthernet0/17     Down   1     --                 00E0.F7A0.6D11
FastEthernet0/18     Down   1     --                 00E0.F7A0.6D12
FastEthernet0/19     Down   1     --                 00E0.F7A0.6D13
FastEthernet0/20     Down   1     --                 00E0.F7A0.6D14
FastEthernet0/21     Down   1     --                 00E0.F7A0.6D15
FastEthernet0/22     Down   1     --                 00E0.F7A0.6D16
FastEthernet0/23     Down   1     --                 00E0.F7A0.6D17
FastEthernet0/24     Down   1     --                 00E0.F7A0.6D18
GigabitEthernet0/1   Down   1     --                 00E0.F7A0.6D19
GigabitEthernet0/2   Down   1     --                 00E0.F7A0.6D1A
Vlan1                Down   1     <not set>          0060.5CEE.D455
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

FIG 4.4 Basic Topology



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa
Switch(config)#int fastEthernet 0/6
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode ace
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security
Switch(config-if)#swi
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#swi
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation shu
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#swi
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address st
Switch(config-if)#switchport port-security mac-address sticky ?
  H.H.H  48 bit mac address
```

FIG 4.5 Configuring Cisco Switch



IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 190.16.1.13

Subnet Mask 255.255.255.0

Default Gateway 190.16.1.1

DNS Server 8.8.8.8

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

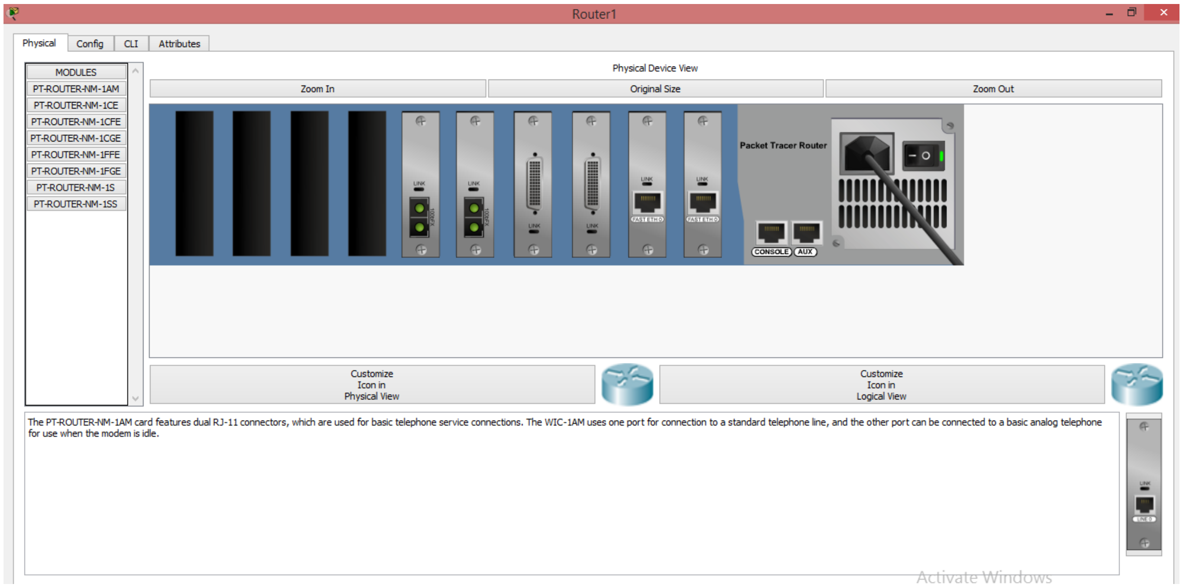
Link Local Address FE80::201:C9FF:FED7:CBC6

IPv6 Gateway

IPv6 DNS Server

□ Top

FIG 4.6 Configuring Client PC's



The PT-ROUTER-NM-1AM card features dual RJ-11 connectors, which are used for basic telephone service connections. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.

FIG 4.7 CiscoRouter back

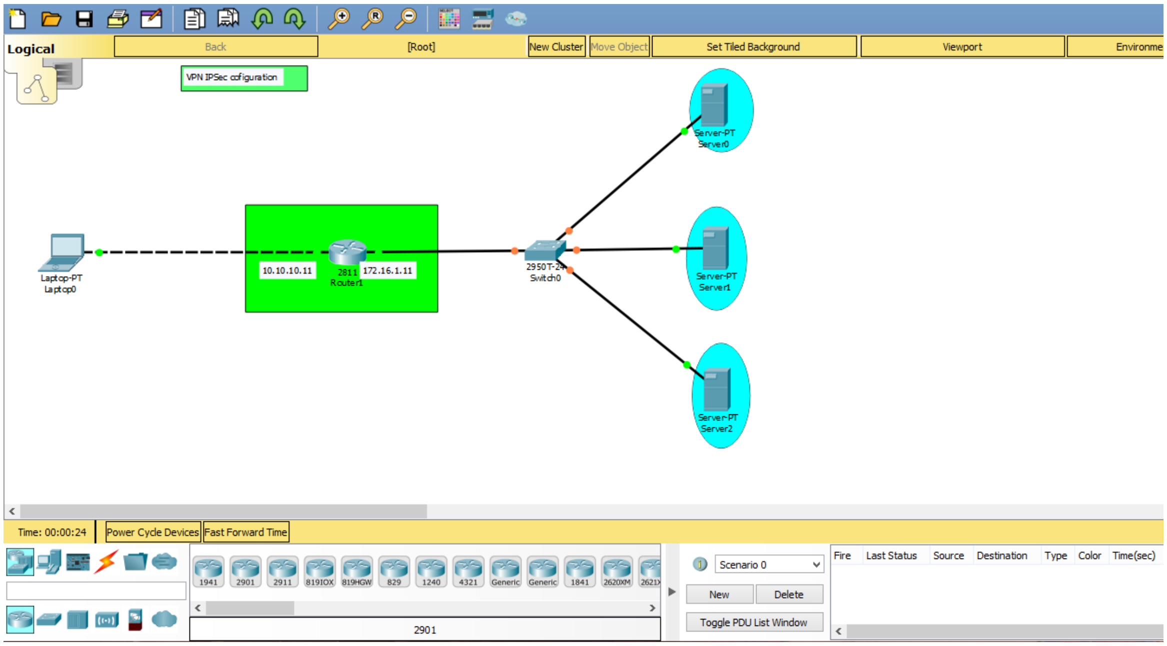


Fig 4.8- VPN

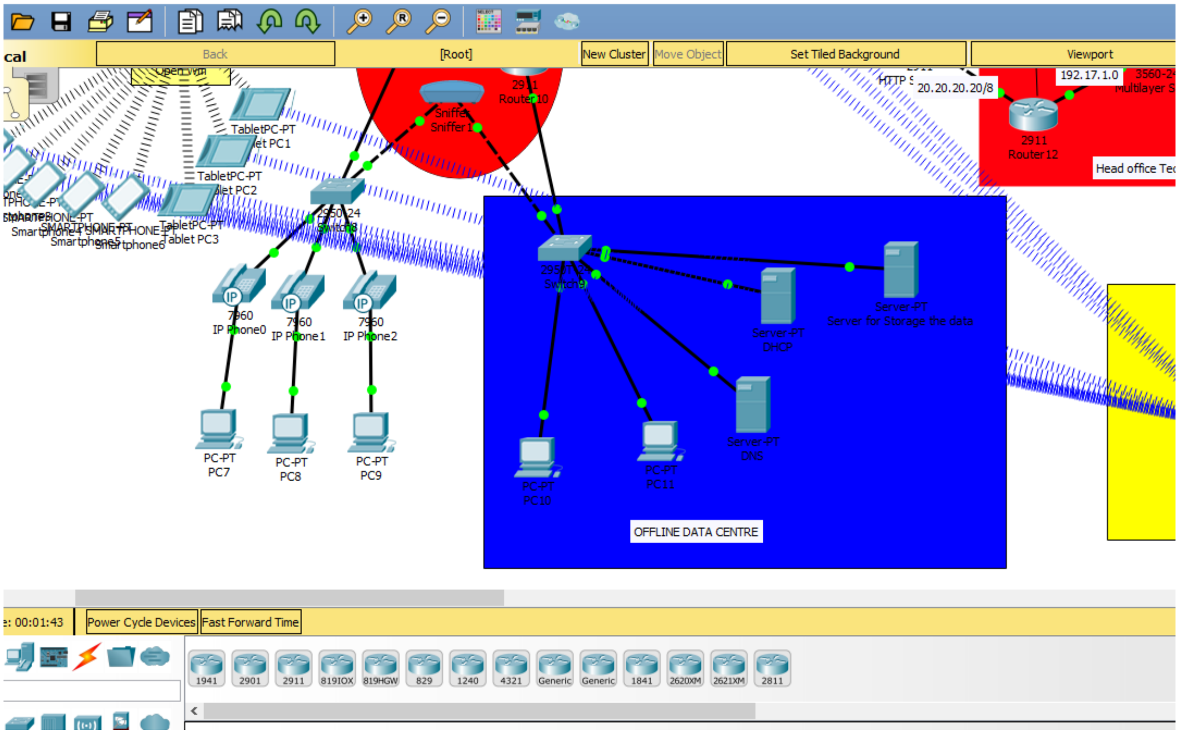


Fig 4.9 offline data center

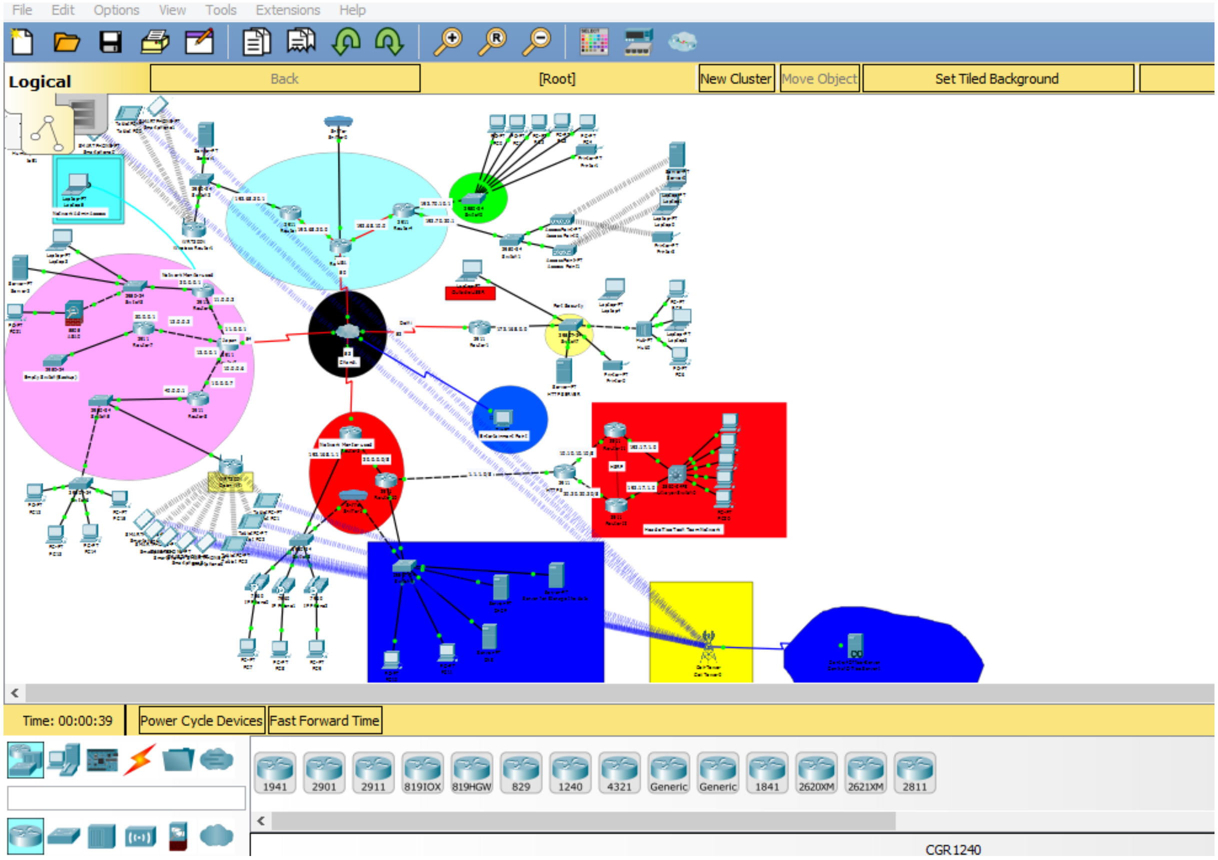


Fig 4.10 Wan module

REFERENCES

1. www.cisco.com/networking/
2. www.searchnetworking.techtarget.com/definition/networking
3. en.wikipedia.org/wiki/ networking
4. CCNA Networking by Todd Lamnle.