

STUDY OF A CORPORATE NETWORK

BY

MD: RATAN MIA

ID: 093-15-863

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Anisur Rahman

Assistant Professor

Department of CSE, CIS & CS
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

OCTOBER 2012

To Whom It May Concern

Oct, 2012

This is to certify that Md. Ratan Mia son of Md Abdul Motalib , ID : 093-15-863, Student of Daffodil International University, Dhanmondi, Dhaka-1207, has undergone an internship program at our Networking department, for period of Jun 2012 to September ,2012.

During the period of internship he worked on .Networking and Configuration of essential servers for an office network. and after completion of the same he has submitted a report to our end.

I wish his every success in future.

MD: Rafiqul Islam
Managing Director
Sigma Oil Industries ltd
Dhaka

APPROVAL

This Internee documentation report on **Study of a Corporate Network** submitted by MD.RATAN MIA, ID: 093-15-863 to the **Department of Computer Science and Engineering, Daffodil International University**, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 21 Oct, 2012.

BOARD OF EXAMINERS

Dr Syed Akhter Hossain Chairman
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr Yousuf Mahbubul Islam Internal
Examiner
Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr Md Kabirul Islam Internal
Examiner
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr Muhammad Shorif Uddin External
Examiner

Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

I hereby declare that, the work presented in internship is **Study of a Corporate Network** has been done by me under the supervision of **Anisur Rahman, Assistant Professor, Department of CSE, CIS & CS** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Anisur Rahman
Assistant Professor
Department of CSE, CIS & CS
Daffodil International University

Submitted by:

Md: Ratan Mia
ID: -093-15-863
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty Allah for His divine blessing makes us possible to complete this project successfully.

We fell grateful to and wish our profound our indebtedness to **Anisur Rahman, Assistant Professor**, Department of CSE,CIS & CS Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of Computer Network influenced us to carry out this project .His endless patience ,scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

I would like to thanks to Md: Rafiqul Islam, Managing Director of Sigma Oil Industries ltd. for his cordial encouragement and help.

We would like to express our heartiest gratitude to **Dr. Sayed Akther Hossain**, Professor and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

This internship is on “**Study of a Corporate Network**”. This is a kind of network using Cisco router, Switch and Different types of server which help a Network Administrator build up a control over the total network.

The aim of the Network is build up a WLAN using broad band router by assign a real IP address. After assigning IP address we configure the DHCP server for the network. When router will configure in DHCP mode every computer will get a IP address automatically. It has a wide variety of uses, from speeding up a web server by caching repeated requests; to caching web, DNS and other computer network lookups for a group of people sharing network resources.

A mail server is a computer that serves as an electronic post office for email. Mail exchanged across networks is passed between mail servers that run specially designed software The most common use of web servers is to host web sites but there are other uses like data storage or for running enterprise applications. FTP operates on the application layer of the OSI model, and is used to transfer files using TCP/IP .In order to do this an FTP server needs to be running and waiting for incoming requests. NFS lowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed.

Output of the system study and working sight then elaborate of all the printable reports including their print screen is attached. Finally this report has shown some limitation of the present system and also few changes that may take place in future to terminate the current limitation of the system.

TABLE OF CONTENTS

CONTENS	PAGE
Board of examiners	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
CHAPTER	
CHAPTER 1: INTRODUCTION	1
1.1 Introduction	1
1.2 Objective	1
CHAPTER 2: ABOUT SIGMA OIL INDUSTRIES LTD	2
2.1 Sigma Oil Industries Ltd.	2
2.2 Objective of doing Internship	2-4
CHAPTER 3: ABOUT COMPUTER NETWORK AND SERVER	5
3.1 Networking	5
3.2 Network Design	5
3.3 Cabling and network device	6-26
3.4 Server	26
CHAPTER 4: NETWORK SIMULATION, CISCO IOS AND IPV4 AND IPV6	27
4.1 Network Simulation	27
4.2 Network Simulator	27-28
4.3 Creating A New Topology	28
4.4 Cisco IOS	29
4.5 CLI Architecture	29-31

4.6 Command Prompt Summary	31-33
4.7 CLI Editor Features	33-33
4.8 Internet Protocol Version 4	33
4.9 Internet Protocol Version 6	33-34
4.10 Difference Between IPv6 And IPv4	34
CHAPTER 5: NETWORK AND ROUTER CONFIGURATION	35
5.1 Network Diagram	35
5.2 Configuring Router	35-36
5.3 Set Hostname and Interface IP Address	37-41
5.4 Routing RIP	41-43
5.5 About Extended ACL	43-44
5.6 Extended ACL for the Network	44
CHAPTER 6: ESSENTIAL SERVER CCONFIGURATION	45
6.1 About Server	45-49
6.2 DHCP Server	50-53
6.3 DNS Server	54-57
6.4 Web Server	57-61
6.5 E-mail Server	61-64
6.6 FTP Server	65

6.7 Configure e-mail Service for Each User	66-67
6.8 Send and Receive E-mail Between two Users	68
CHAPTER 7: CONCLUSION	68
7.1 Conclusion	69
REFERENCES	

LIST OF FIGURE

FIGURES	PAGE
Figure:2.1 Ground Floor in Sigma Oil Ltd.	3
Figure:2.2 1 st Floor in Sigma Oil Ltd.	4
Figure.3.1 Unshielded Twisted Pair (UTP) Cable	7
Figure.3.2 Straight-through connection	7
Figure.3.3 Cross-over Connection	8
Figure.3.4 Rollover Connection	8
Figure.3.5 RJ45 Connector	9
Figure.3.6 Shielded Twisted Pair (STP) Cable	10
Figure.3.7 Coaxial Cable	10
Figure.3.8 Fiber Optic Cable	11
Figure.3.9 Single-mode Optical fiber	12
Figure.3.10 Multimode Optical fiber	13
Figure.3.11 Fiber media connectors	14
Figure. 3.12 Hub	15
Figure.3.13 Unmanaged switch	16
Figure.3.14 Managed switch	17
Figure.3.15 Media Converter	19
Figure.3.16 Router (Cisco 7200 VXR)	17
Figure.3.17 Internal components of a Router	21
Figure.3.18 Router external connections (Interface)	22

Figure.3.19 Router external connections (connectors)	23
Figure.3.20 Bandwidth Management	26
Figure 4.1: Packet Tracer Outlook	28
Figure 4.2: IOS CLI hierarchy	30
Figure 5.1: Full Network Diagram	35
Figure 5.2: Set Host Name and Ip	40
Figure 5.3: Set ip in Fastethernet	40
Figure 5.4: Set ip in Interface Serial	41
Figure 5.5: Router RIP CLI Mode	43
Figure 6.3:DHCP Set First Ethernet IP	47
Figure 6.4: Set DHCP IP	48
Figure 6.5: IP configure Using DHCP	49
Figure 6.6: IP configure Successful	49
Figure.22 How DNS server work	50
Figure 6.8: DNS FastEthernet IP Setting	52
Figure 6.9: DNS Service Setup	53
Figure. 25 How the web browser and web client interact	55
Figure 6.11: WEB Server	56
Figure 6.12: WEB Server HTTP Settings	57
Figure. 24 How Mail server work	58
Figure 6.14: E-mail Server	59
Figure 6.6 E-mail Settings in E-mail Server	61

Figure. 26 How FTP server is connected with client	62
Figure 6.17: FTP Server Global Settings	63
Figure 6.18 FTP Server User Setup	64
Figure 6.19: Configure e-mail Account	65
Figure 6.20: Send E-mail From one Host to Other Host	66
Figure 6.21: Successfully Receive Mail	67

CHAPTER 1: INTRODUCTION

1.1 OVERVIEW:

First and foremost, internships and co-ops help you gain experience. Classroom knowledge is important and makes you competitive for internships, but practical knowledge in an industry is what attracts employers. Internship is the requirements for the Degree of Bachelor of Science in Computer Science and Engineering. It is essential part of study. The Internet has gone from near-invisibility to near-ubiquity in little more than a year. Computer networking or data communication is a most important part of the information technology. Today every business in the world needs a computer network for smooth operations, flexibly, instant communication and data access. A computer network is comprised of connectivity devices and components. To share data and resources between two or more computers is known as networking. There are different types of a computer network such as LAN, MAN, WAN and wireless network. The key devices involved that make the infrastructure of a computer network are Hub, Switch, Router, Modem, Access point, LAN card and network cables.

1.2 OBJECTIVE:

During the internship period, we can gather practical knowledge and actual working experience. So that we can work confidently after successfully completion our graduation. Doing an internship significantly increases your networking opportunities by connecting you with professionals in your chosen field. Networking also allows you to develop references who can attest to your abilities. We have worked to build a server platform for all kinds of essential servers for official use. Those servers are very important for office and corporate area. The main objective of my internship was to create a highly functional, security enforced, multi segmented LAN design for 48 users. I successfully completed this objective by implementing stronger security by creating access-control lists on the routers, firewalls, and VLAN's for the switches. In addition, a private addressing scheme was designed in the "internal" network and a public addressing scheme on the "external" boundary of the network. A large portion of my time was spent researching LAN design, Enhanced Gateway Routing Protocol (RIP), which is a Cisco proprietary routing protocol, and WAN design principles.

CHAPTER 02:

ABOUT SIGMA OIL INDUSTRIES LTD

2.1 SIGMA OIL INDUSTRIES LTD:

Sigma lubricants and Sigma Oil Industries Ltd (SOIL) is a renowned lubricants brand in Bangladesh. They started their business in 2006 within 4 years they becomes a famous brand in Bangladesh. Corporate office are situated in Bangla Bazar and Industries are in Narayangonj.

2.2 OBJECTIVE OF DOING INTERNSHIP:

Computer networking enables the dissemination of information swiftly and effortlessly across the globe via computer and internet. Computer networking is the branch of engineering which helps in setting up communications between computer systems and related devices. It may be seen as an interdisciplinary field with IT, computer engineering, computer science and telecommunication. Networking is changing the world of consumer electronics, biomedicine, industrial automation, supercomputing and defense. Knowledge of computer hardware is the foundation for a career in computer networking. Sigma Oil Industries Ltd. hosted their all servers on Windows system. They have Different type of server , bandwidth management system and local network. They need configuration and maintenance. By configuring those router, servers and implementation we can know about various types of servers and routing. Beside it , we can know how actual servers act and perform their task considering stability and performance. Practical implementation of their configuration and testing can give confidence and real world experience.

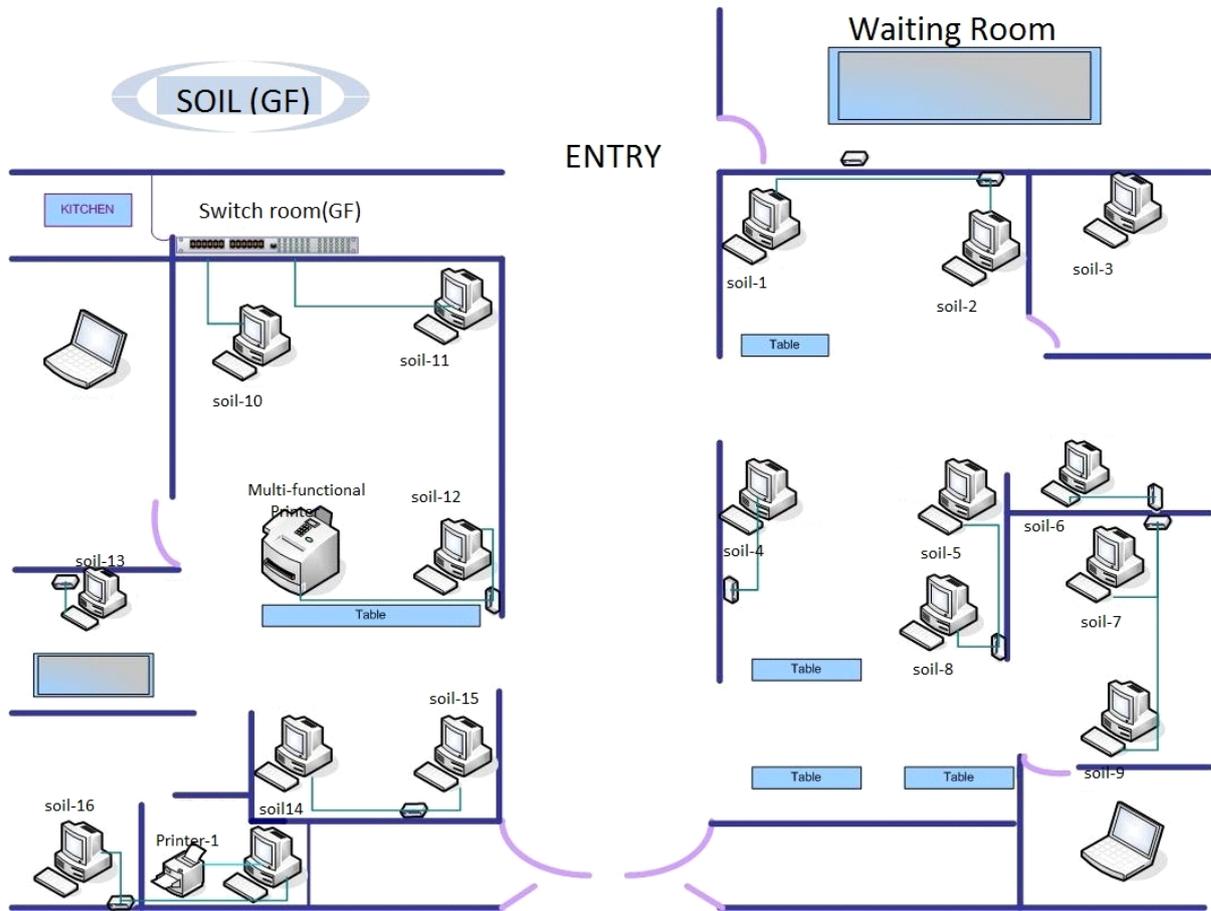


Figure:2.1 Ground Floor in Sigma Oil Ltd.

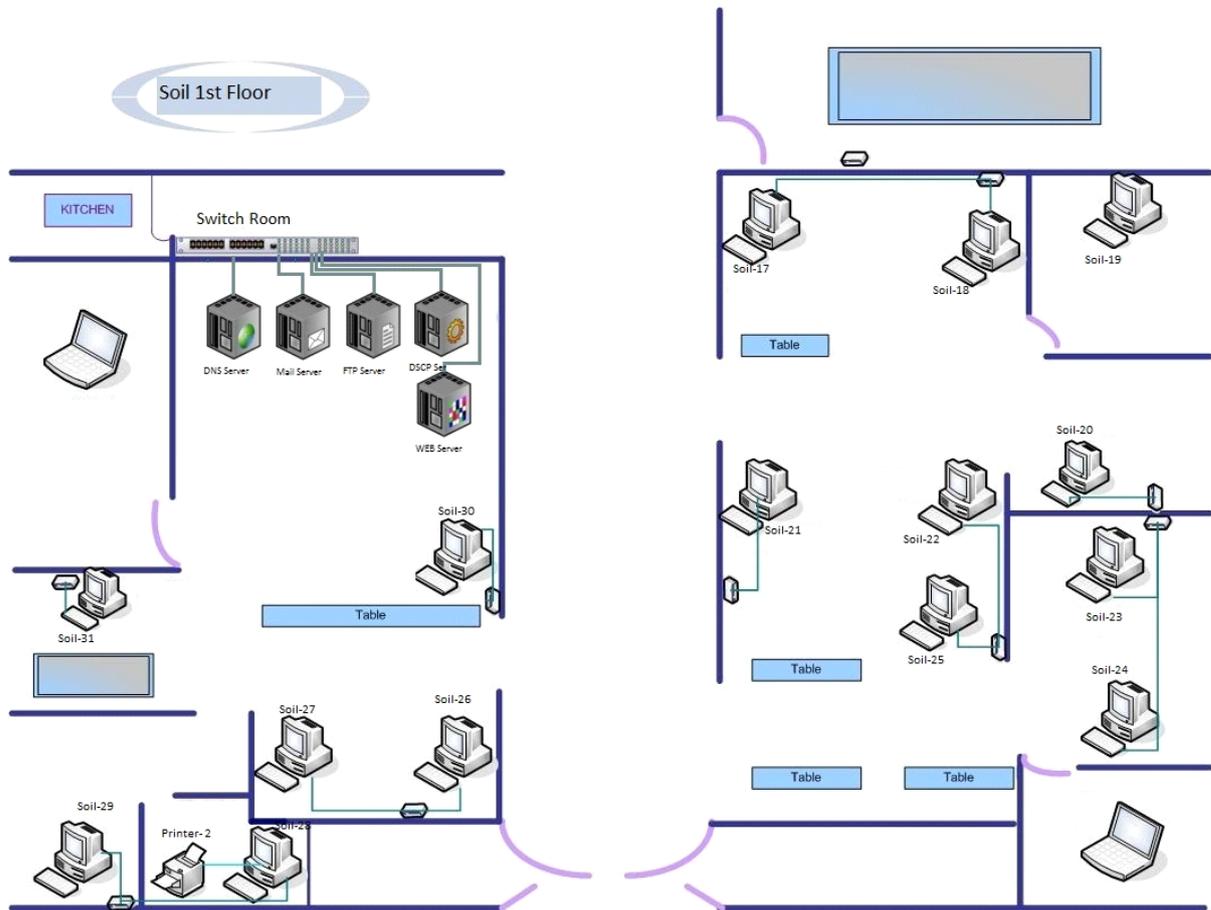


Figure:2.2 1st Floor in Sigma Oil Ltd.

CHAPTER 03:

ABOUT COMPUTER NETWORK AND SERVER

3.1 NETWORKING:

A group of computers and other devices, such as printers and scanners, connected by a communications link, enabling all the devices to interact with each other. Networks can be small or large, permanently connected through wires or cables, or temporarily connected through phone lines or wireless transmissions. The largest network is the Internet, which is a worldwide group of networks. In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. Networks can be categorized in several different ways. One approach defines the type of network according to the geographic area it spans. Local area networks (LANs), for example, typically reach across a single home, whereas wide area networks (WANs), reach across cities, states, or even across the world. The Internet is the world's largest public WAN.

3.2 NETWORK DESIGN:

Computer networks also differ in their design. The two types of high-level network design are called client-server and peer-to-peer. Client-server networks feature centralized server computers that store email, Web pages, files and or applications. On a peer-to-peer network, conversely, all computers tend to support the same functions. Client-server networks are much more common in business and peer-to-peer networks much more common in homes. A network topology represents its layout or structure from the point of view of data flow. In so-called bus networks, for example, all of the computers share and communicate across one common conduit, whereas in a star network, all data flows through one centralized device. Common types of network topologies include bus, star, ring and mesh.

3.3 CABLING AND NETWORK DEVICE

For LAN/WAN connection, different cables and connectors are used.

Cables: UTP, STP and Fiber optic cable.

Connectors: RJ-45, LC, SC.

Unshielded twisted-pair (UTP)

Unshielded twisted-pair (UTP) cabling, as it is used in Ethernet LANs, consists of four pairs of color-coded wires that have been twisted together and then encased in a flexible plastic sheath. As seen in the figure (3.1), the color codes identify the individual pairs and wires in the pairs and aid in cable termination. UTP is a four-pair wire medium used in a variety of networks. Each of the eight copper wires in the UTP cable is covered by insulating material. In addition, each pair of wires is twisted around each other. This type of cable relies on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by EMI and RFI. To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. Like STP cable, UTP cable must follow precise specifications as to how many twists or braids are permitted per foot of cable.

TIA/EIA-568-B.2 contains specifications that govern cable performance. It involves the connection of two cables, one for voice and one for data, to each outlet. The cable for voice must be four-pair UTP. Category 5 is the cable most frequently recommended and implemented in installations. However, analyst predictions and independent polls indicate that Category 6 cable will supersede Category 5 cable in network installations. The fact that Category 6 link and channel requirements are backward compatible to Category 5e makes it very easy for customers to choose Category 6 and supersede Category 5e in their networks. Applications that work over Category 5e will work over Category 6. UTP cable has many advantages. It is easy to install and is less expensive than other types of networking media. In fact, UTP costs less per meter than any other type of LAN cabling

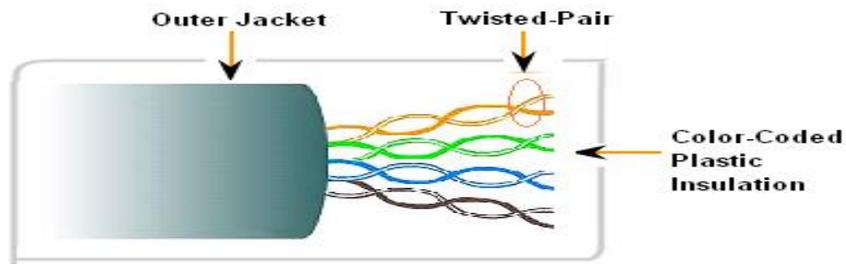


Figure.3.1 Unshielded Twisted Pair (UTP) Cable

UTP Cable Types

UTP cabling, terminated with RJ-45 connectors, is a common copper-based medium for interconnecting network devices, such as computers, with intermediate devices, such as routers and network switches. The following are main cable types that are obtained by using specific wiring conventions:

- Ethernet Straight-through
- Ethernet Crossover
- Rollover

Straight Through Connection: A straight-through network cable is just what the name implies, a cable that passes data straight through from one end to another. Straight-through cables are used for a variety of connections. where each pin is connected to the same pin at the other end.

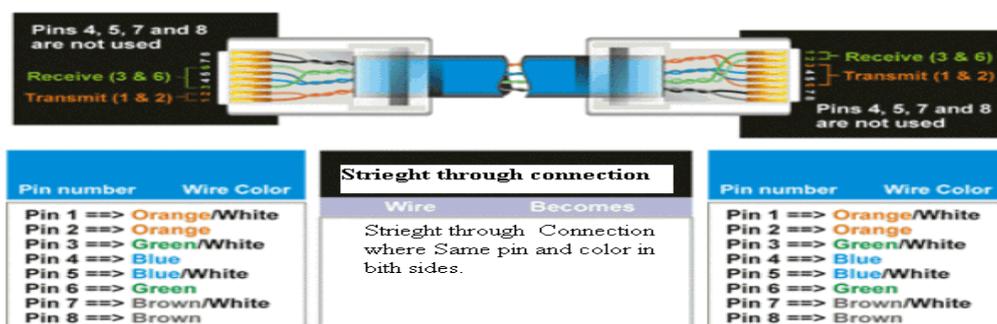


Figure.3.2 Straight-through connection

Cross-over: A crossover cable connects two similar items, computers (nic to nic), router to router and so on. where pins (1, 2) are connected to (3, 6) at the other end, and vice-versa.

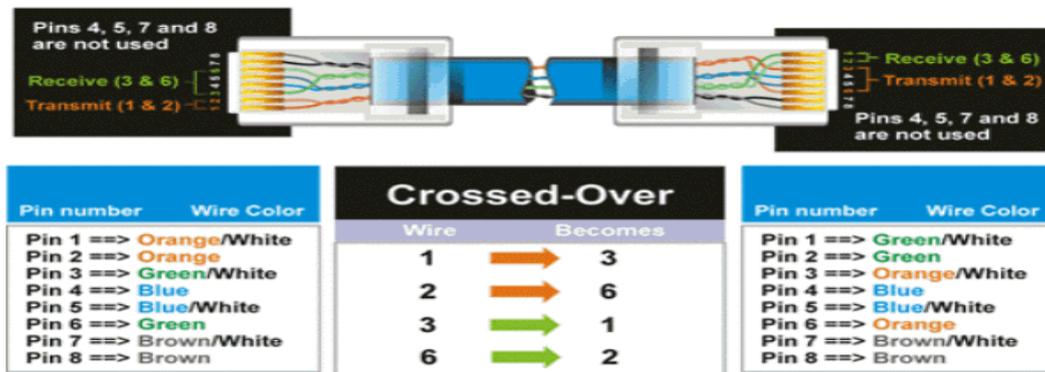


Figure.3.3 Cross-over Connection

A straight cable is for hooking up two components that aren't the same, a computer to a router, switch or hub. A crossover cable connects two similar items, computers(nic to nic),router to router and so on. The difference in the two is pinout of the cable ends or plugs they are both made out of the same cable and use the same ends. With other configurations, the general rule is that NIC-to-hub needs a straight-through cable, but NIC-to-NIC and hub-to-hub require cross-over cables.

Rollover : A null-modem cable that is most commonly used to connect a computer terminal to a router's or switch's console port.

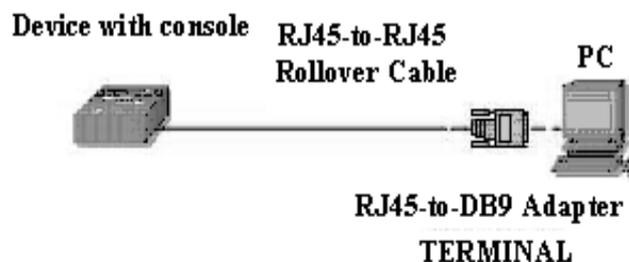


Figure.3.4 Rollover Connection

UTP Connector

RJ45 (Registered Jack 45) is a standard type of connector for network cables. RJ45 connectors are most commonly seen with Ethernet cables and networks. RJ45 connectors feature eight pins to which the wire strands of a cable interface electrically. Standard RJ-45 pinouts define the arrangement of the individual wires needed when attaching connectors to a cable. Several other kinds of connectors closely resemble RJ45 and can be easily confused for each other. The RJ-11 connectors used with telephone cables, for example, are only slightly smaller (narrower) than RJ-45 connectors.

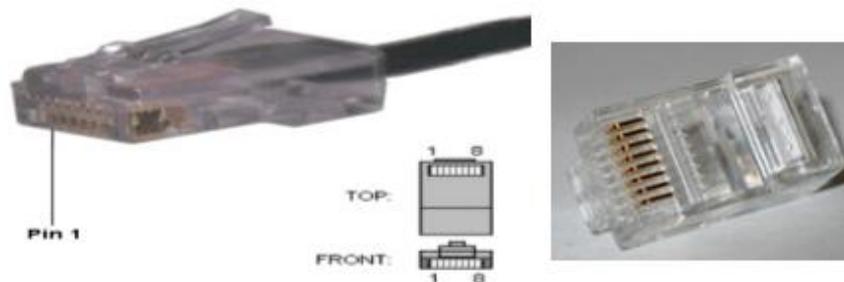


Figure.3.5 RJ45 Connector

STP cable

Another type of cabling used in networking is shielded twisted-pair (STP). As shown in the figure, STP uses two pairs of wires that are wrapped in an overall metallic braid or foil. STP cable shields the entire bundle of wires within the cable as well as the individual wire pairs. STP provides better noise protection than UTP cabling, however at a significantly higher price. For many years, STP was the cabling structure specified for use in Token Ring network installations. With the use of Token Ring declining, the demand for shielded twisted-pair cabling has also waned. The new 10 GB standard for Ethernet has a provision for the use of STP cabling. This may provide a renewed interest in shielded twisted-pair cabling.

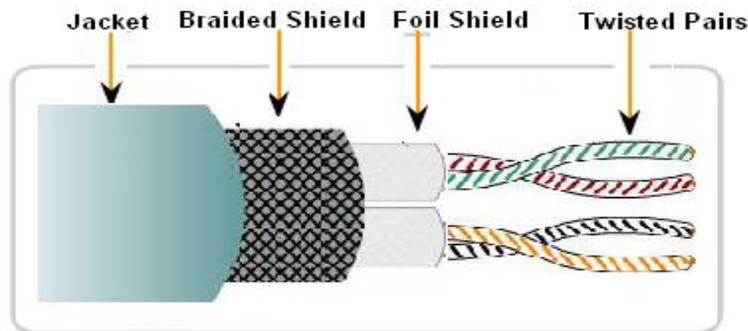


Figure.3.6 Shielded Twisted Pair (STP) Cable

Coaxial cable

Coaxial cable consists of a copper conductor surrounded by a layer of flexible insulation. The center conductor can also be made of tin plated aluminium cable allowing for the cable to be manufactured inexpensively. Over this insulating material is a woven copper braid or metallic foil that acts as the second wire in the circuit and as a shield for the inner conductor. This second layer or shield also reduces the amount of outside electromagnetic interference. Covering this shield is the cable jacket.

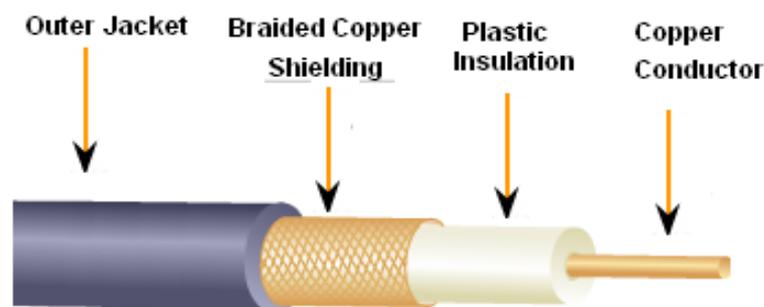


Figure.3.7 Coaxial Cable

For LANs, coaxial cable offers several advantages. It can be run longer distances than shielded twisted pair, STP, unshielded twisted pair, UTP, cable without the need for repeaters. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less expensive than fiber-optic cable and the technology is well known. It has been used for many years for many types of data communication

such as cable television. Coaxial cable is more expensive to install than twisted-pair cable.

Fiber Optic Cable

Fiber-optic cabling uses either glass or plastic fibers to guide light impulses from source to destination. The bits are encoded on the fiber as light impulses. Optical fiber cabling is capable of very large raw data bandwidth rates. Most current transmission standards have yet to approach the potential bandwidth of this media. Given that the fibers used in fiber-optic media are not electrical conductors, the media is immune to electromagnetic interference and will not conduct unwanted electrical currents due to grounding issues. Because optical fibers are thin and have relatively low signal loss, they can be operated at much greater lengths than copper media, without the need for signal regeneration. Some optical fiber Physical layer specifications allow lengths that can reach multiple kilometers.

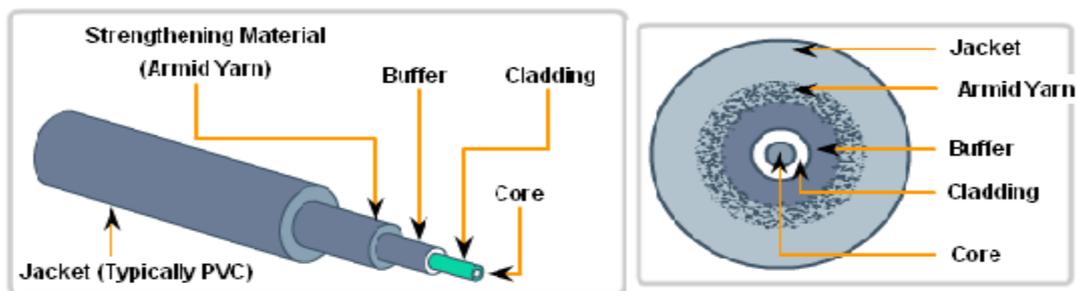


Figure.3.8 Fiber Optic Cable

Optical fiber media implementation issues include:

- More expensive (usually) than copper media over the same distance (but for a higher capacity).
- Different skills and equipment required to terminate and splice the cable infrastructure.
- More careful handling than copper media.

At present, in most enterprise environments, optical fiber is primarily used as backbone cabling for high-traffic point-to-point connections between data distribution

facilities and for the interconnection of buildings in multi-building campuses. Because optical fiber does not conduct electricity and has low signal loss, it is well suited for these uses.

Fiber optic cables can be broadly classified into two types:

- Single-mode and
- Multimode.

Single -mode

Single-mode optical fiber carries a single ray of light, usually emitted from a laser. Because the laser light is uni-directional and travels down the center of the fiber, this type of fiber can transmit optical pulses for very long distances.

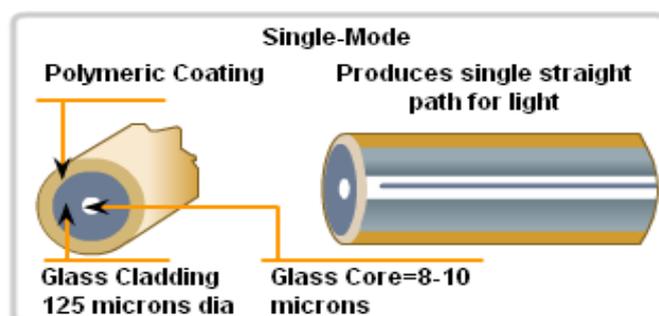


Figure.3.9 Single-mode Optical fiber

Multimode

Multimode fiber typically uses LED emitters that do not create a single coherent light wave. Instead, light from an LED enters the multimode fiber at different angles. Because light entering the fiber at different angles takes different amounts of time to travel down the fiber, long fiber runs may result in the pulses becoming blurred on reception at the receiving end. This effect, known as modal dispersion, limits the length of multimode fiber segments. Multimode fiber and the LED light source used with it, are cheaper than single-mode fiber and its laser-based emitter technology.

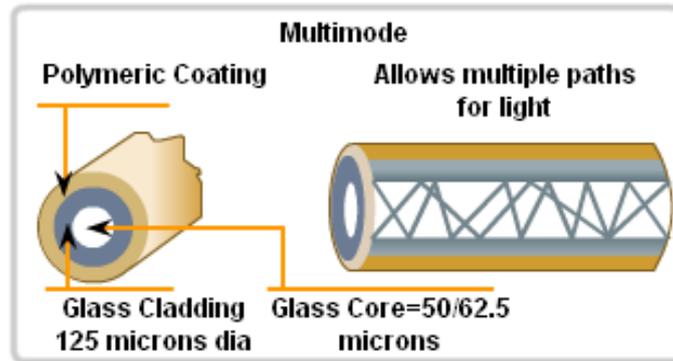


Figure.3.10 Multimode Optical fiber

Common Optical Fiber Connectors

Fiber-optic connectors come in a variety of types. The figure shows some of the most common:

Straight-Tip (ST) (trademarked by AT &T) - A very common bayonet style connector widely used with multimode fiber.

Subscriber Connector (SC)- A connector that uses a push-pull mechanism to ensure positive insertion. This connector type is widely used with single-mode fiber.

Lucent Connector (LC)- A small connector becoming popular for use with single-mode fiber and also supports multi-mode fiber.

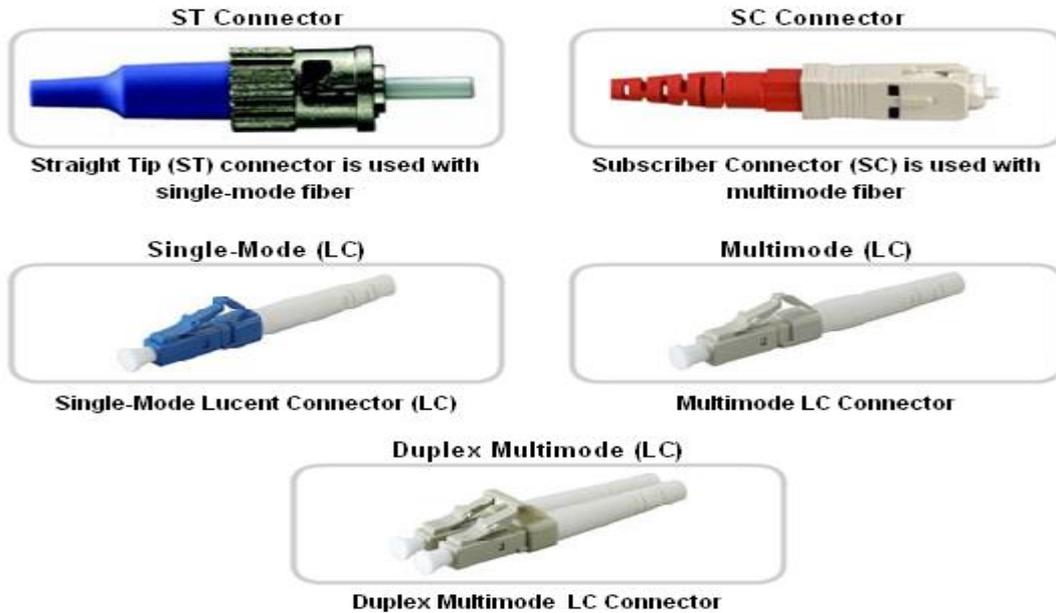


Figure.3.11 Fiber media connectors

HUB

Hub is an intermediary network device that enables more nodes to connect to the shared media. Also known as multi-port repeaters, hubs retransmit received data signals to all connected devices, except the one from which it received the signals. A common connection points for devices in a network. Hubs are commonly used to connect segments of a LAN. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Hubs classify as Physical layer (Layer 1) devices in the OSI model. At the physical layer, hubs can support little in the way of sophisticated networking. Hubs and repeaters are intermediary devices that extend the distance that Ethernet cables can reach. Because hubs operate at the Physical layer, dealing only with the signals on the media, collisions can occur between the devices they connect and within the hubs themselves. Hubs do not read any of the data passing through them and are not aware of their source or destination. Essentially, a hub simply receives incoming packets, possibly amplifies the electrical signal, and broadcasts these packets out to all devices on the network including the one that originally sent the packet.

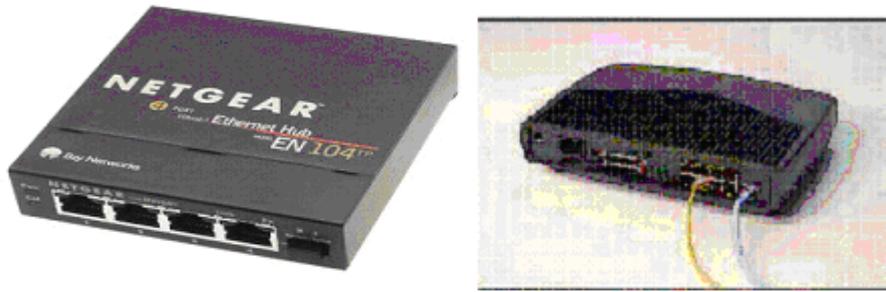


Figure. 3.12 Hub

Further, using hubs to provide network access to more users reduces the performance for each user because the fixed capacity of the media has to be shared between more and more devices. The connected devices that access a common media via a hub or series of directly connected hubs make up what is known as a collision domain. A collision domain is also referred to as a network segment. Hubs and repeaters therefore have the effect of increasing the size of the collision domain. An increased number of collisions reduce the network's efficiency and effectiveness until the collisions become a nuisance to the user.

Hubs come in three basic types

- **Passive** – A passive hub serves as a physical connection point only. It does not manipulate or view the traffic that crosses it. It does not boost or clean the signal. A passive hub is used only to share the physical media. A passive hub does not need electrical power.
- **Active** – An active hub must be plugged into an electrical outlet because it needs power to amplify a signal before it is sent to the other ports.
- **Intelligent** – Intelligent hubs are sometimes called smart hubs. They function like active hubs with microprocessor chips and diagnostic capabilities. Intelligent hubs are more expensive than active hubs. They are also more useful in troubleshooting situations.

Switch

A switch receives a frame and regenerates each bit of the frame on to the appropriate destination port. This device is used to segment a network into multiple collision domains. Unlike the hub, a switch reduces the collisions on a LAN. Each port on the switch creates a separate collision domain. This creates a point-to-point logical topology to the device on each port. Since it is an external device it becomes part of the hardware peripherals used in the operation of a computer system. This connection is done within an existing Local Area network (LAN) only and is identical to an Ethernet hub in terms of appearance except with more intelligence. These switches not only receive data packets, but also have the ability to inspect them before passing them on to the next computer. That is, they can figure out the source, the contents of the data, and identify the destination as well. Because of this uniqueness; it sends the data to the relevant connected system only, thereby using less bandwidth at high performance rates. Additionally, a switch provides dedicated bandwidth on each port, which can increase LAN performance. A LAN switch can also be used to interconnect network segments of different speeds.

Unmanaged switches: These switches have no configuration interface or options. They are plug and play. They are typically the least expensive switches, found in home or small businesses. They can be desktop or rack mounted.



Figure.3.13 Unmanaged switch

Managed switches: These switches have one or more methods to modify the operation of the switch. Common management methods include: a serial console or command line interface accessed via telnet or Secure Shell, an embedded Simple Network Management Protocol (SNMP) agent allowing management from a remote console or management station, or a web interface for management from a web browser. Examples of configuration changes that one can do from a managed switch include: enable features such as Spanning Tree Protocol, set port speed, create or modify Virtual LANs (VLANs), etc.



Figure.3.14 Managed switch

Advantages of Switches over Hubs

Switches are intelligent devices that can read the data packets that pass through them. By storing the MAC address of each host and its corresponding port in a table, switches ensure that bandwidth is not wasted by intelligently directing traffic. Hubs are dumb devices that do not do any processing. Unlike hubs, switches are modern, fast, and support full-duplex operation. In short, they are much better.

In general, switches are chosen for connecting devices to a LAN. Although a switch is more expensive than a hub, its enhanced performance and reliability make it cost effective. There is a range of switches available with a variety of features that enable the interconnection of multiple computers in a typical enterprise LAN setting.

Differences between Hub and Switch

When a hub receives a packet (chunk) of data at one of its ports from a PC on the network, it transmits (repeats) the packet to all of its ports and, thus, to all of the other PCs on the network. If two or more PCs on the network try to send packets at the same time a collision is said to occur. When that happens all of the PCs have to go through a routine to resolve the conflict. The process is prescribed in the Ethernet Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. Each Ethernet Adapter has both a receiver and a transmitter. If the adapters didn't have to listen with their receivers for collisions they would be able to send data at the same time they are receiving it (full duplex). Because they have to operate at half duplex (data flows one way at a time) and a hub retransmits data from one PC to all of the PCs, the maximum bandwidth is 100 MHz and that bandwidth is shared by all of the PC's connected to the hub. The result is when a person using a computer on a hub downloads a large file or group of files from another computer the network becomes congested. In a 10 MHz 10Base-T network the affect is to slow the network to nearly a crawl. The affect on a small, 100 Mbps (million bits per second), 5-port network is not as significant.

An Ethernet switch automatically divides the network into multiple segments, acts as a high-speed, selective bridge between the segments, and supports simultaneous connections of multiple pairs of computers which don't compete with other pairs of computers for network bandwidth. It accomplishes this by maintaining a table of each destination address and its port. When the switch receives a packet, it reads the destination address from the header information in the packet, establishes a temporary connection between the source and destination ports, sends the packet on its way, and then terminates the connection.

Network Media Converter

Network media converters are used to interconnect different types of cables within an existing network. They receive data from one type of cable and convert the signals for

transmission along another cable type. For example, fiber optic media converters allow standard copper based Cat5 and Cat6 LAN networks to work with a fiber optic back bone which provides much higher bandwidth. The most commonly used media converters are twisted pair to fiber media converters. The standard fiber connectors on these media converters are commonly ST or SC connectors. Media converters can connect to network switches, hubs, routers and even direct to computer servers.



Figure.3.15 Media Converter

Router

A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect. It runs software that allows it to move data from one network to another. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts. Routers operate at the network layer (OSI layer 3). There are several companies that make routers: Cisco, Juniper, Nortel (Bay Networks), Red back, Lucent, 3Com, and HP just to name a few.

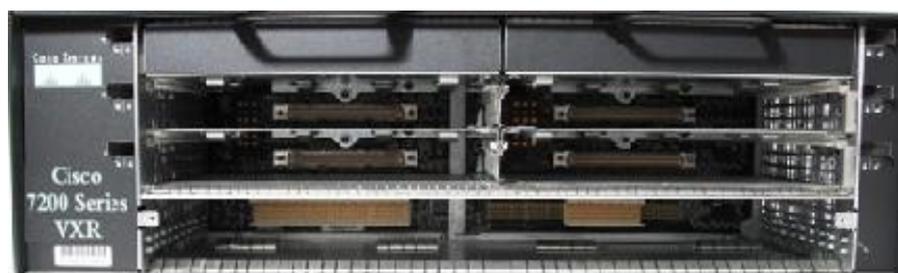


Figure.3.16 Router (Cisco 7200 VXR)

Internal components of Router

While the exact architecture of the router varies between router models, here I will introduce the major internal components. Figures show the internal components of some of the Cisco router models. The common components are as follows:

CPU – The Central Processing Unit (CPU) executes instructions in the operating system. Among these functions are system initialization, routing functions, and network interface control. The CPU is a microprocessor. Large routers may have multiple CPUs.

RAM – RAM is used for routing table information, fast switching caches, running configurations, and packet queues. In most routers the RAM provides run time space for executable Cisco IOS software and its subsystems. RAM is usually logically divided into main processor memory and shared input/output (I/O) memory. Shared I/O memory is shared among interfaces for temporary storage of packets. The contents of RAM are lost when power is removed. RAM is generally dynamic random-access memory (DRAM) and can be upgraded with the addition of dual in-line memory modules (DIMMs).

Flash – Flash memory is used for storage of a full Cisco IOS software image. The router normally acquires the default IOS from flash. These images can be upgraded by loading a new image into flash. The IOS may be in uncompressed or compressed form. In most routers an executable copy of the IOS is transferred to RAM during the boot process. In other routers the IOS may be run directly from flash. The flash single in-line memory modules (SIMMs) or PCMCIA cards can be added or replaced to upgrade the amount of flash.

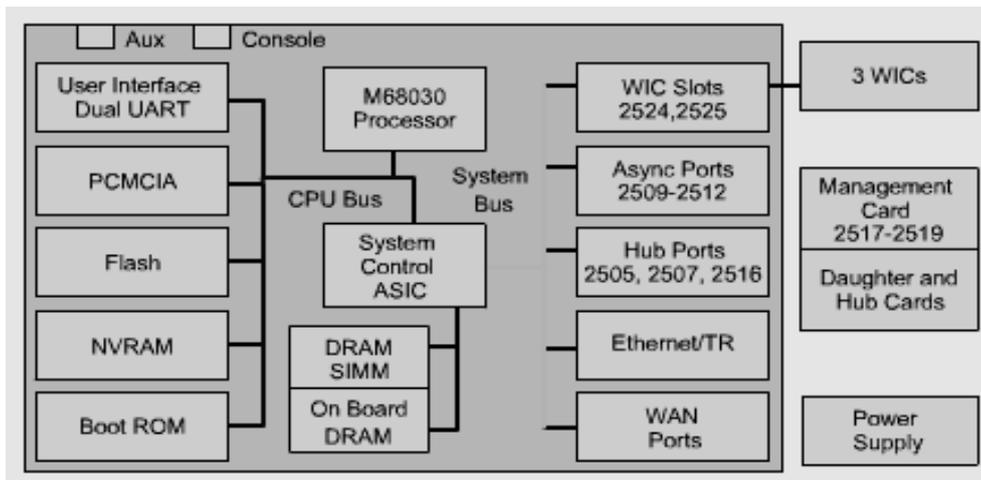


Figure.3.17 Internal components of a Router

NVRAM – NVRAM is used to store the startup configuration. In some devices, EEPROMs can be used to implement NVRAM. In other devices it is implemented in the same flash device from which the boot code is loaded. In either case these devices retain contents when power is removed.

Buses – Most routers contain a system bus and a CPU bus. The system bus is used to communicate between the CPU and the interfaces or expansion slots. This bus transfers the packets to and from the interfaces. The CPU bus is used by the CPU for accessing components from router storage. This bus transfers instructions and data to or from specified memory addresses.

ROM – ROM is used to permanently store the startup diagnostic code, which is called the ROM monitor. The main tasks for ROM are hardware diagnostics during router bootup and loading the Cisco IOS software from flash to RAM. Some routers also have a scaled down version of the IOS that can be used as an alternative boot source. ROMs are not erasable. They can only be upgraded by replacing the ROM chips in the sockets.

Interfaces – The interfaces are the router connections to the outside. The three types of interfaces are LANs, WANs, and console or auxiliary (AUX). The LAN interfaces are usually one of several different varieties of Ethernet or Token Ring. These

interfaces have controller chips that provide the logic for connecting the system to the media. The LAN interfaces may be a fixed configuration or modular.

The WAN interfaces include serial, ISDN, and integrated CSUs. As with LAN interfaces, WAN interfaces also have special controller chips for the interfaces. The WAN interfaces may be a fixed configuration or modular.

The console and AUX ports are serial ports that are used primarily for the initial configuration of a router. They are used for terminal sessions from the communication ports on the computer or through a modem.

Power Supply – The power supply provides the necessary power to operate the internal components. Larger routers may use multiple or modular power supplies. In some of the smaller routers the power supply may be external to the router.

Router external connections

Here I will describe the three basic types of connections on routers, which are LAN interfaces, WAN interfaces, and management ports.

LAN interfaces allow routers to connect to the LAN media. This is usually some form of Ethernet. However, it could be some other LAN technology such as Token Ring or FDDI.

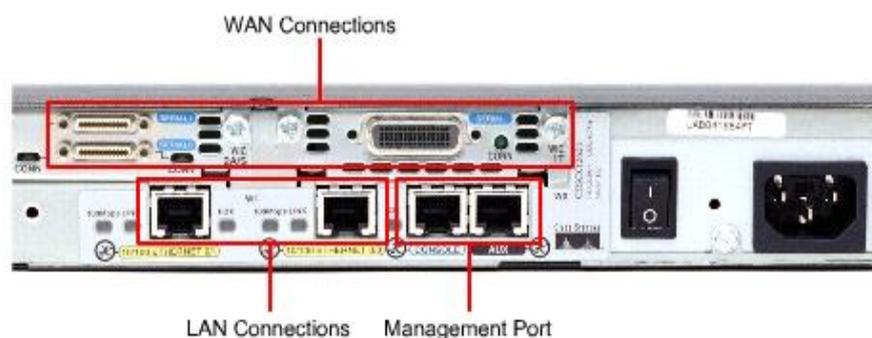


Figure.3.18 Router external connections (Interface)

WANs provide connections through a service provider to a distant site or to the Internet. These may be serial connections or any number of other WAN interfaces. With some types of WAN interfaces, an external device such as a CSU is required to connect the router to the local connection of the service provider. With other types of WAN connections, the router may be directly connected to the service provider.

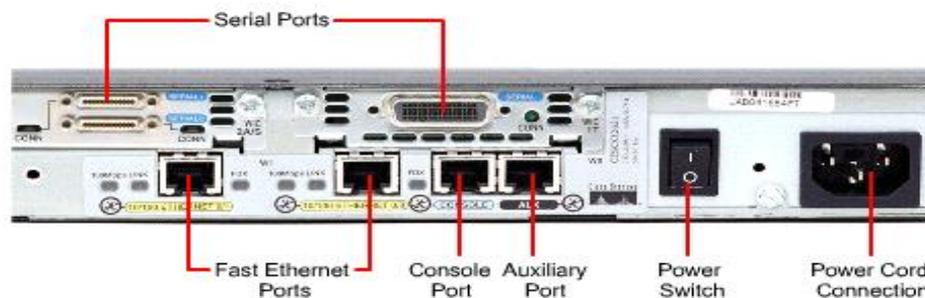


Figure.3.19 Router external connections (connectors)

The function of management ports is different from the other connections. The LAN and WAN connections provide network connections through which packets are forwarded. The management port provides a text-based connection for the configuration and troubleshooting of the router. The common management interfaces are the console and auxiliary ports. These are EIA-232 asynchronous serial ports. They are connected to a communications port on a computer. The computer must run a terminal emulation program to provide a text-based session with the router. Through this session the network administrator can manage the device.

Function of Router

The functions of a router are as follows:

- Restrict network broadcasts to the local LAN
- Act as the default gateway.
- Move data between networks

Restrict Broadcasts to the Local LAN

Networks use broadcast traffic (transmissions sent to all hosts on the network) to communicate certain kinds of information that makes the network function (ARP, RARP, DHCP, IPX-SAP broadcasts etc.). As the number of hosts on the network increases, the amount of what is called "broadcast" traffic increases. If enough broadcast traffic is present on the network, then ordinary communication across the network becomes difficult. To reduce broadcasts, a network administrator can break up a network with a large number of hosts into two smaller networks. Broadcasts are then restricted to each network, and the router performs as the 'default gateway' to reach the hosts on the other networks.

Act as the Default Gateway

Especially in today's networks, people are connecting to the Internet. When your PC wants to talk to a PC on another network, it does so by sending your data to the default gateway (your router). The router receives your data, looks for the remote address of that far-off PC makes a routing decision and forwards your data out a different interface that is closer to that remote PC. There could be several routers between you and the remote PC, so several routers will take part in handing off the packet, much like a fireman's bucket brigade. A router can take in an Ethernet frame, strip the Ethernet data off, and then drop the IP data into a frame of another type. In this way a router can also perform 'protocol conversion', provided it has the appropriate hardware and software to support such a function. The whole point, however, is to forward the data from the interface it receives data on, to another interface that retransmits the received data onto another interface serving another network.

Move Data between Networks

Routers have the capability to move data from one network to another. This allows two networks managed by different organizations to exchange data. They create a network between them and exchange data between the routers on that network. Because a router can accept traffic from any kind of network it is attached to, and

forward it to any other network, it can also allow networks that could not normally communicate with each other to exchange data. In technical terms, a token ring network and an Ethernet network can communicate over a serial network. Routers make all this possible.

Routing Protocols

A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. For a discussion of the concepts behind routing protocols. Many routing protocols used in the public Internet are defined in documents called RFCs. Although there are many types of routing protocols, two major classes are in widespread use in the Internet:

- Link-state routing protocols, such as OSPF and IS-IS; and
- Path vector or distance vector protocols, such as BGP, RIP and EIGRP.

Bandwidth Manager

Nowadays, most of ISP deals with a good volume of bandwidth and users are enjoying broadband Internet connection. ISP provides a specific amount of bandwidth to clients (mostly Corporate and VOIP). It means they allow each client to use specific amount of total Internet bandwidth. So, there must be a limiting process to control usages.

We need to manage our traffic to limit bandwidth overuse by user. It is also important to assure the correct/ committed amount of bandwidth to users. We may also need to make decisions about traffic priority when there is more traffic than the available

bandwidth. If the bandwidth remains open, some clients may not get as much as they had purchased, some will get much more than they had purchased. So, bandwidth management is a significant issue for service.

“Bandwidth Manager” manages bandwidth and controls distribution inconsistency. Bandwidth Manager is a device or, in some cases, software in a computer, that controls the flow of traffic to and from our network. It manages and controls traffic which is traveling through it, based on rules-set. Administrators create and maintain that rules-set on demand. A bandwidth manager takes place between Router and ISP LAN. It controls inbound and outbound bandwidth when traffic transmits to/from Internet. It also works to queue packets for further delivery. Some ISP improves their service enabling QOS (Quality of Service) feature in bandwidth manager.



Figure.3.20 Bandwidth Management

3.4 SERVER:

A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, e.g. "Our mail server is down today, that's why e-mail isn't getting out." A single server machine can (and often does) have several different server software packages running on it, thus providing many different servers to clients on the network.

CHAPTER 04:

NETWORK SIMULATION,CISCO IOS AND IPV4 AND IPV6

4.1 NETWORK SIMULATION:

In communication and computer network research, network simulation is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/routers, data links, packets, etc.) using mathematical formulas, or actually capturing and playing back observations from a production network. The behavior of the network and the various applications and services it supports can then be observed in a test lab; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions. When a simulation program is used in conjunction with live applications and services in order to observe end-to-end performance to the user desktop, this technique is also referred to as network emulation.

4.2 NETWORK SIMULATOR:

A network simulator is a piece of software or hardware that predicts the behavior of a network, without an actual network being present. A network simulator is a software program that imitates the working of a computer network. In simulators, the computer network is typically modeled with devices, traffic etc. and the performance is analyzed. Typically, users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as WLAN, Wi-Max, UDP, and TCP. Examples of notable network simulation software are:

1. OPNET
2. NetSim
3. Cisco Packet Tracer

Cisco Packet Tracer is a Cisco router simulator that can be utilized in training and education, but also in research for simple computer network simulations. The tool is

created by Cisco Systems and provided for free distribution to faculty, students, and alumni who are or have participated in the Cisco Networking Academy. The purpose of Packet Tracer is to offer students and teachers a tool to learn the principles of networking as well as develop Cisco technology specific skills.

4.3 CREATING A NEW TOPOLOGY:

Purpose: The purpose of this lab is to become familiar with building topologies in Packet Tracer.

Requisite knowledge: This lab assumes some understanding of the Ethernet protocol. At this point we have not discussed other protocols, but will use Packet Tracer in later labs to discuss those as well.

Version: This lab is based on Packet Tracer 5.3.

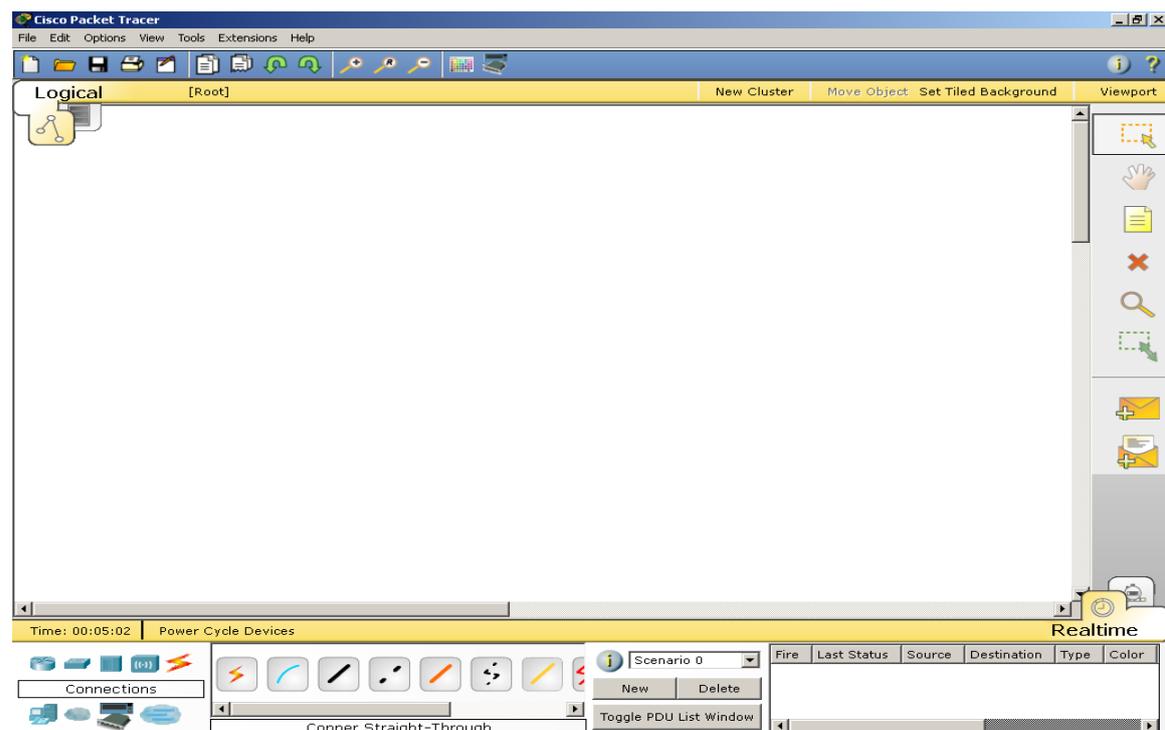


Figure 4.1: Packet Tracer Outlook

4.4 CISCO IOS :

The Cisco IOS is a proprietary kernel that provides routing, switching, internetworking and telecommunications features. The first IOS was written by William Yeager in 1986, and it enabled networked applications.

The Cisco IOS responsible for:

1. Carrying network protocols and functions
2. Connecting high-speed traffic between devices
3. Adding security to control access and stop unauthorized network use
4. Providing scalability for ease of network growth and redundancy
5. Supplying network reliability for connecting to network resources

4.5 CLI ARCHITECTURE

A Cisco IOS router command line interface can be accessed through either a console connection, modem connection, or a telnet session. Regardless of which connection method is used, access to the IOS command line interface is generally referred to as an EXEC session.

Critical commands (e.g. configuration and management) require that the user be at the privileged EXEC level. To change to the privileged EXEC level, type "enable" at the Router> prompt. If an enable password is configured, the router will then prompt for that password. When the correct enable password is entered, the router prompt will change to "Router#" indicating that the user is now at the privileged EXEC level. To switch back to user EXEC level, type "disable" at the Router# prompt. Typing a question mark (?) at the privileged EXEC level will now reveal many more command options than those available at the user EXEC level. The text below illustrates the process of changing EXEC levels.

```
Router> enable
Password: [enable password]
Router# disable
```

Router>

Once an EXEC session is established, commands within Cisco IOS are hierarchically structured. In order to successfully configure the router, it is important to understand this hierarchy. To illustrate this hierarchy, Figure 1 provides a simple high-level schematic diagram of some IOS commands.

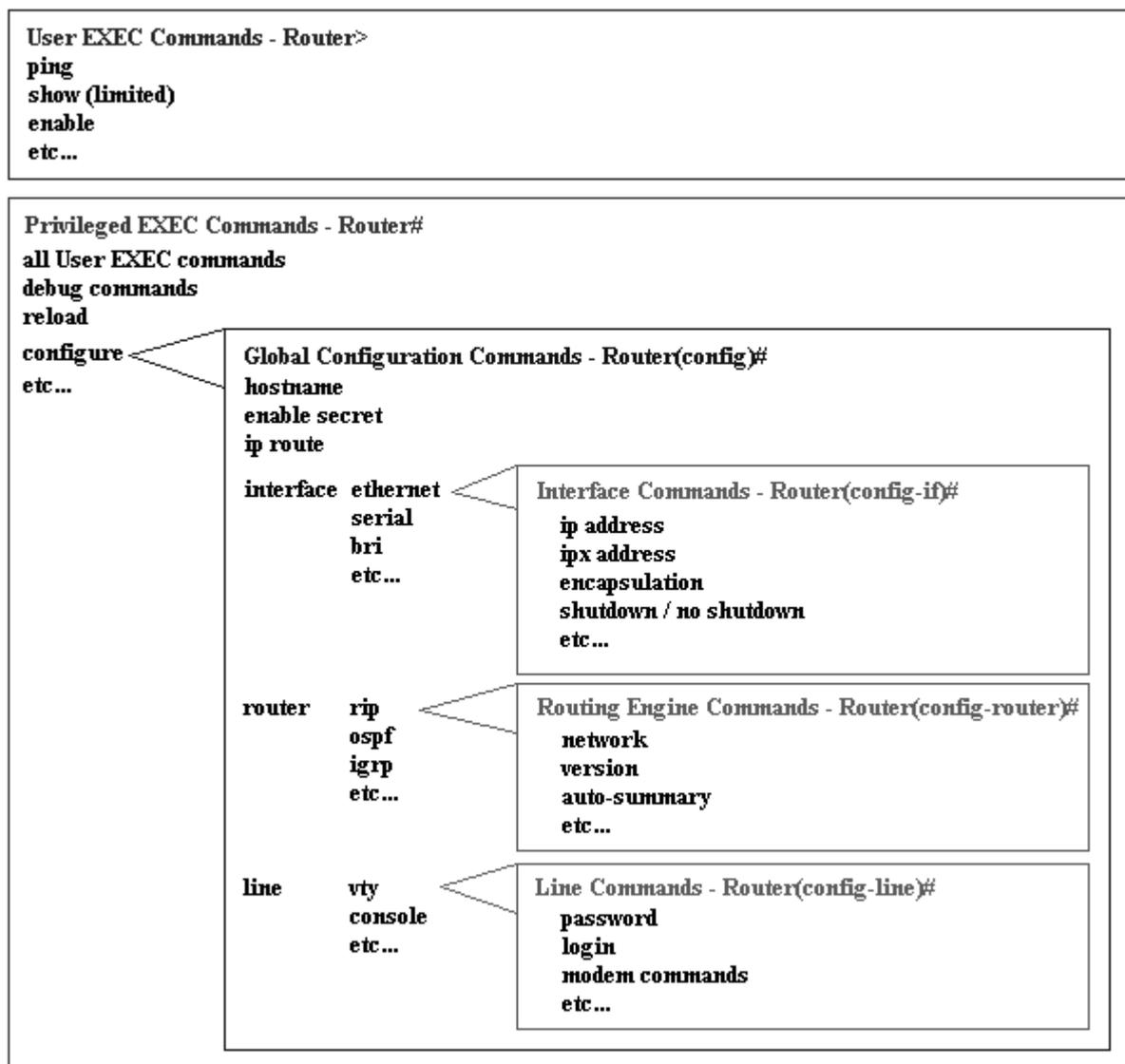


Figure 4.2: IOS CLI hierarchy

4.6 COMMAND PROMPT SUMMARY:

Router>	- User EXEC mode
Router#	- Privileged EXEC mode

Router(config)#	- Configuration mode (notice the # sign indicates this is only accessible at privileged EXEC mode.)
Router(config-if)#	- Interface level within configuration mode.
Router(config-router)#	- Routing engine level within configuration mode.
Router(config-line)#	- Line level (vty, tty, async) within configuration mode.

4.7 CLI EDITOR FEATURES

Context Sensitive Help:

Cisco IOS CLI offers context sensitive help. This is a useful tool for a new user because at any time during an EXEC session, a user can type a question mark (?) to get help. Two types of context sensitive help are available - word help and command syntax help.

Word help can be used to obtain a list of commands that begin with a particular character sequence. To use word help, type in the characters in question followed immediately by the question mark (?). Do not include a space before the question mark. The router will then display a list of commands that start with the characters that were entered. The following is an example of word help:

```
Router# co?
configure connect copy
```

Command syntax help can be used to obtain a list of command, keyword, or argument options that are available based on the syntax the user has already entered. To use command syntax help, enter a question mark (?) in the place of a keyword or argument. Include a space before the question mark. The router will then display a list of available command options with <cr> standing for carriage return. The following is an example of command syntax help:

```
Router# configure ?
memory          Configure from NV memory
```


Summary Of Hot Keys

Delete	- Removes one character to the right of the cursor.
Backspace	- Removes one character to the left of the cursor.
TAB	- Finishes a partial command.
Ctrl-A	- Moves the cursor to the beginning of the current line.
Ctrl-R	- Redisplays a line.
Ctrl-U	- Erases a line.
Ctrl-W	- Erases a word.
Ctrl-Z	- Ends configuration mode and returns to the EXEC.
Up Arrow	- Allows user to scroll forward through former commands.
Down Arrow	- Allows user to scroll backward through former commands.

4.8 INTERNET PROTOCOL VERSION 4

IPv4 (**I**nternet **P**rotocol **V**ersion **4**) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks.

IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^{32} addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device -- including computers, smart phones and game consoles -- that connects to the Internet requires an address.

4.9 INTERNET PROTOCOL VERSION 6

IPv6 (**I**nternet **P**rotocol **V**ersion **6**) is also called IPng (**I**nternet **P**rotocol **n**ext **g**eneration) and it is the newest version of the Internet Protocol (IP) reviewed in the IETF standards committees to replace the current version of IPv4 (Internet Protocol Version 4). IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was

designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted. IPv6 is often referred to as the "next generation" Internet standard and has been under development now since the mid-1990s. IPv6 was born out of concern that the demand for IP addresses would exceed the available supply.

While increasing the pool of addresses is one of the most often-talked about benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (say good-bye to DHCP)

4.10 DIFFERENCE BETWEEN IPv6 AND IPv4 IP

An IP address is binary numbers but can be stored as text for human readers. For example, a 32 bit numeric address (IPv4) is written in decimal as four numbers separated by periods. Each number can be zero to 255. For example, **1.160.10.240** could be an IP address. IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this: **3ffe:1900:4545:3:200:f8ff:fe21:67cf**

CHAPTER 05:

NETWORK DESIGN AND ROUTER CNFIGURATION

5.1 NETWORK DIAGRAM

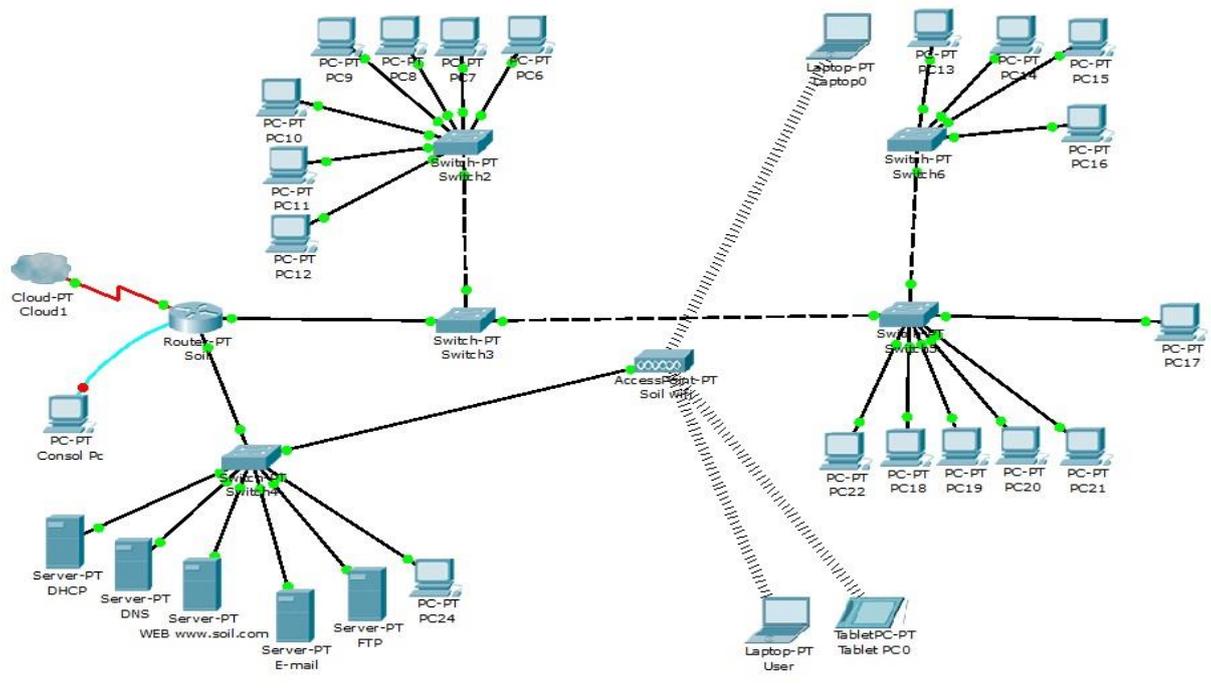


Figure 5.1: Full Network Diagram

5.2 CONFIGURING ROUTER:

The Cisco 2800 series of integrated services routers offers secure, wire-speed delivery of concurrent data, voice, and video services. The modular design of the Cisco 2800 series routers provides maximum flexibility, allowing you to configure your router to meet evolving needs. The Cisco 2800 series routers incorporate data, security, and voice services in a single system for fast, scalable delivery of crucial business applications. The routers offer features such as hardware-based VPN encryption acceleration, intrusion-protection and firewall functions, and optional integrated call processing and voice mail. The routers offer a wide variety of network modules and

interfaces, voice digital signal processor (DSP) slots, high-density interfaces for a wide range of connectivity requirements, and sufficient performance and slot density for future network expansion requirements and advanced applications.

IP ADDRESSING

An IP address is a numeric identifier assigned to each machine on an IP network. It designates the location of a device on the network. An IP address is a software address, not a hardware address the latter is hardware coded on a network interface card (NIC) and used for finding hosts on a local network. IP addressing was designed to allowed a host on one network: to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in.

An IP address consists of 32 bits of information. The 32-bit IP address is a structured or hierarchical address. 32 bits are divided 4 sections. And every section is 8-bit address. And the 32 bits address are divided two parts one is Host section, and another is network section. 32 bits address have also 5 classes, which is...

	Sbits	Sbits	8bits	Sbits	
Class A:	Network	Host	Host	Host	Host
Class B:	Network	Network	Host	Host	Host
Class C:	Network	Network	Network	Host	Host
Class D:	Multicast				
Class E:	Research				

Network address of Class A: 1 to 126

Network address of Class B: 128 to 191

Network address of Class C: 192 to 223

Network address of Class D and E: The address between 224 and 255 are reserved for class D and E networks. Class D is used for multicast address, Class E is used for scientific purpose.

5.3 SET HOSTNAME AND INTERFACE IP ADDRESS:

Step 1- Select the router and click the CLI button from Toolbar

System Bootstrap is started when it's complete the message is shown in the window

```
Continue with configuration dialog? [yes/no]:  
% Please answer 'yes' or 'no'.  
Continue with configuration dialog? [yes/no]: no
```

Step 2- Type “no” and press “enter”

Step 3- Now we are configure Router for the Network using the command line interface

Set HostName FastEthernet0/0 Ip : (Figure 5.2)

```
Soil>  
Soil>enabl  
Soil>enable  
Soil#conf  
Soil#conf ter  
Soil#conf  
Soil#conf ter  
Soil#conf ter  
    ^  
% Invalid input detected at '^' marker.  
  
Soil#conf ter  
Soil#conf terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Soil(config)#int  
Soil(config)#interface fa  
Soil(config)#interface fastEthernet 0/0
```

```
Soil(config-if)#192.168.1.1 255.255.255.0
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
Soil(config-if)#ip add
```

```
Soil(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Soil(config-if)#no shut
```

```
Soil(config-if)#no shutdown
```

```
Soil(config-if)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

Set HostName FastEthernet1/0 Ip : (Figure 5.3)

```
router02>
```

```
router02>enable
```

```
router02>enable
```

```
router02#conf
```

```
router02#conf t
```

```
router02#conf terminal
```

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

```
router02(config)#host
```

```
router02(config)#hostname Soil
```

```
Soil(config)#int
```

```
Soil(config)#interface fast
```

```
Soil(config)#interface fastEthernet 1/
```

```
Soil(config)#interface fastEthernet 1/0
```

```
Soil(config-if)#ip
```

```
Soil(config-if)#ip add
```

```
Soil(config-if)#ip address 172.16.10.1 255.255.0.0
```

```
Soil(config-if)#noshu
```

```
Soil(config-if)#no shu
```

```
Soil(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

Set HostName Interface Serial2/0 Ip(Figure 5.4)

Soil>

Soil>ena

Soil>enable

Soil#conf

Soil#configure te

Soil#configure terminal

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

Soil(config)#int

Soil(config)#interface se

Soil(config)#interface serial 2/0

Soil(config-if)#ip add

Soil(config-if)#ip address 10.10.10.5 255.0.0.0

Soil(config-if)#no shu

Soil(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

Soil(config-if)#

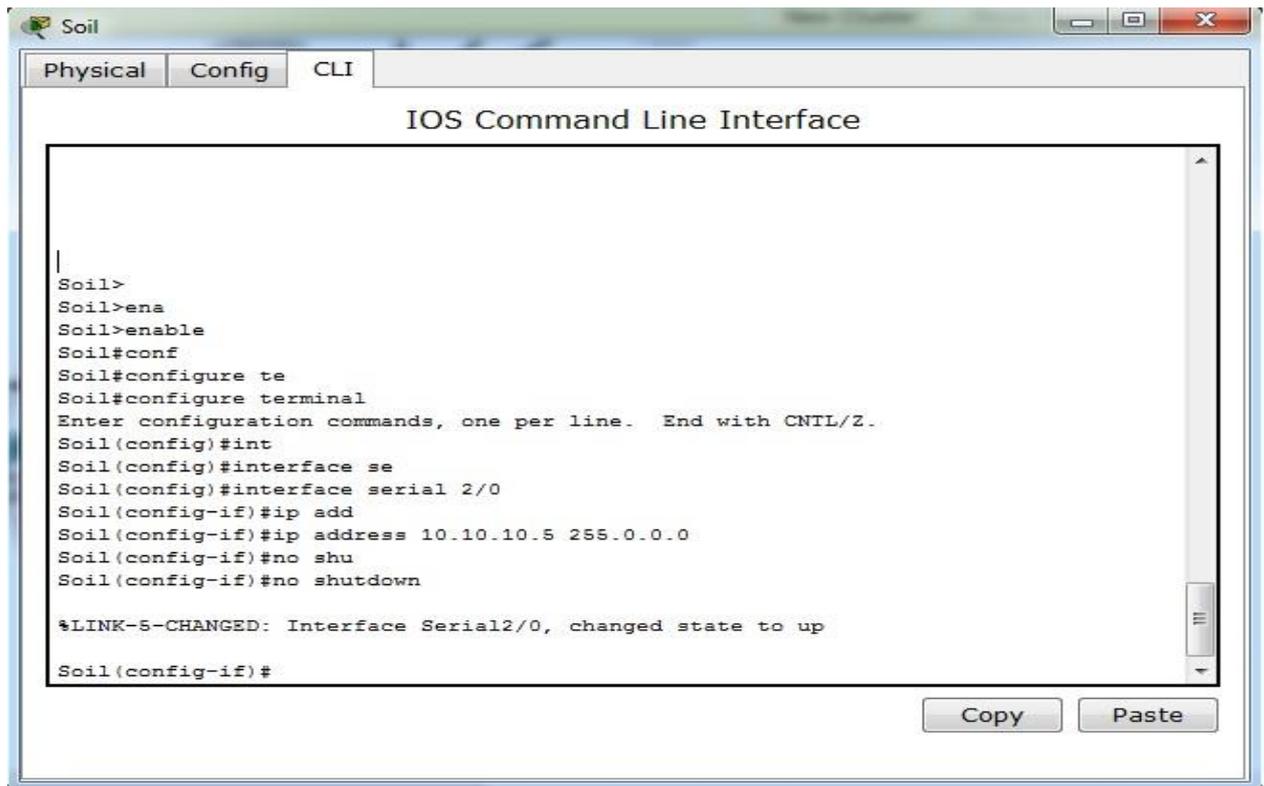


Figure 5.4: Set ip in Interface Serial

5.4 ROUTING RIP:

Routing Information Protocol (RIP) is a standards-based, distance-vector, interior gateway protocol (IGP) used by routers to exchange routing information. RIP uses hop count to determine the best path between two locations. Hop count is the number of routers the packet must go through till it reaches the destination network. The maximum allowable number of hops a packet can traverse in an IP network implementing RIP is 15 hops.

Step 1- Select the router and click the CLI button from Toolbar

Step 2- Now we are configure Router RIP for the Network using the command line interface

```
Soil>ena
Soil>enable
Soil#conf
Soil#configure ter
Soil#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Soil(config)#rou
Soil(config)#router ri
Soil(config)#router rip
Soil(config-router)#net
Soil(config-router)#network 172.16.10.0
Soil(config-router)#network 192.168.1.0
Soil(config-router)#net
Soil(config-router)#network 10.10.10.0
Soil(config-router)#exit
Soil(config)#exit
Soil#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Soil#
Soil#exiyt
Translating "exiyt"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
```

```
Soil>ena
Soil>enable
Soil#conf
Soil#configure ter
Soil#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Soil(config)#rou
Soil(config)#router ri
Soil(config)#router rip
Soil(config-router)#net
Soil(config-router)#network 172.16.10.0
Soil(config-router)#network 192.168.1.0
Soil(config-router)#net
Soil(config-router)#network 10.10.10.0
Soil(config-router)#exit
Soil(config)#exit
Soil#
%SYS-5-CONFIG_I: Configured from console by console

Soil#
Soil#exiyt
Translating "exiyt"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
```

Figure 5.5: Router RIP CLI Mode

5.5 ABOUT EXTENDED ACL

Like standard ACLs, extended ACLs check the source packet addresses, destination address, protocols and port numbers. Extended Access Control Lists (ACLs) provide a greater range of control and, therefore, an addition to your security solution. Extended ACLs provides for more precise traffic-filtering control, you can use extended ACLs numbered 100 to 199 and 2000 to 2699 providing a total of 800 possible extended ACLs. Extended ACLs can also be named.

Extended Access Control Lists Offers a greater range of criteria on which to base the ACL.

For example: you can use extended ACL to simultaneously allow e-mail traffic from a network to a specific destination while denying file transfers and web browsing. A specific built extended ACLs Uses it's logical decisions to filter on source and destination addresses, and protocol and port numbers.

Lets look at it this way; Extended ACLs can be built to:

1. Filter on the source address.
2. Then filter the port and protocol address,
3. Filters on the destination address.

Then on the port and protocol of the destination, then makes a final permit / deny decision.

5.6 EXTENDED ACL FOR THE NETWORK:

Before we configure Extended Access list you should cram up some important port number.

Well-Known Port Numbers and IP Protocols:

Port Number	IP Protocol
20 (TCP)	FTP data
21 (TCP)	FTP control
23 (TCP)	Telnet
25 (TCP)	Simple Mail Transfer Protocol (SMTP)
53(TCP/UDP)	Domain Name System (DNS)
69 (UDP)	TFTP
80 (TCP)	HTTP

Now we are configuring Extended access list. With extended access list we can filter the packets as soon as they generate.

CHAPTER 06:

ESSENTIAL SERVER CCONFIGURATION

6.1 ABOUT SERVER

A system that provides network service such as disk storage and file transfer, or a program that provides such a service. A kind of daemon which performs a service for the requester, which often runs on a computer other than the one which the server runs.

6.2 DHCP SERVER

The Dynamic Host Confirmation Protocol (DHCP) service enables devices on a network to obtain IP addresses and other information from a DHCP server. This service automates the assignment of IP addresses, subnet masks, gateway and other IP networking parameters.

When a computer uses a static IP address, it means that the computer is manually configured to use a specific IP address. One problem with static assignment, which can result from user error or inattention to detail, occurs when two computers are configured with the same IP address. This creates a conflict that results in loss of service. Using DHCP to dynamically assign IP addresses minimizes these conflicts.

A client configured for DHCP will send out a broadcast request to the DHCP server requesting an address. The DHCP server will then issue a "lease" and assign it to that client. The time period of a valid lease can be specified on the server. DHCP reduces the amount of time required to configure clients and allows one to move a computer to various networks and be configured with the appropriate IP address, gateway and subnet mask. For ISP's it conserves the limited number of IP addresses it may use.

DHCP servers may assign a "static" IP address to specified hardware. Many ISPs use dynamic IP addressing for dial-up users.

Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:

Configuring the DHCP Server:

First set connection to the first Ethernet card and second Ethernet card with internal switch.

Step1- Select a server to drag and drop to the workspace

Step 2- Select the server and click the cofig button from the Toolber

Step 3- Click Global Settings and set:

- Display Name to “**DHCP**”,
- Set the Gateway to 172.16.10.1
- Set the DNS Sever 172.16.10.3

Step 4- Click FastEthernet from the Sidebar and set:

- Set the IP address to **172.16.10.2**
- Set the Subnet Mask to **255.255.255.0**

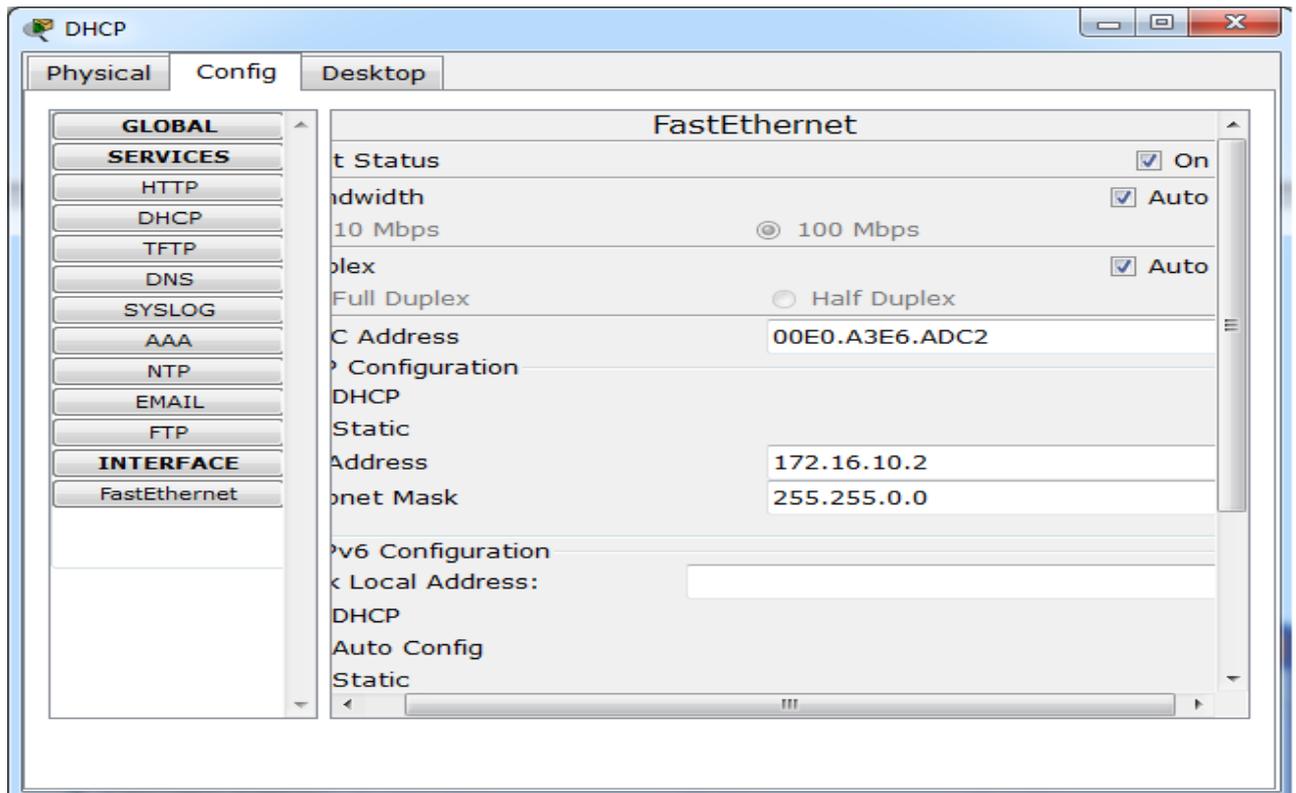


Figure 6.3:DHCP Set Fast Ethernet IP

Step 5- Click FastEthernet from the Sidebar and set:

- Set HTTP Service and HTTPS Service to **Off**

Step 6- Click DHCP from the Sidebar and set:

- Set the pool Name **Soil**
- Set the Default Gateway to **172.16.10.1**
- Set the DNS Server to **172.16.10.3**
- Set the Start IP Address to **172.16.10.0**

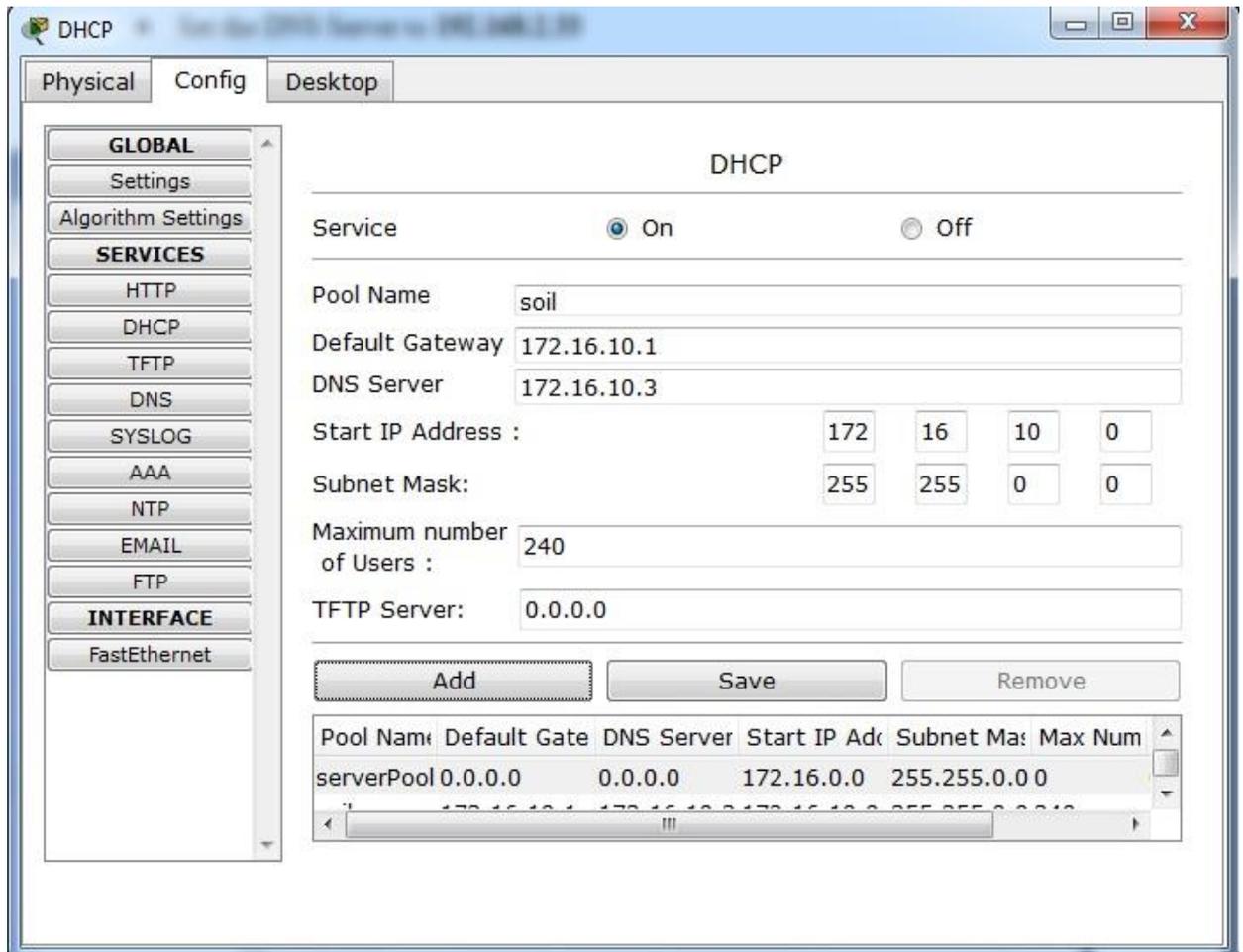


Figure 6.4: Set DHCP IP

Step 7- Click DNS from the Sidebar and set:

- Set the Service to **Off**

Step 8- Click DHCP from the Sidebar and set:

- Set the SMTP Service and POP3 Service to **Off**

DHCP Server Test:

Step 1- Select a Host from the workspace

Step 2- Click the Desktop button from the Toolbar

Step 3- Click IP Configuration

Step 4- Check mark the DHCP.

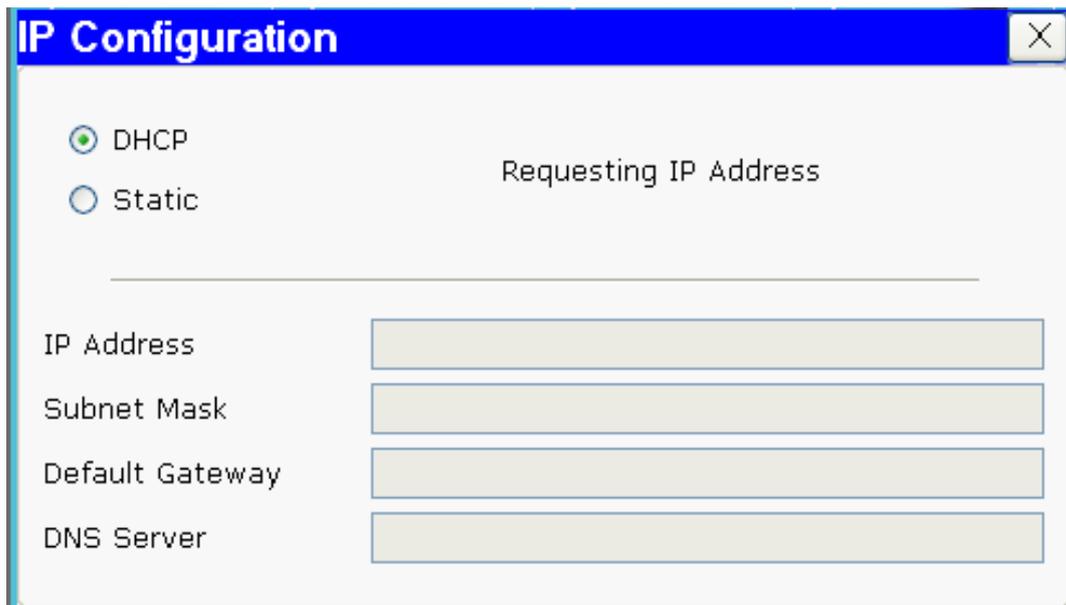


Figure 6.5: IP configure Using DHCP

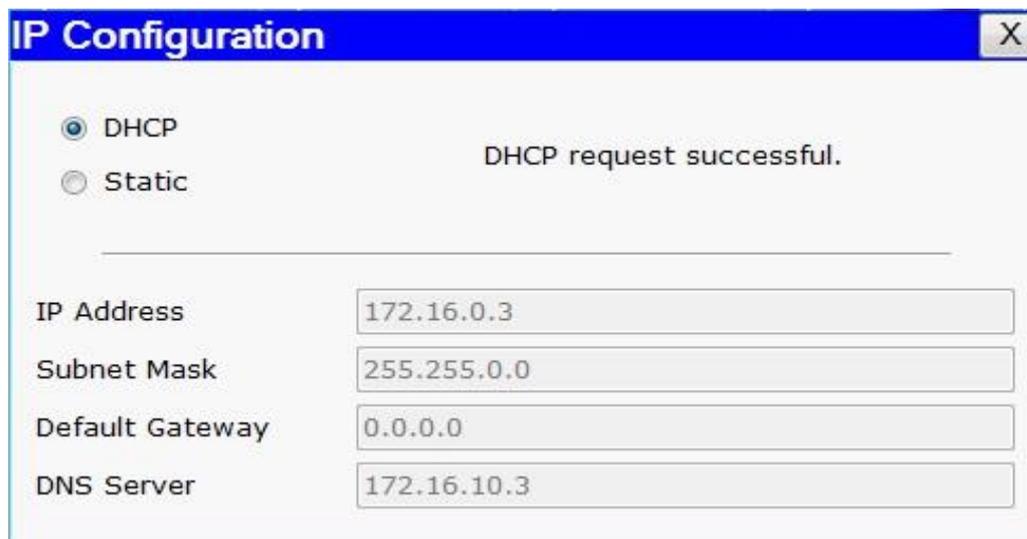


Figure 6.6: IP configure Successful

Step 5- DHCP request Successful.

6.3 DNS SERVER

Short for Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time we use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might translate to `198.105.232.4`.

How DNS work

Step 1: User's PC sends a resolution request (For example `www.google.com`) to its configured DNS Server, typically at ISP.

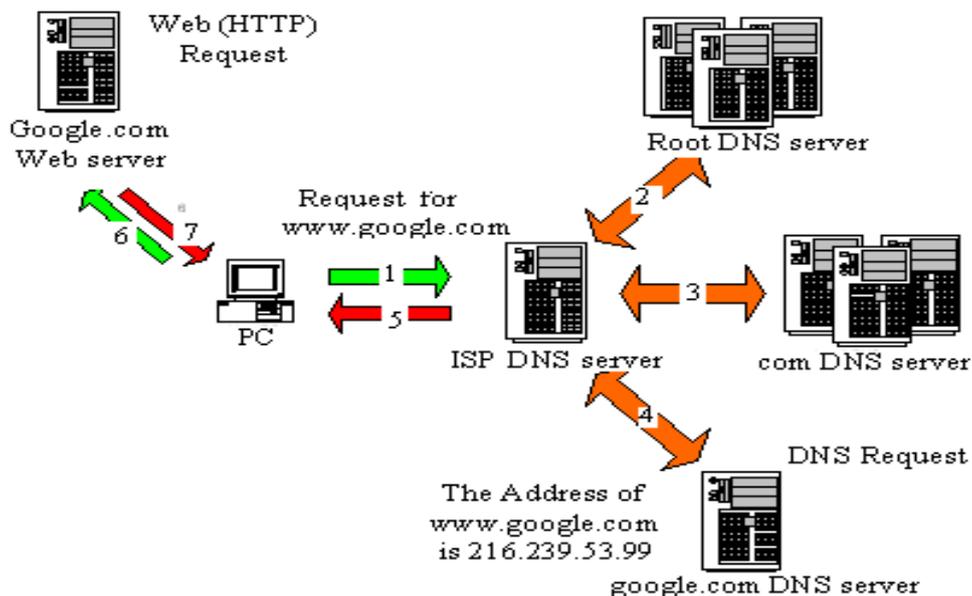


Figure.22 How DNS server work

Step 2: ISPs recursive name server starts by asking one of the root servers predefined in its "hints" file.

Step 3: ISPs recursive name server then asks one of the “com” name servers as directed.

Step 4: ISPs recursive name server then asks one of the “google.com” name servers as directed.

Step 5: ISP DNS server then send the answer back to user’s PC. The DNS server will “remember” the answer for a period of time.

Step 6: User’s PC can then make the actual HTTP request to the web server.

Configuring the DNS Server:

Step 1- Select a server to drag and drop to the workspace

Step 2- Select the server and click the config button from the Toolber

Step 3- Click Global Settings and set:

Global Settings:

- Change the Display Name to “**DNS**”
- Set the Gateway to **172.16.10.1**
-

Step 4- Click FastEthernet from the Sidebar and set:

FastEthernet:

- Set the IP address to **172.16.10.3**
- Set the Subnet Mask to **255.255.255.0**

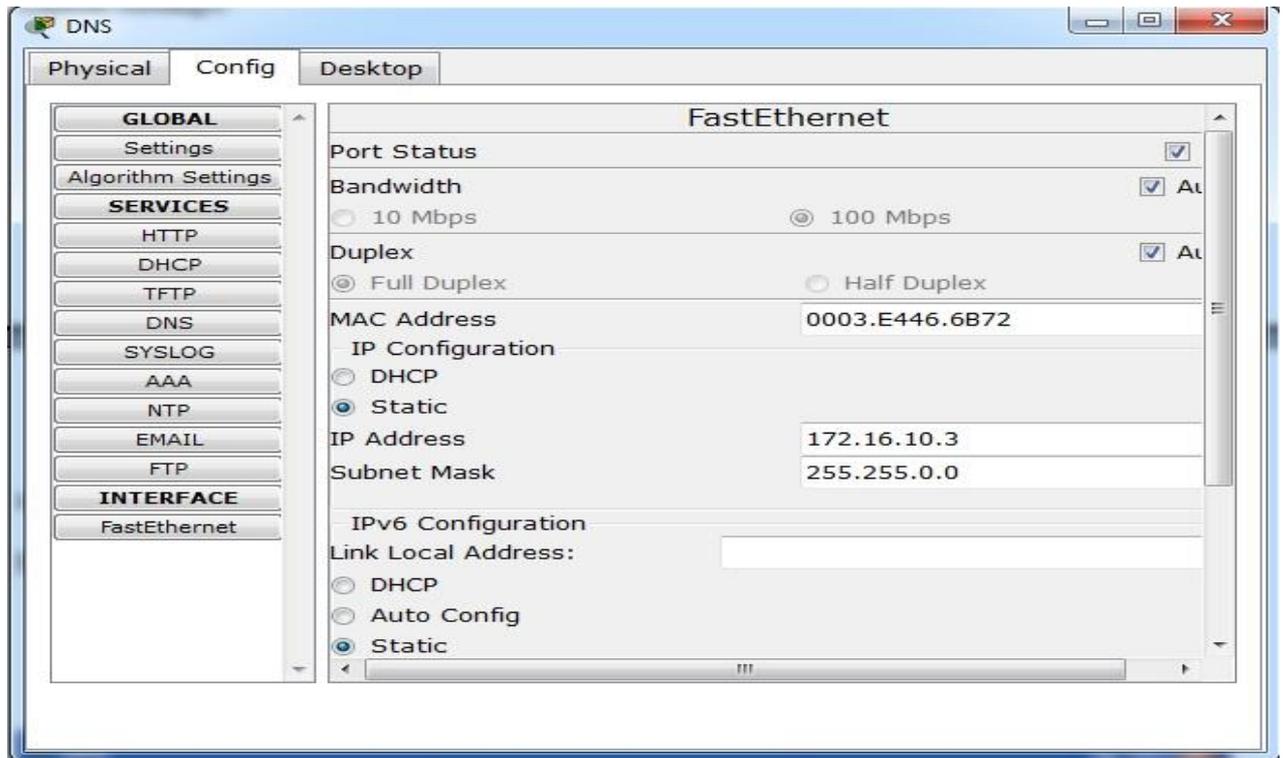


Figure 6.8: DNS FastEthernet IP Setting

Step 5- Click HTTP from the Sidebar and set:

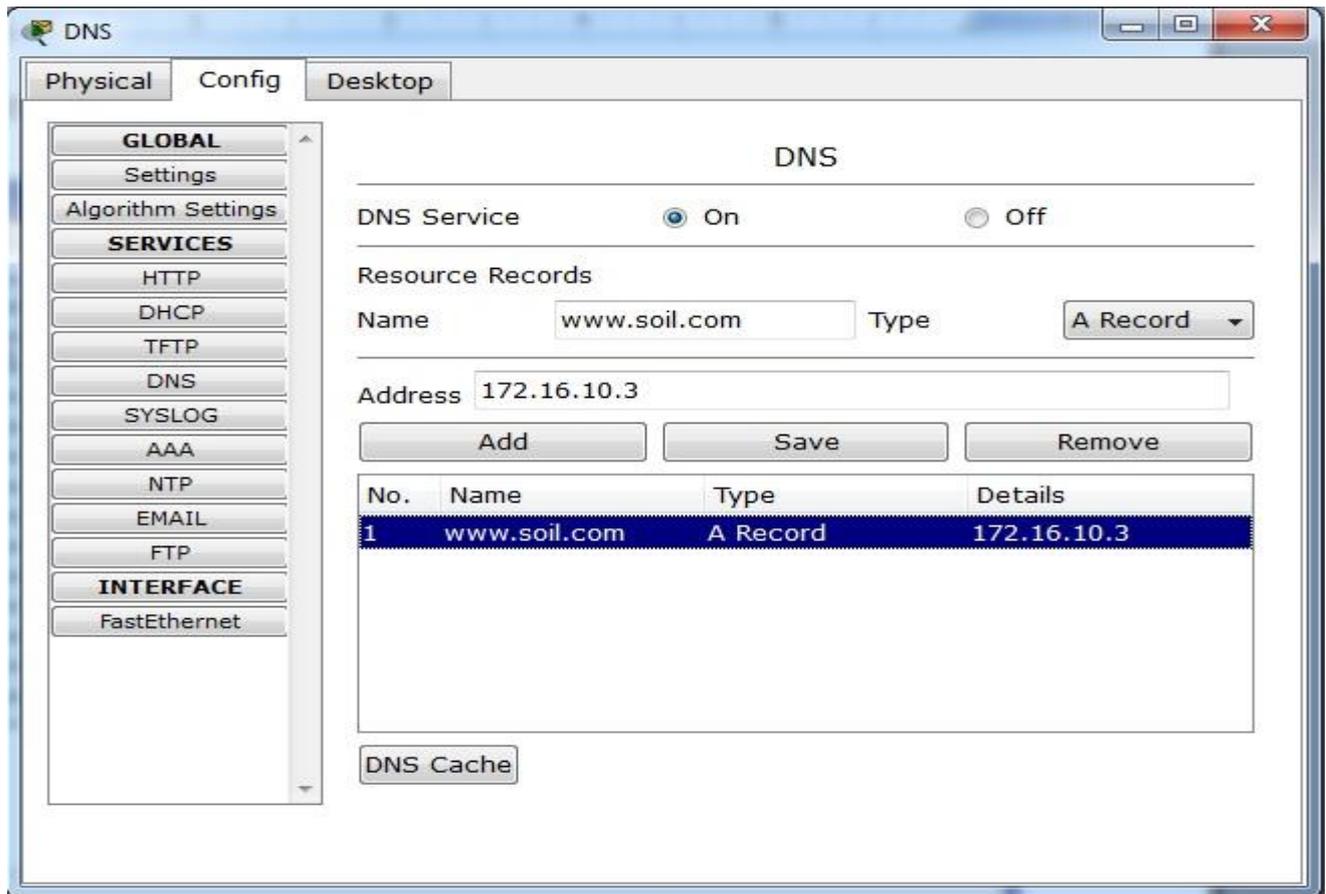


Figure 6.9: DNS Service Setup

- Set HTTP Service and HTTPS Service to **Off**

Step 6- Click DHCP from the Sidebar and set:

- Set the Service to **Off**

Step 7- Click DNS from the Sidebar and set:

- Enter for the Domain Name **Soil.com**
- Enter for IP Address **172.16.10.3**
- Click **Add**

Step 8- Click Email from the Sidebar and set:

- Set the SMTP Service and POP3 Service to **Off**

WEB SERVER

If we wish to host any website, we need a web server. A web server satisfies web browsers query by sending requested web page. ISPs actually host their own website only. A computer program that is responsible for accepting HTTP requests from clients (user agents such as web browsers), and serving them HTTP responses along with optional data contents, which usually are web pages such as HTML documents and linked objects (images, etc.).

When a web address (or URL) is typed into a web browser, the web browser establishes a connection to the web service running on the server using the HTTP protocol. URLs (or Uniform Resource Locator) and URIs (Uniform Resource Identifier) are the names most people associate with web addresses. For example, if we enter the URL `http://www.example.com/index.html` in our browser, this sends a request to the server whose domain name is `example.com`. The server then fetches the page named `index.html` and sends it to our browser. Browsers can interpret and present many data types, such as plain text or Hypertext Markup Language (HTML, the language in which web pages are constructed).

The browser then checks with a name server to convert `www.cisco.com` <`http://www.cisco.com` > into a numeric address, which it uses to connect to the server. Using the HTTP protocol requirements, the browser sends a GET request to the server and asks for the file `web-server.htm`. The server in turn sends the HTML code for this web page to the browser. Finally, the browser deciphers the HTML code and formats the page for the browser window.

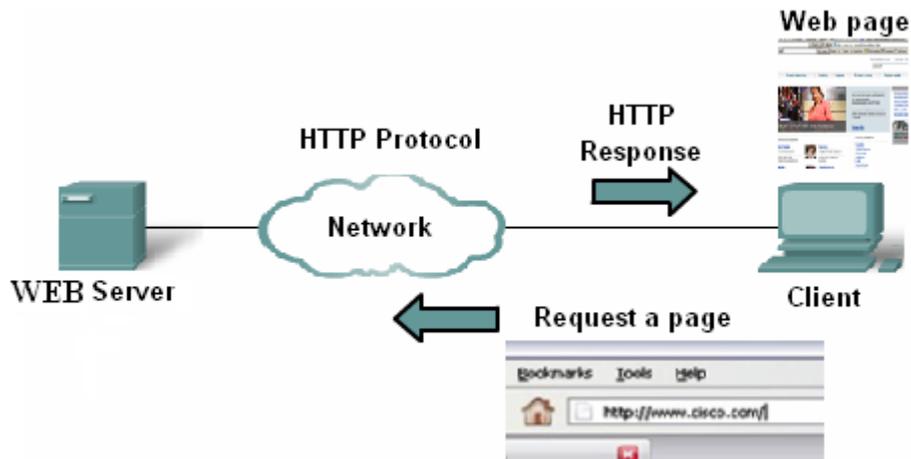


Figure. 25 How the web browser and web client interact

Configuring the www.Soil.com Web Server:

Step 1- Select a server to drag and drop to the workspace

Step 2- Select the server and click the cofig button from the Toolber

Step 3- Click Global Settings and set:

- Change the Display Name to `www.aimway.com`
- Set the Gateway to **172.16.10.1**

Step 4- Click FastEthernet and set:

- Set the IP address to **172.16.10.4**
- Set the Subnet Mask to **255.255.255.0**

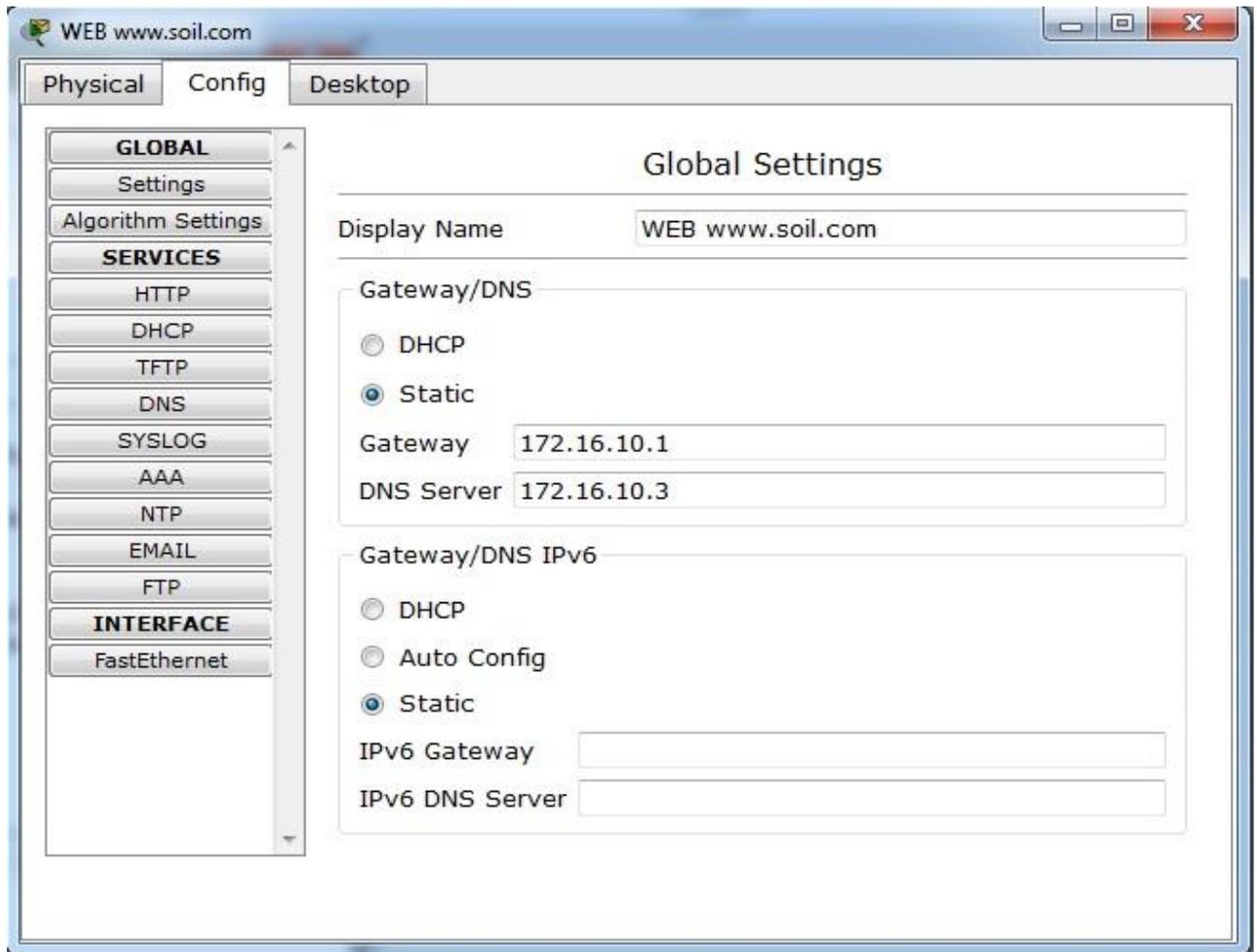


Figure 6.11: WEB Server

Step 5- Click DHCP and set:

- Set the Service to **Off**

Step 6- Click DNS and set:

- Set the Service to **Off**

Step 7- Click HTTP and set:

- Set the both the HTTP and HTTPS Service to **On**
- Change the sentence, “<hr>Sigma Oil Industries Ltd.”
- Set the SMTP Service and POP3 Service to **Off**

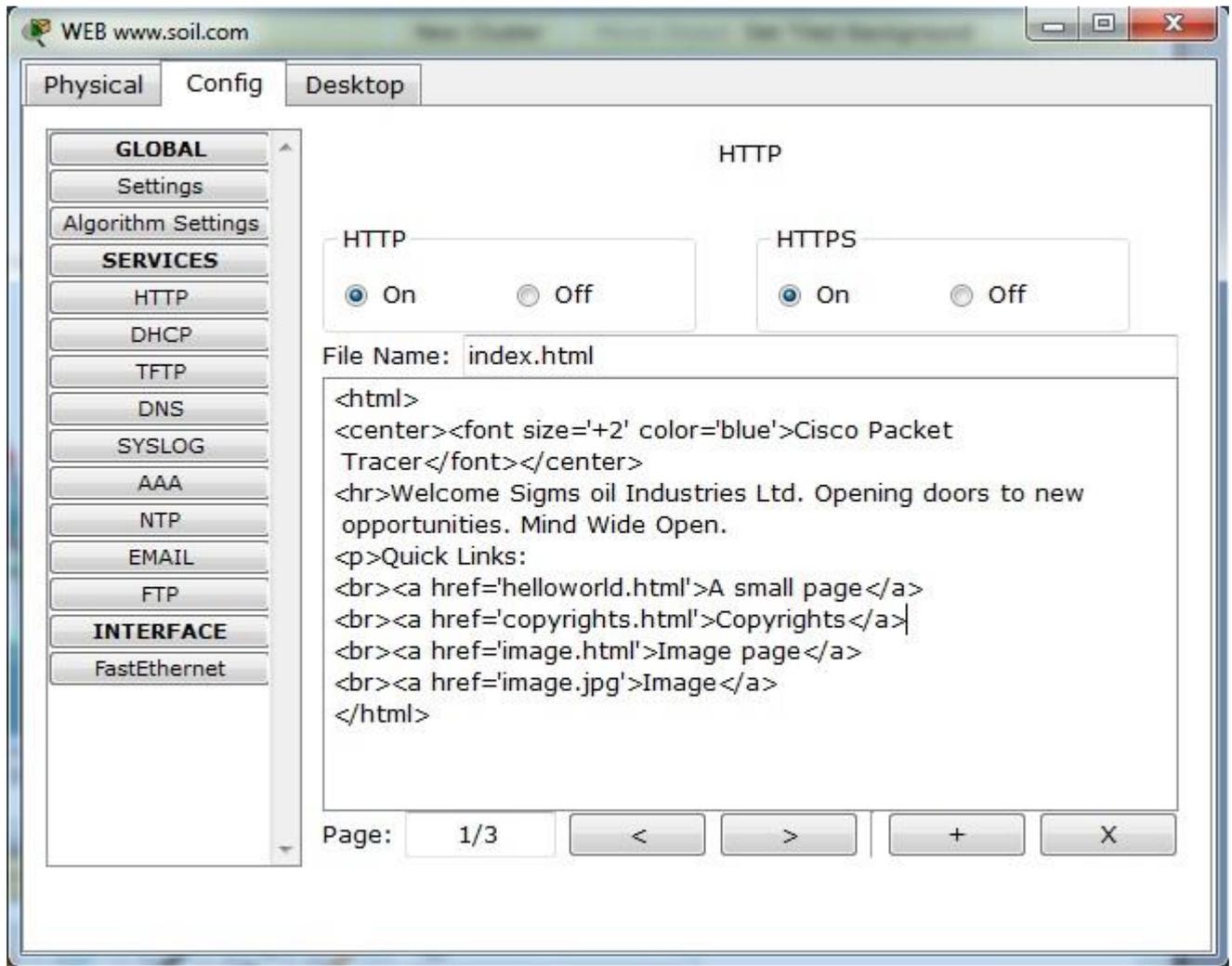


Figure 6.12: WEB Server HTTP Settings

E-MAIL SERVER

E-mail, the most popular network service, has revolutionized how people communicate through its simplicity and speed. It is one of the most public service of an ISP. As a service provider need to provide facility for sending and receiving mail from each user.

A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, qmail, Exim and sendmail are among the more common mail server programs. The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. When you send an e-mail

message, your e-mail program, such as Outlook or Eudora, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later.

How mail server work

The e-mail server operates two separate processes:

- Mail Transfer Agent (MTA)
- Mail Delivery Agent (MDA)

The Mail Transfer Agent (MTA) process is used to forward e-mail. As shown in the figure, the MTA receives messages from the MUA or from another MTA on another e-mail server. Based on the message header, it determines how a message has to be forwarded to reach its destination. If the mail is addressed to a user whose mailbox is on the local server, the mail is passed to the MDA. If the mail is for a user not on the local server, the MTA routes the e-mail to the MTA on the appropriate server.

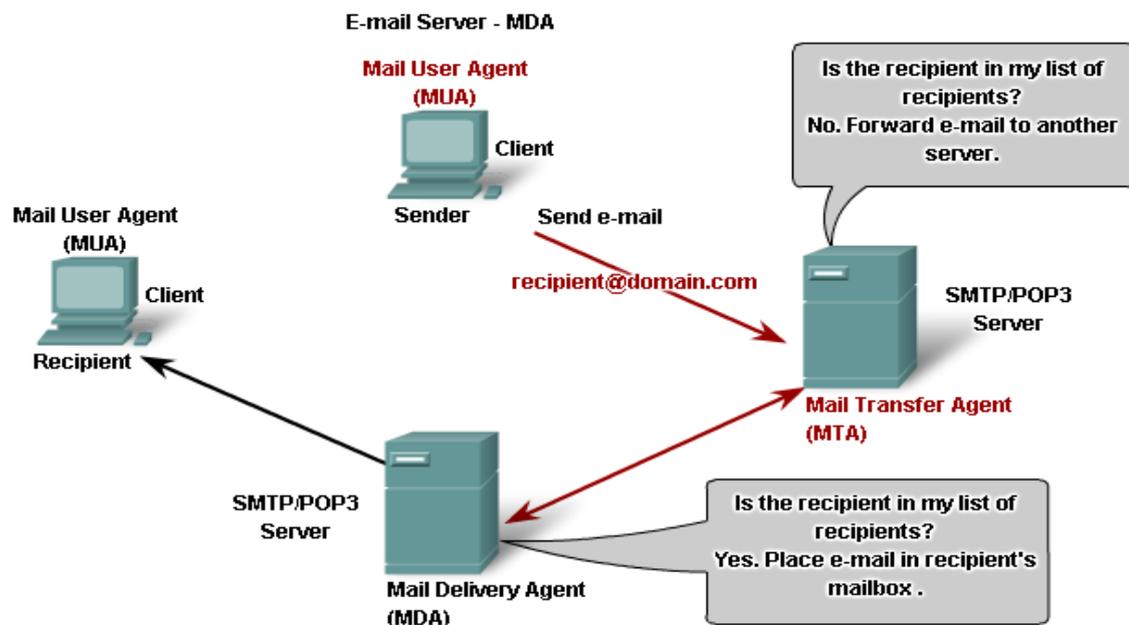


Figure. 24 How Mail server work

In the figure, we see that the Mail Delivery Agent (MDA) accepts a piece of e-mail from a Mail Transfer Agent (MTA) and performs the actual delivery. The MDA

receives all the inbound mail from the MTA and places it into the appropriate users' mailboxes. The MDA can also resolve final delivery issues, such as virus scanning, spam filtering, and return-receipt handling.

Configuring the Email Server:

Step 1- Select a server to drag and drop to the workspace

Step 2- Select the server and click the config button from the Toolber

Step 3- Click Global Settings and set:

Configuring the aimway.com Email Server

- Change the Display Name to **aimway.com**
- Set the Gateway to **172.16.10.1**

Step 4- Click the FastEthernet and set:

- Set the IP address to **172.16.10.5**
- Set the Subnet Mask to **255.255.255.0**

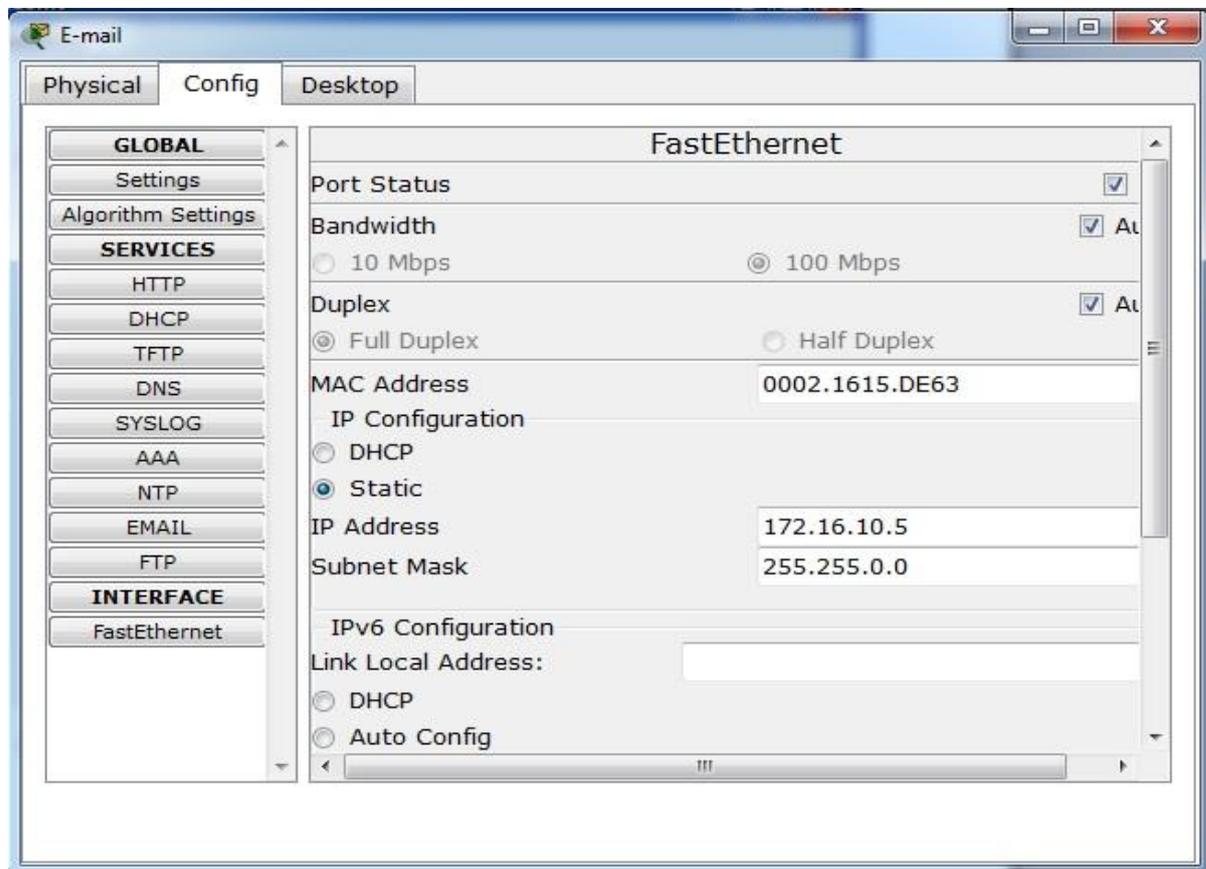


Figure 6.14: E-mail Server

Step 5- Click the DHCP and set:

- Set the Service to **Off**

Step 6- Click the DNS and set:

- Set the Service to **Off**

Step 7- Click the HTTP and set:

- Set HTTP Service and HTTPS Service to **Off**

Step 8- Click the Email and set:

- Set SMTP and POP3 Service to **On**.
- Set the domain name to aimway.com
- Setup three user accounts as follows:

Users	Password
Ratan	111111
Soil	123456
Reza	222222

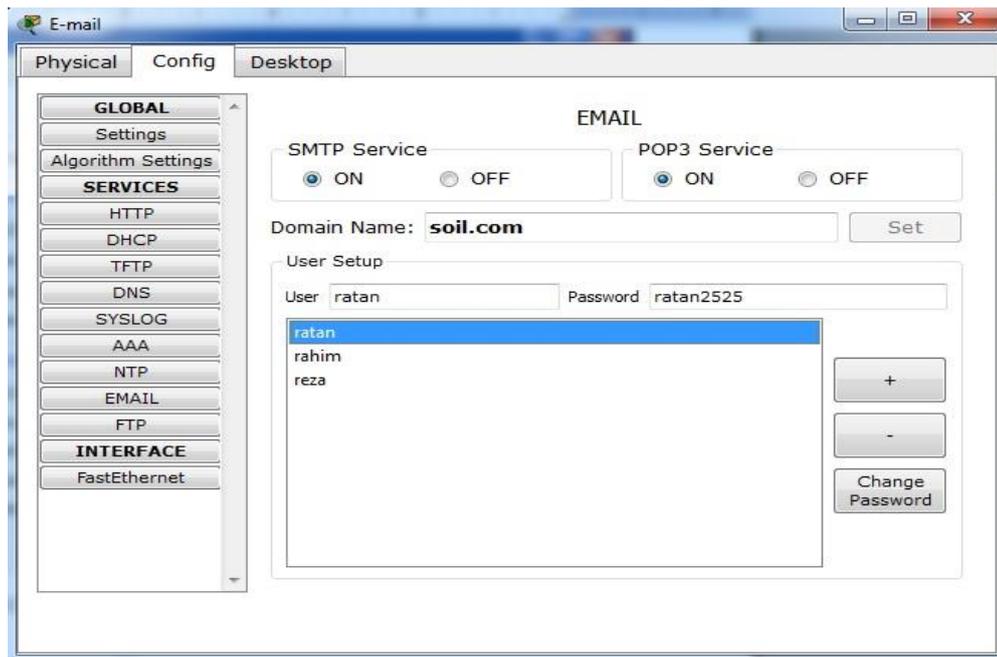


Figure 6.6 E-mail Settings in E-mail Server

FTP SERVER

File Transfer Protocol (FTP) is a standard network protocol used to exchange and manipulate files over an Internet Protocol computer network, such as the Internet. FTP is built on client-server architecture and utilizes separate control and data connections between the client and server applications. Client applications were originally interactive command-line tools with standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today. FTP is also often used as an application component to automatically transfer files for program internal functions. FTP can be used with user-based password authentication or with anonymous user access.

Nowadays it is essential for us to keep some of our important files like CV, Address book, personal profile in such place that would be available from everywhere in the world. It is possible through the internet. If we wish to transfer large number of files over internet, we need FTP. FTP is the most convenient method for transferring

private/public files. Private files can be shared by username and password authentication. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server.

To successfully transfer files, FTP requires two connections between the client and the server: one for commands and replies, the other for the actual file transfer. The client establishes the first connection to the server on TCP port 21. This connection is used for control traffic, consisting of client commands and server replies. The client establishes the second connection to the server over TCP port 20. This connection is for the actual file transfer and is created every time there is a file transferred. The file transfer can happen in either direction. The client can download (pull) a file from the server or, the client can upload (push) a file to the server.

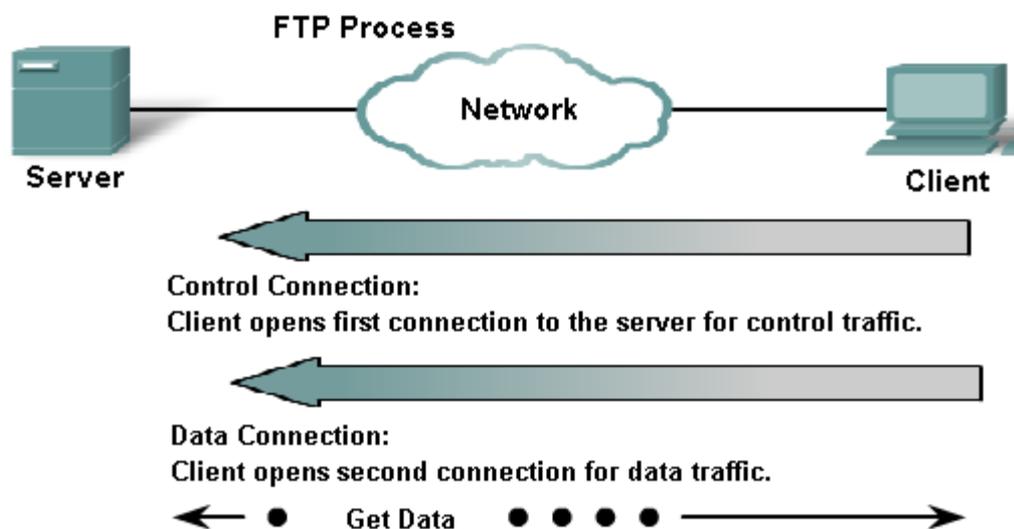


Figure. 26 How FTP server is connected with client

Configuring the FTP Server :

Step 1- Select a server to drag and drop to the workspace

Step 2- Select the server and click the cofig button from the Toolber

Step 3- Click Global Settings and set:

- Change the Display Name to **File Server**
- Set the Gateway to **172.16.10.1**

Step 4- click FastEthernet and set :

- Set the IP address to **172.16.10.6**
- Set the Subnet Mask to **255.255.255.0**

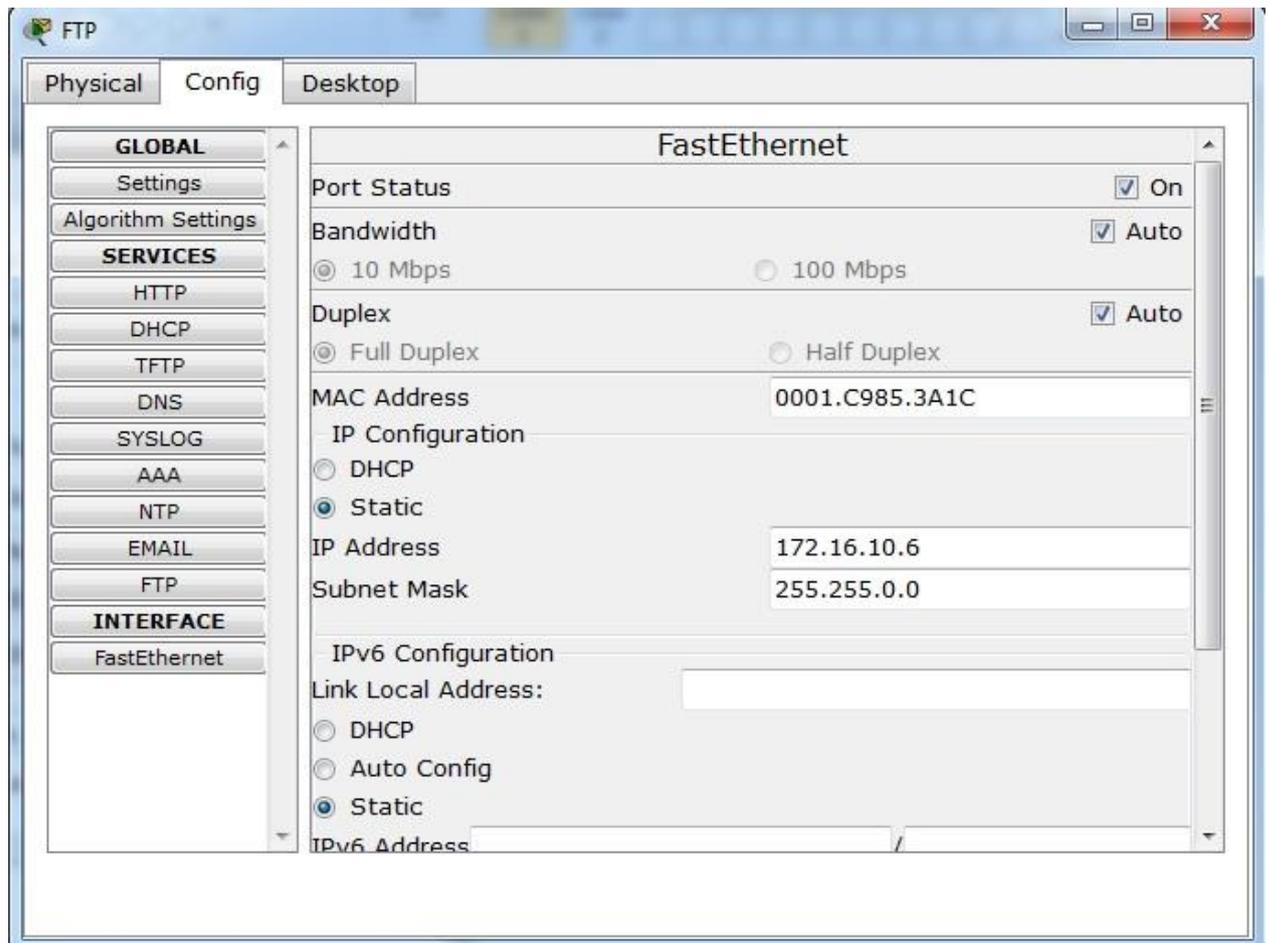


Figure 6.17: FTP Server Global Settings

Step 5- Click DHCP and set :

- Set the Service to **Off**

Step 6- Click DNS and set :

- Set the Service to **Off**

Step 7- Click HTTP and set :

- Set HTTP Service and HTTPS Service to **Off**

Step 8- Click FTP and set :

- Set Service ON
- User Name **Soil** Password **11111**
- Check mark Write, Read, Delete, Rename and List
- Click Add Button

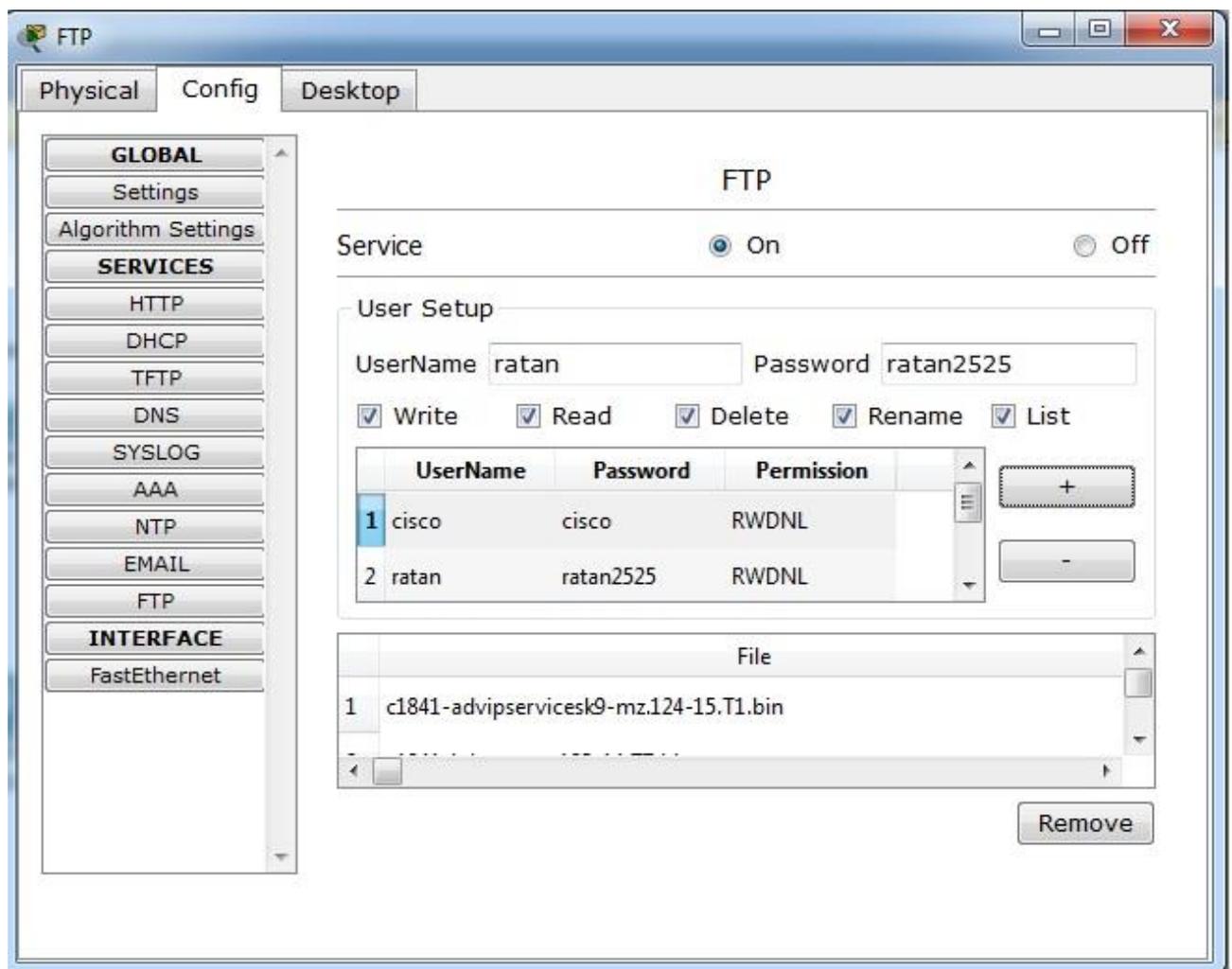


Figure 6.18 FTP Server User Setup

6.7 CONFIGURE MAIL SERVICE FOR EACH USER :

Step 1- Select a Host to drag and drop to the workspace

Step 2- Click Desktop button from toolbar

Step 3- Click E-mail Button

Step 4- Configure mail Service

Step 5- Set User Information

Step 6- Set Server Information

Step 7- Logon Information

The screenshot shows a software window titled 'PC24' with a tabbed interface. The 'Config' tab is active, displaying a 'Configure Mail' dialog box. The dialog has a blue title bar and is organized into three sections: 'User Information', 'Server Information', and 'Logon Information'. Each section contains text labels and input fields. The 'User Information' section includes 'Your Name' (filled with 'Soil') and 'Email Address' (filled with 'Soil@Soil.com'). The 'Server Information' section includes 'Incoming Mail Server' and 'Outgoing Mail Server', both filled with '172.16.10.5'. The 'Logon Information' section includes 'User Name' (filled with 'Soil') and 'Password' (filled with seven dots). At the bottom of the dialog, there are 'Save' and 'Reset' buttons. The background window shows tabs for 'Physical', 'Config', and 'Desktop'.

Figure 6.19: Configure e-mail Account

6.8 SEND AND RECIEVE E-MAIL BETWEEN TWO USER:

Step 1- Click Desktop button from toolbar

Step 2- Click E-mail Button

Step 3- Write to e-mail Address

Step 4- Write Subject

Step 5- Compose Mail

Step 6- Click Send Button

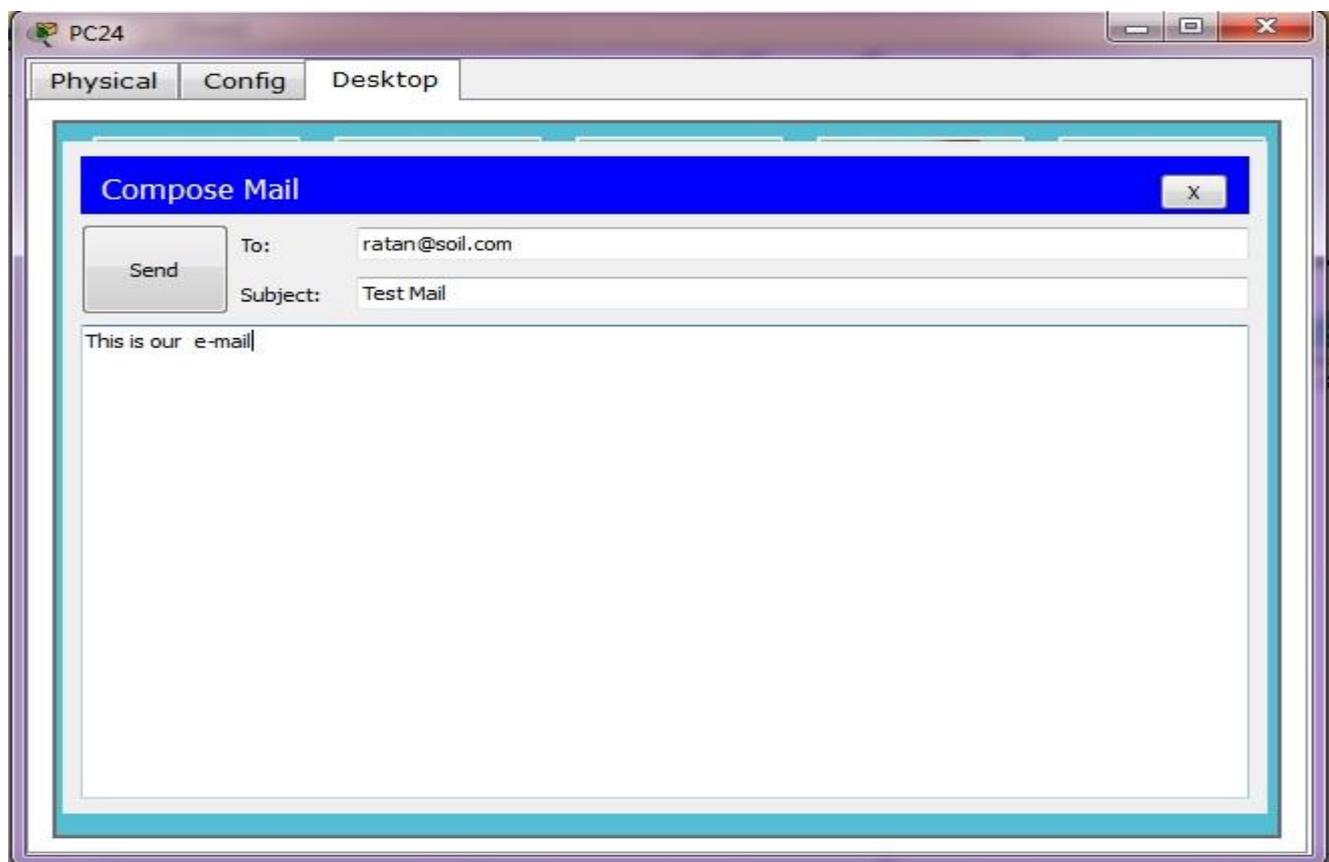


Figure 6.20: Send E-mail From one Host to Other Host

Check Mail :

Step 1- Click Desktop button from toolbar

Step 2- Click E-mail Button

Step 3- The e-mail successfully receive.

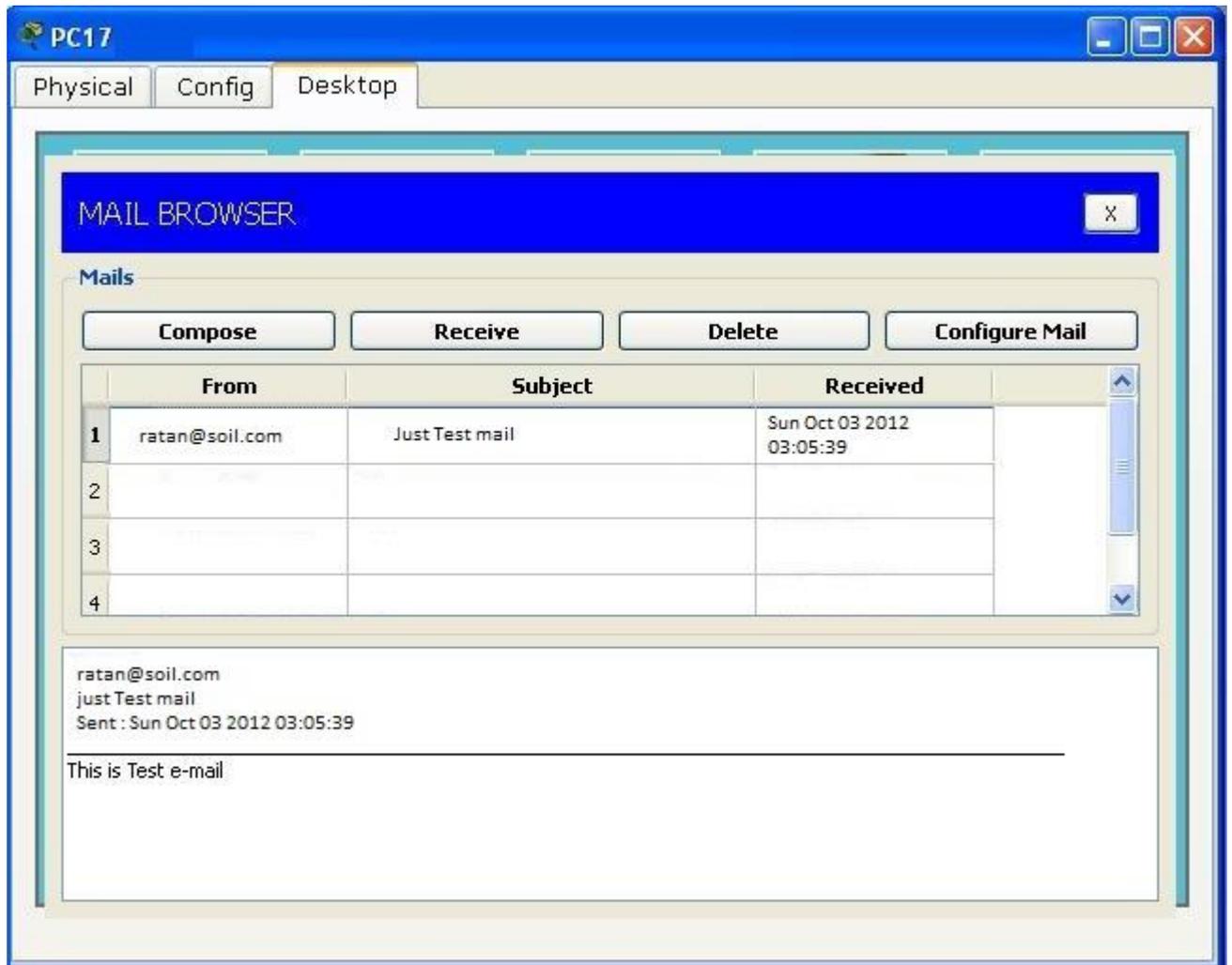


Figure 6.21: Successfully Receive Mail

CHAPTER 07: CONCLUSION

7.1 CONCLUSION

To build up a complete Office Network want to know about those essential server and Router, Switch configuration. Though some offices need more servers and other network Device as per their requirement. But if we can configure those servers and Network Device then we can make other server and Device too. I have learned a lot from those configurations and successfully completed my internship. If we can use Cisco Router Switch then we can get stability and many more facilities.

REFERENCES

1. www.swcp.com/~jgentry/topo/cisco.htm
2. http://www.tomax7.com/mcse/cisco_routerconfig.htm
3. www.youtube.com/watch?v=8q6IVWrI8hE
4. www.cisco.com/en/US/docs/wireless/.../configuration/.../c70err.html
5. www.youtube.com/watch?v=OFmJiiqJciY
6. www.tomshardware.com › [Forum](#) › [Networking](#) › [LAN/WAN](#)
7. www.packettracernetwork.com/dhcpconfiguration.html
8. www.cisco.com/en/US/docs/ios/12_0t/12_0t1/.../Easyip2.html
9. www.youtube.com/watch?v=8q6IVWrI8hE
10. www.w4shl.com/n8qb-10pacgate.html
11. www.glennavendano.com/DCLab/Experiment%203.doc
12. www.bitsbyjohn.com/.../cisco-ccna-tutorial-configure-dhcp-on-cisco-...
13. www.packettracernetwork.com/voipconfiguration.html
14. www.youtube.com/watch?v=5TBUALTxrtI
15. www.packettracertrivia.com/PacketTracer/index.html
16. en.wikipedia.org/wiki/Internet
17. www.engineersgarage.com/articles/what-is-internet-history-working
www.cyberethics.info/cyethics2/page.php?pageID=73&mpath=/