

TABLE OF CONTENTS

Chapter No.	Topics	Page No.
	Certificate from the supervisor	I-IV
	Acknowledgement	V
Chapter-1	Introduction	1
Chapter-2	Models of Networking	2
	2.1 Client –Server Model	2
	2.2 Peer to Peer Model	2
	2.3 Domain Model	2
Chapter-3	Categories of network	3
	3.1 Local Area Network (LAN)	3
	3.2 Metropolitan Area Network (MAN)	4
	3.3 Wide Area Network (WAN)	5
Chapter-4	IP Addresses and MAC Addresses	6
	4.1 IP Address Classes	6
	4.2 MAC Addressing	7
Chapter-5	Networking media	8
	5.1 Coaxial Cable	8
	5.2 Fiber Optical Cable	8
	5.3 Twisted Pair Cable	9
Chapter-6	Networking devices	12
	6.1 Routers	12
	6.1.1 Modes of Router	13
	6.1.2 Configuring Password	14
	6.1.3 Commands to assign IP addresses	16
	6.2 Switches	17
	6.2.1 Working of switch	18
	6.3 LAN Cards	18
	6.4 Hubs	19
	6.5 Modems	20
	6.6 Network Repeater	20
	6.7 Servers	21
	6.7.1 DNS Server	21

	6.7.2 DHCP SERVER	22
Chapter-7	Technologies	25
	7.1 ROUTING	25
	7.1.1 Types of Routing	26
	7.1.2 Types of routing protocols	28
	7.2 Subnetting	28
	7.2.1 Subnet Mask	29
	7.2.2 Default Mask	29
	7.2.3 Types of Subnetting	29
	7.2.4 Advantages of subnetting	30
	7.3 LAN Switching	30
	7.3.1 Layer-2 Switching	30
	7.3.4 Switching methods	31
	7.4 RIP (Routing Information Protocol)	32
	7.4.1 Features	33
	7.5 IGRP (Interior Gateway Protocol)	33
	7.6 EIGRP (Enhanced Interior Routing Protocol)	33
	7.6.1 Features	34
	7.6.2 Neighbor Discovery	34
	7.7 OSPF (Open Shortest Path First)	35
	7.7.1 Features	36
	7.7.2 Advantages	36
	7.7.3 OSPF Terminology	37
	7.7.4 OSPF areas	38
	7.7.5 Steps to apply OSPF	38
	7.8 NAT (Network Address Translation)	39
	7.8.1 Steps to enable NAT server	39
	7.8.2 Advantages of NAT	40
	7.8.3 Disadvantages of NAT	40
	7.9 PAT (Port Address Translation)	41
	7.10 TELNET	42
	7.10.1 To Access the Device Remotely	42
	7.10.2 To Telnet a device from router	43
	7.11 Trunking	43
	7.12 VLAN (Virtual LAN)	44
	7.12.1 Creating port based Vlan	45
	7.12.2 Advantages of VLAN	45
	7.12.3 Types of VLAN	46
	7.12.4 VLAN links	47

	7.12.5 VLAN Operation	47
	7.12.6 Commands	47
	7.13 Access Control Lists (ACLs)	48
	7.13.1 Working of ACLs	48
	7.13.2 Use of ACLs	49
	7.13.3 Types of Access Control Lists	50
Chapter-8	Coding	51
	8.1 Configuration of Router	51
	8.2 Configuration of Switch	58
Chapter-9	Result	61
Chapter-10	References	66
	List of figures	67

ACKNOWLEDGEMENT

I would like to express my sincere thanks to _____ for providing me the opportunity to work on this extremely interesting and important topic. His guidance and support have been a constant source of encouragement throughout the work of this project. It has been a great honour to have worked under her supervision. His valuable suggestions and feedback at every critical phase throughout the work were of utmost importance for timely completion of the project. His tremendous knowledge about the subject has gone a long way in ensuring the successful completion of this project.

A special thanks to all the staff of the Department of Computer science without whose help this work would not have been possible.

Finally, I would like to thank my family and friends for their continued support which has helped me stay strong and focused on the project work.

Signature of the Student

Name of Student ASHU SHARMA

 NEHA BHADANA

 SANDEEP SAINI

 SUNUBIA KHAN

Date



CHAPTER -1

INTRODUCTION

Networking is a practice of linking of two or more computing devices such as PCs, printers, faxes etc., with each other. Connection between two devices is through physical media or logical media to share information, data and resources. Networks are made with the hardware and software.

In this project, we are going to set up a network for a bank. We will connect the three branches of bank with each other that will be situated in three different states so, the information between the branches can exchange & update.

It is networking based project and in this project we are trying to use some technologies of networking that will help us to do our work more easily. As we mentioned that it is a networking based project so, we will use some technologies of networking such as D.H.C.P, V-LAN, TRUNKING, P.A.T, O.S.P.F etc.

This network will be more secure because, there will be many restriction for accessing data from bank website. These restrictions will be allocated only for security of the data so, only the authorize person can access the information of the bank.

In this project we will also create a website for the bank, a mail server for the e-mail purpose. These website and mail services of the bank will help the customer to connect easily with the bank .



CHAPTER -2

MODELS OF NETWORKING

Model means the connectivity of two computers. We have many types of networking models.

- Client – Server Model
- Peer to Peer Model (Workgroup Model)
- Domain Model

2.1 Client –Server Model

In a Client server model we have one server and many clients. A Client can share the resources of server, but a server cannot share the resources on clients. On the point of view of administrator it's very easy to control the network because we combine with the server also at security point of view. It is very useful because it uses user level security in which users have to remember only one password to share the resources.

2.2 Peer to Peer Model (Workgroup Model)

In Peer to Peer networking model all computers are in equal status, that is we can not manage centralization, administration security. In Peer to Peer networking client use operating system like Window 98, Window XP, Window 2000, Window Vista.

2.3 Domain Model

It is a mixture of client server and peer-to-peer model. In this clients can share their resources as peer-to-peer but with the permission of the server as in client server model therefore it is commonly used model because in this security is more as we can put restriction on both server and clients.

CHAPTER -3

CATEGORIES OF NETWORK

Networks can be categorized as per geographical area to be covered by the network. Computer network are divided into four categories includes: Local Area Network (LAN), Campus Area Network (CAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN).

3.1 Local Area Network (LAN)

LAN is a computer network that is used to connect computers and work station to share data and resources such as printers or faxes. LAN is restricted to a small area such as home, office or college. Devices used in LAN are : HUB and switch. Media for LAN is UTP cables. Figure 1.2 shows how all work stations, server and printer are interconnected with the help of the network device.

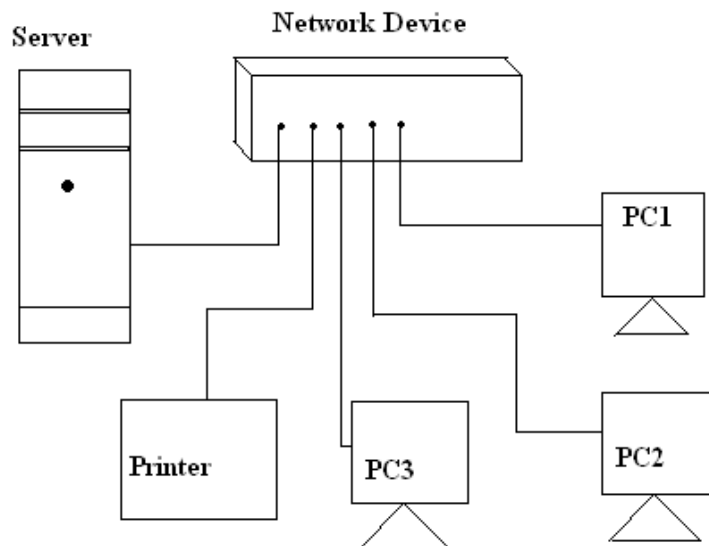


Fig. 3.1 : Local Area Network

Advantages of LAN

- Provides communication in smaller networks, easy to install and configure.
- many users can share data or network elements at the same time which results in fast work.

Disadvantages of LAN

- limited number of computers are connected in a LAN.
- LAN cannot cover large area.
- Network performance degrades as the number of users exceeds

3.2 Metropolitan Area Network (MAN)

MAN is the interconnection of networks in a city. MAN is not owned by a single organization. It act as a high speed network to allow sharing resources within a city. MAN can also be formed by connecting remote LANs through telephone lines or radio links. MAN supports data and voice transmission. The best example of MAN is cable T.V network in a city.

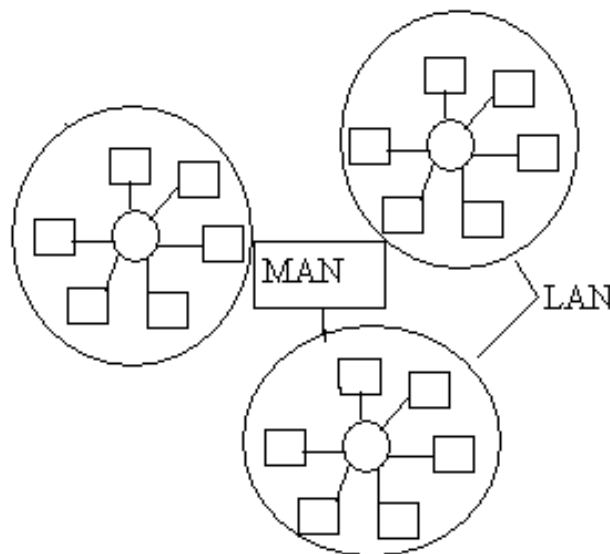


Fig. 3.2 : Metropolitan Area Network

3.3 Wide Area Network (WAN)

WAN covers a wide geographical area which include multiple computers or LANs. It connects computer networks through public networks like, telephone system, microwave, satellite link or leased line.

Most of the WANs use leased lines for internet access as they provide faster data transfer. WAN helps an organization to establish network between all its departments and offices located in the same or different cities. It also enables communication between the organization and rest world.

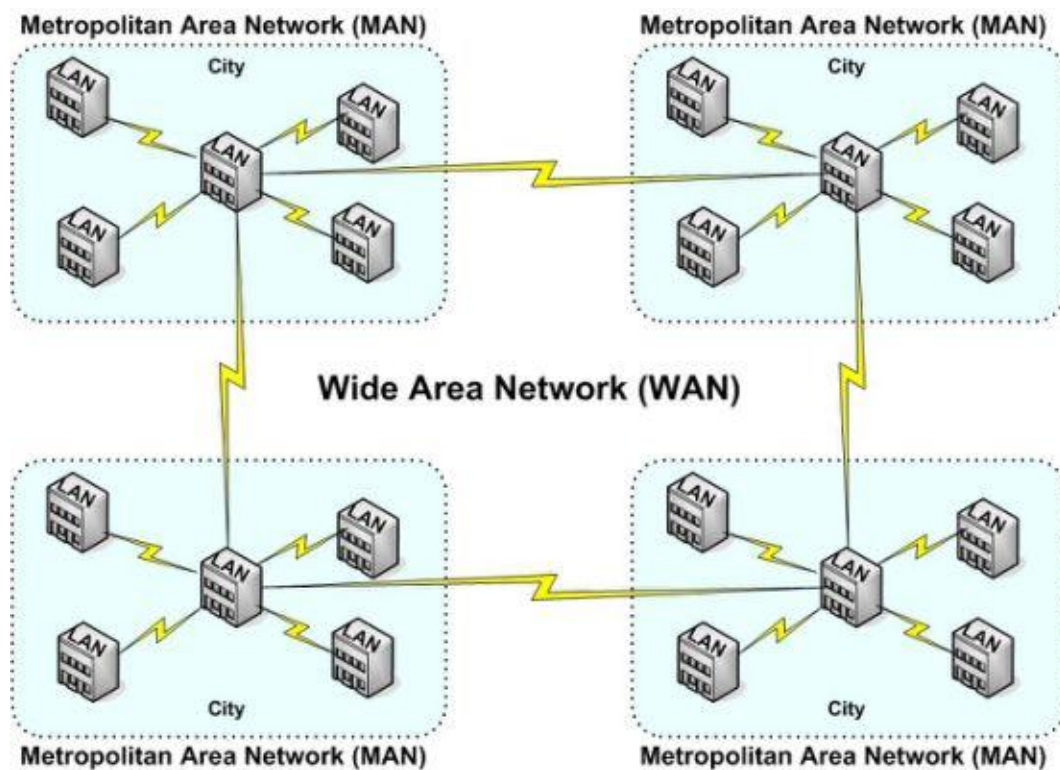


Fig. 3.3 : Wide Area Network

CHAPTER -4

IP ADDRESSES AND MAC ADDRESS

It is also called as logical addresses. IP is a 32 bit long and it is divided into 4 octets and dot (.) is used to separate one octet from another. It is represented in the form of decimals.

There are two versions of IP addresses:

- IPv4
- IPv6

4.1 IP Address Classes

IP address is a 32 bit address. It is divided into various classes namely Class A, Class B, Class C, Class D and Class E. TCP/IP defines Class D for experimental purpose. TCP /IP address contains two addresses embedded within one IP address; Network address and host address as shown in figure.

NETWORK ADDRESS	HOST ADDRESS
0 bits	31 bits

Class A consists of 8-bit network ID and 24-bit host ID. Class B consists of 16- bit network ID and 16-bit of host ID. And Class C consists of 24-bit of network ID and 8-bit of host ID.

How to Assign IP Address to Computer

An IP address assigned to a computer may either be permanent address or address that is assigned to a computer on a time lease or for temporary basis. Hence, the address granted to computers is divided into two categories Dynamic IP addresses and Static addresses.



Dynamic IP Addresses

Dynamic IP addresses are assigned to the devices that require temporary connectivity to the network or non-permanent devices such as portable computer. The most common protocol used for assigning Dynamic IP address is DHCP also called Dynamic Host Configuration Protocol. The DHCP grants IP address to the computer on lease basis.

Static IP Addresses

Static IP addresses are assigned to the device on the network whose existence in the network remains for a longer duration. These static IP addresses are semi-permanent IP addresses which remain allocated to a specific device for longer time e.g. Server.

4.2 MAC Addressing

MAC address is a hardware address that is embedded in the NIC card. It is also known as hardware address or physical address. Every NIC card has a unique MAC address assigned by IEEE. MAC address is used to identify the nodes at lower levels of OSI model. The MAC address operates at the data link layer of the OSI model.

MAC address is a 12 digit hexadecimal number (48 bit address). It is made up of numbers from 0-9 or a letter from A-F. MAC address can be written in any one of the formats:

- ▶ MM:MM:MM:SS:SS:SS
- ▶ MM:MM:MM:SS:SS:SS

To identify the MAC address in window:

- Click **Start** → **Run**
- Enter **cmd** in the **Open** text box
- Type **ipconfig /all**
- Press **Enter**

The 12 digit MAC address will be shown as say **00:11:11:EA:8D:F6**

CHAPTER -5

NETWORKING MEDIA

To do networking we need to use some type of media. There are many types of media.

- Coaxial Cable
- Fiber optic cable
- Twisted Pair of Cables
- Micro- wave
- Satellite

5.1 Coaxial Cable

Coaxial cable consists of an insulated copper conductor surrounded by a tube shaped copper braid outer copper tube and the inner conductor have the same axis of curvature hence it called coaxial cable. It is basically of two types:

(i) Base Band Cable (RG – 59)

(ii) Broad Band Cable (RG – 58)

We used Base Band signal cable in Networking of Computers, It is so called because it carries single frequency. Its speed is 10 Mbps and impedance is 50 Ω . Where as Broad Band Cables carries multiple frequencies. Connector used for Coaxial cable is BNC(British Novel Connector) connector. ARCnet uses RG-62 coaxial cable. It has an impedance of 93 Ω and has a comparatively lesser attenuation, hence yield greater distances. These cables are expensive and provide high propagation factor.

5.2 Fiber Optical Cable

Fiber optic cable consists of a very fine fiber made from two types of glass, one for the inner core and the other for the outer layer. Here signal is transmitted in the form of light. Different varieties of fiber optics is used depending on the size of the

network. Single mode fiber optics is used for networks spanning longer distance. Fiber Optics has lower propagation factor than coaxial cable. It is a costly but more secure transmission media.

5.3 Twisted Pair Cable

There are two wires, which are twisted with each other to avoid EMI (Electro Magnetic Induction).these cables are easy to terminate. However they have a slightly higher value of attenuation value and hence have limited distance covering capacity. Connector used for Twisted Pair of Cable is (Registered Jack) RJ-45 and RJ-11.

There are two types of twisted pair of cables:

5.3.1 STP (Shielded Twisted Pair)

In this an extra wire which is called shielded wire is wrapped over the inner cover which holds copper in pairs. This protection is used to protect signal from external noise.

5.3.2 UTP (Unshielded Twisted Pair)

In this type of wire no shielded cover is there for extra protection from noise. There are different categories of UTP cables:

Table 5.1 : Category and Speed of UTP cables

Category	Speed
CAT-1	56 Mbps
CAT-2	4 Mbps
CAT-3	10 Mbps
CAT-4	16-20 Mbps
CAT-5	100 Mbps
CAT-6	1Gbps
CAT-7	1Gbps

Ethernet Cabling

There are two types of Ethernet cables:

- Straight cable
- Crossover cable

Straight cable

It is used when we have to connect

PC TO Switch

PC to Hub

Hub to Router

Switch to Router

Table 5.2 : Colour Coding for straight Cable

568A		568B	
(one end)	(other end)	(one end)	(other end)
Green/white	Green/white	Orange/white	Orange/white
Green	Green	Orange	Orange
Orange/white	Orange/white	Green/white	Green/white
Blue	Blue	Blue	Blue
Blue/white	Blue/white	Blue/white	Blue/white
Orange	Orange	Green	Green
Brown/white	Brown/white	Brown/white	Brown/white
Brown	Brown	Brown	Brown

Crossover Cable

It is used when we have to connect:

- PC to PC
- Hub to Hub
- Switch to switch
- Router to Router
- PC to Router
- Hub to Switch

Table 5.3 : Colour Coding for Crossover cable

One end	Other end
Orange/white	Green/white
Orange	Green
Green/white	Orange/white
Blue	Blue
Blue/white	Blue/white
Green	Green
Brown/white	Brown/white
Brown	Brown

CHAPTER -6

NETWORKING DEVICES

Computer networking devices are units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU).

6.1 Routers

A router is a communication device that is used to connect two logically and physically different networks, two LANs, two WANs and a LAN with WAN. The main function of the router is to sorting and the distribution of the data packets to their destinations based on their IP addresses. Routers provides the connectivity between the enterprise businesses, ISPs and in the internet infrastructure, router is a main device. Cisco routers are widely used in the world. Every router has routing software, which is known as IOS. Router operates at the network layer of the OSI model. Router does not broadcast the data packets.



Fig. 6.1 : Real Router



Fig. 6.2 : Router in packet tracer

A router is a device that forwards data packets across computer networks. Routers perform the “data traffic directing” functions on the Internet. A router is connected to two or more data lines from different networks. When data comes in on one

of the lines, the router reads the address information in the packet to determine its ultimate destination.

6.1.1 Modes of Router

When we access router command prompt the router will display different modes. According to the modes, privileges and rights are assigned to the user.

I. User mode

Router>

In this mode, we can display basic parameter and status of the router we can test connectivity and perform telnet to other devices. In this mode we are not able to change and save router configuration.

II. Privileged mode

Router#

In this mode, we can display all information, configuration, perform administration task, debugging, testing and connectivity with other devices. We are not able to perform here configuration editing of the router.

The command to enter in this mode is 'enable'. We have to enter enable password or enable secret password to enter in this mode. Enable secret has more priority than enable password. If both passwords are configured then only enable secret will work.

III. Global configuration mode

Route(config)#

This mode is used for the configuration of global parameters in the router. Global parameters applied to the entire router. All the changes are performed in this mode. But here we cannot see and save the changes. For e.g: - router hostname or access list of router, password, Banner, Routing, Security. The command to enter in this mode is 'configure terminal'

IV. Line configuration mode

In this mode we can set the password of the user mode, i.e to set user mode password. This mode is used to configure lines like console, vty and auxiliary. There are main types of line that are configured.

(i) Console

Router(config)#line console 0

(ii) Auxiliary

Router(config)#line aux 0

(iii) Telnet or vty

Router(config)#line vty 0 4

V. Interface configuration mode

In this mode we can set ip addresses of the interfaces. This mode is used to configure router interfaces. For e.g:- Ethernet, Serial, BRI etc.

Router(config)#interface <type> <number>

Router(config)#interface serial 1

VI. Routing configuration mode

This mode is used to configure routing protocol like RIP, EIGRP, OSPF etc.

Router(config)#router <protocol> [<option>]

Router(config)#router rip

Router(config)#router eigrp 10

6.1.2 Configuring Password

There are five types of password available in a router.

Console Password

router#configure terminal

router(config)#line console 0

router(config-line)#password <word>

router(config-line)#login

```
router(config-line)#exit
```

To erase password do all steps with no command.

Vty Password

```
router>enable
```

```
router#configure terminal
```

```
router(config)#line vty 0 4
```

```
router(config-line)#password <word>
```

```
router(config-line)#login
```

```
router(config-line)#exit
```

Auxiliary Password

```
router#configure terminal
```

```
router(config)#line Aux 0
```

```
router(config-line)#password <word>
```

```
router(config-line)#login
```

```
router(config-line)#exit
```

Enable Password

```
router>enable
```

```
router#configure terminal
```

```
router(config)#enable password <word>
```

```
router(config)#exit
```

Enable Secret Password

Enable Password is the clear text password. It is stored as clear text in configuration where as enable secret password is the encrypted password.

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#enable secret <word>
```

```
Router(config)#exit
```

Encryption all passwords

All passwords other than enable secret password are clear text password. The command to encrypt all password are

```
Router#configure terminal
```

```
Router(config)#service password-encryption
```

6.1.3 Commands to assign IP addresses to the interfaces

At Router1:

```
Router>
```

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#interface fa0/0
```

```
Router(config-if)#ip address 10.0.0.1 255.0.0.0
```

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

```
Router(config-if)#exit
```

```
Router#configure terminal
```

```
Router(config)#interface fa0/1
```

```
Router(config-if)#ip address 20.0.0.1 255.0.0.0
```

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

```
Router(config-if)#exit
```

Now to check the assigned IP addresses to the interfaces the command used is:

```
Router#show ip interface brief
```

6.2 Switches

Like the router, a switch is an intelligent device that maps the IP address with the MAC address of the LAN card. Unlike the hubs, a switch does not broadcast the data to all the computers, it sends the data packets only to the destined computer. Switches are used in the LAN, MAN and WAN. In an Ethernet network, computers are directly connected with the switch via twisted pair cables. In a network, switches use the three methods to transmit the data i.e. store and forward, cut through and fragment free.

A switch is a networking device which filters and forward packets through the network. It is a layer 2 device. It is more advanced than hub but not as advanced as router. The basic function of a switch is to manage the signal flow. A switch is a hardware device that filters and forward data packets between network segments. . Ethernet switches are used in LAN to create Ethernet networks.



Fig. 6.3 Real Switch



Fig. 6.4 Switch in packet tracer

We have two types of switch.

- **Mangeable switch:** It has console port.
- **Non-mangeable :**It has no console port.

Switches are generally used to segment a large LAN smaller segments. Smaller switches such as the Cisco Catalyst 2924XL have 24 ports capable of creating 24 different network segment for the LAN. Larger switches such as the Cisco Catalyst 6500 can have hundreds of ports. Switches can also be used to connect LANs with different media, for example, a 10 Mbps Ethernet LAN and 100 Mbps Ethernet LAN can be connected using a switch.

When the switch is open, it allows the signal to flow through it and when it is closed, it stops the signal to flow. Switch connects separate LAN segment. It allows multiple system to transmit simultaneously. Switches forward the traffic on the basis of MAC address. Switches maintain a switching table in which MAC addresses and port numbers are used to perform switching decision.

6.2.1 Working of switch

When switches receives data from one of connected devices, it forward data only to the port on witch the destined system is connected. It use the media access Control (MAC) address of the device to determine the correct port. The MAC address is a unique number that is programmed in to every Network Interface Card(NIC). Consider, device A wants to send data to device B. When device A passes the data, switch receives it. Switch than cecks the MAC address of the destination system. It then transfer data to device B only instead of brodcasting to all the devices.

6.3 LAN Cards

LAN cards or network adapters are the building blocks of a computer network. No computer can communicate without a properly installed and configured LAN card. Every LAN card is provided with a unique IP address, subnet mask, gateway and DNS (if applicable). An UTP/STP cable connects a computer with the hub or switch. Both ends of the cable have the RJ-45 connectors one is inserted into the LAN card and one in the hub/switch. LAN cards are inserted into the expansion slots inside the computer. Different LAN cards support different speed from 10/100 to 10/1000.

Ethernet = speed 10mbps

Fast Ethernet = 100mbps

Giga Ethernet = 1000mbps

Fastgiga Ethernet = 10000mbps



Fig. 6.5 : Lan Cards

6.4 Hubs

The central connecting device in a computer network is known as a hub. There are two types of a hub i.e. active hub and passive hub. Every computer is directly connected with the hub. When data packets arrive at the hub, it broadcasts them to all the LAN cards in a network and the destined recipient picks them and all other computers discard the data packets. Hub has five, eight, sixteen and more ports and one port is known as uplink port, which is used to connect with the next hub.



Fig.6.6 : Real Hub



Fig. 6.7 : Hub in packet tracer

6.5 Modems

A modem is a communication device that is used to provide the connectivity with the internet. Modem works in two ways i.e. Modulation and Demodulation. It converts the digital data into the analogue and analogue to digital.



Fig. 6.8 : Modem

6.6 Network Repeater

A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.



Fig. 6.9 : Network Repeater

6.7 Servers

A server is primarily a program that runs on a machine, providing a particular and specific service to other machines connected to the machine on which it is found. Nowadays, server functionality has become so rich, complex and varied in nature that there are whole very powerful computers dedicated to being exclusively servers. This has led many non-technical people to denote servers as being machines that run services.

A **network server** is a computer designed to process requests and deliver data to other (client) computers over a local network or the Internet. Network servers typically are configured with additional processing, memory and storage capacity to handle the load of servicing clients.

6.7.1 DNS Server

DNS stands for domain name system. DNS system is a standard technology for managing the names of websites and other internet domains. DNS techniques allows you to type names into your web browser like computer networking, about computer and allow your computer to automatically find that address on internet. DNS is the resolution mechanism used by Window Server 2003 clients to find other computers and services running on those computers for computers in a window 2003 network infrastructure to talk to one another, one of the key ingredients is the DNS server .Host name alone do not communicate globally but communicate locally, but if domain name is added along with it then the host name can communicate globally.



DNS is use for name reservation i.e. to convert IP address to host name and host name to IP address or the function of DNS is to resolve host name such as www.yahoo.com to an IP address. User identify only user friendly name and all computers and technologies identify IP address and MAC address DNS is use to solve this

problem because DNS is used to convert host name FQDN (fully qualified domain name) to IP address and IP address to host name .

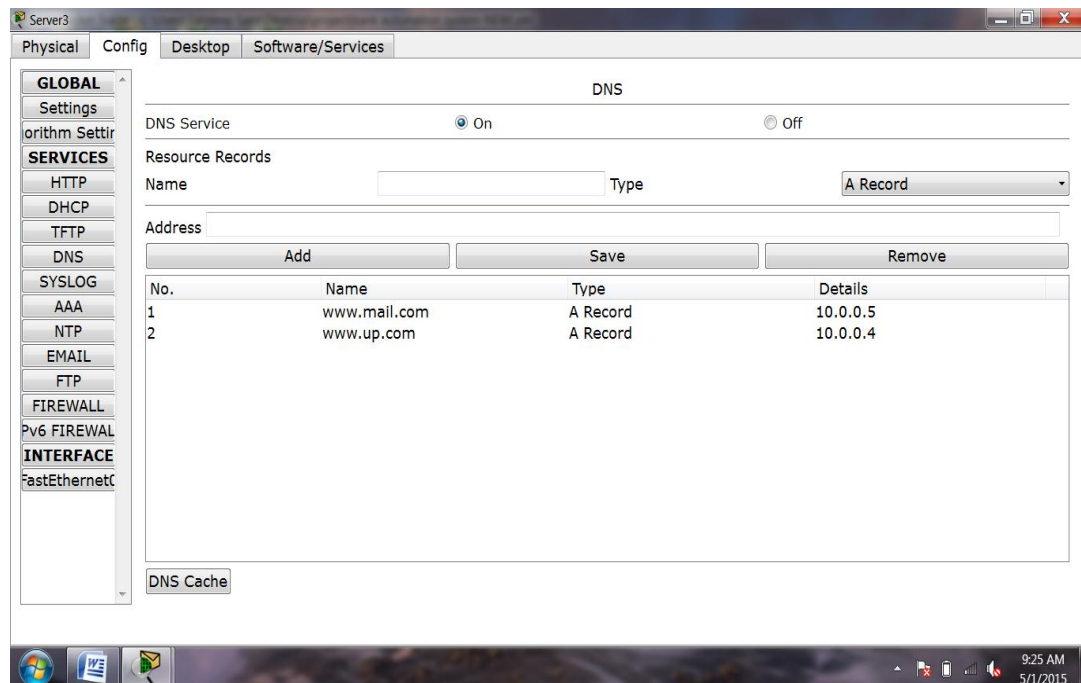


Fig. 6.10 : DNS Server in packet tracer

6.7.2 DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol that allocates IP address to computer on a network. DHCP centralized the management of IP address allocation and reduces human error associated with manual IP configuration. DHCP server supplies all the necessary networking parameters. Two things are always handed out as a part of DHCP configuration: IP address and subnet mask. Further DHCP will frequently configure clients with optional values, such as a default gateway, DNS server address, and the address of a Window Internet Naming Server, if one is present. Scenario showing DHCP server IP address allocation.

Installation Steps of DHCP Server

- **Start**→ **control panel**
- **Add and remove program**→ **add and remove window components**
- Select **networking services** and click on **detail button**
- Check box of **DHCP server**
- **Ok**→ **finish**

Steps To Configure DHCP Server

- **Start**→ **program**→ **administrative tool**
- Select **DHCP**
- **Create new scope in action menu**→ **new scope** → **next**
- Give **scope name**→ **next**
- Give **IP address range**→ **next**
- Add **exclusion name**→ **next**
- Check **lease duration**→ **next**→ **finish**

On Client Side

- Go to **LAN card properties** → select **TCP/IP protocol**→ **properties**
- Select **obtain IP address automatically**
- Go to **command prompt (cmd)**
- Give **command**

Backup of DHCP Server

We can take backup of all the configuration in DHCP server with the help of administrator. Backup means to export the DHCP database to another system, as it is helpful in case due to any reason our data is corrupted or deleted, we can take our database from the place where it is stored. Steps of taking backup :

- Stop the DHCP server and disable the DHCP server services
- Copy the DHCP server directory to a temporary location, say pen drive or on a new DHCP server.

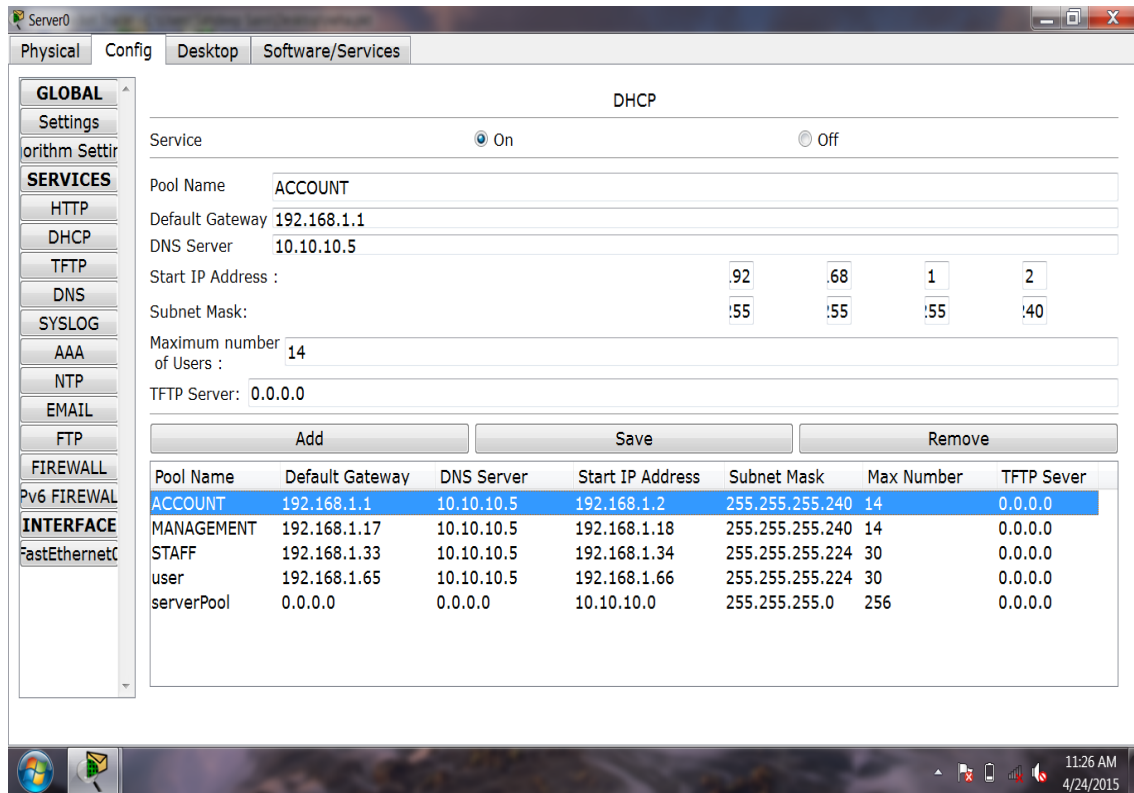


Fig. 6.11 : DHCP Server in packet tracer

CHAPTER -7

TECHNOLOGY

7.1 Routing

It is a process of transferring information through an inter network i.e from one network to another. Routing connect different networks having ID help in process of routing. The dial-in properties also allow for specific IP address to be assigned to a user. This is the only way in Window Server 2003 that you can assign a specific IP to a user. To assign a specific IP to a user, check the box next to assign A Static IP Address and enter a valid IP in the space provided. Static routing can also be specified as per user. By defining static routes, users can be limited to only specific parts of networks. In an internetwork a router must then about all the networks present in the for effort websites, there are hardware routers like CISCO. Even win 2003 server computer configured as router. In simple words Router is a computer with two network cards.

These two network cards, then, are attached to two different logical IP networks. The routing table helps direct traffic that is passed through the router. Now when there is a router, also there is a routing table, there is a need to configure the router in order for that router to pass along traffic to the proper network. There are two ways the routing table can be built and modified: either manually or automatically.

Routing is a process or technique to identify the path from one network to another. Routers don't really care about hosts—they only care about networks and the best path to each network. To route the packet the router must know the following things:

- Destination network
 - Neighbor device from witch it can learn about remote Networking.
 - Possible number of routers to reach the destination.
 - Best route to reach the destination.
 - How to maintain & verify the routing information.
-

7.1.1 Types of Routing

- (i) Static Routing
- (ii) Default Routing
- (iii) Dynamic Routing

(i) Static Routing

In this routing information required for routing is manually entered into the router by administrator. In static routing an administrator specifies all the routes to reach the destination. Static routing occurs when you manually add routes in each router's routing table. By default, Static routes have an Administrative Distance (AD) of 1

Features

- There is no overhead on the router CPU.
- There is no bandwidth usage between routers.
- It adds security, because the administrator can choose to allow routing access to certain networks only.

Advantages of static routing

- Fast and efficient.
- More control over selected path.
- Less overhead for router.
- Bandwidth of interfaces is not consumed in routing updates.

Disadvantages of static routing

- More overheads on administrator.
- Load balancing is not easily possible.
- In case of topology change routing table has to be change manually.

Syntax for Static Routing

Router (config)# ip route <destination N/w> <Subnet mask> <Next Hope- address or exit interface> [<administrative distance>Permanent].

(ii) Default Routing

Default routing is used to send packets with a remote destination network not in the routing table to the next-hop route. Default routing is also a type of static routing which reduces the routing overhead & default routing is also used with stub networks. Stub networks are those having a single exit interface. Default routing is also used for unknown destination. A special address is used to perform the default routing ie 0.0.0.0

The scenario for default routing is same and but the commands used at the routers having single exit interface like R1 and R3 have different commands.

At Router (R1)

```
Router(config)#ip route 0.0.0.0 0.0.0.0 40.0.0.2
```

```
Router#show ip route
```

At Router (R3)

```
Router(config)#ip route 0.0.0.0 0.0.0.0 50.0.0.1
```

```
Router#show ip route
```

(iii) Dynamic Routing

The other way to manage a router routing tables is to let the computer do it for you. Just like DHCP allocate IP addresses, configuring the dynamic routing protocol usually means less errors due to human error, and less administrative overhead. In dynamic routing, routing information is automatically entered in the router using protocols like RIP AND OSPF. These routing protocols used by Window Server 2003 use one of two kinds of algorithms to determine the best possible path for a packet to get to its destination, either distance vector or link state. RIP is used for small networks where as OSPF is used for large networks Dynamic routing is when protocols are used to find networks and update routing table on routers.

In dynamic routing, we will enable a routing protocol on router. This protocol will send its routing information to the neighbor router. The neighbors will analyze the information and write new routes to the routing table. The routers will pass routing information receive from one router to other router also. If there are more than one path available then routes are compared and best path is selected. Some examples of dynamic protocol are: - RIP, IGRP, EIGRP, OSPF.

7.1.2 Types of routing protocols

There are two type of routing protocols used in internetworks:

(i) Interior Gateway Protocols (IGPs)

IGPs are used to exchange routing information with routers in the same Autonomous System(AS) number. Routing which is performed within a single autonomous system is known as interior routing. The protocol that are used to perform this type of routing are known as IGP(Interior Gateway Protocol).

These protocols are:-

- (i) RIPv1 (Routing Information Protocol Version 1)
- (ii) RIPv2 (Routing Information Protocol Version 2)
- (iii) EIGRP (Enhanced Interior Gateway Routing Protocol)
- (iv) OSPF (Open Shortest Path First)
- (v) IS-IS (Intermediate System to Intermediate System)

(ii) Exterior Gateway Protocols (EGPs)

EGPs are used to communicate between different Autonomous System. Protocol that used to do this type of routing are called exterior gateway protocols.

Autonomous System:- An autonomous system is a collection of networks under a common administrative domain, which basically means that all routers sharing the same routing table information are in the same AS.

7.2 Subnetting

Subnetting is a process or a technique to divide large and complex networks into smaller parts or smaller networks and each network is called as subnet. Subnetting is done to reduce the wastage of IP addresses ie instead of having a single huge network for an organization smaller networks are created within a given huge network. Subnetting allows the user to create multiple logical networks within a single Class A, B or C based networks. In subnetting, the IPv4 address is broken into two parts; network id and host id. This process borrows bits from the host id field.

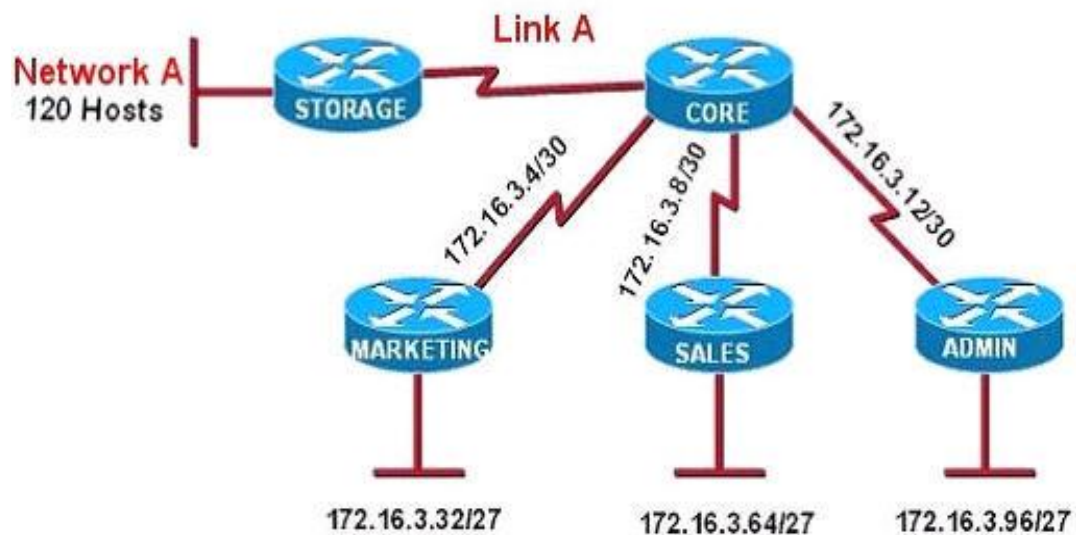


Fig. 7.1 : Configuration example of subnetting

7.2.1 Subnet Mask

A subnet mask specifies the part of IP address that is to be used for identifying a sub network. A subnet mask when logically ANDed with IP address provides a 32-bit network address. This binary address gives the first address in the subnet block specified in the large network.

7.2.2 Default Mask

Classful addresses consist of three classes; Class A, Class B, Class C used for subnetting. Each class has a default subnet mask. Class A consists of eight 1s in the network address field and 24 0s in the remaining field, Class B consists of 16 1s in network address field and 16 0s in the remaining field, and Class C contains 24 1s in the network address field and the remaining 8 bytes as 0s. The default address mask in binary and dotted-decimal is shown in the table

7.2.3 Types of Subnetting

- Fixed Length Subnet Mask (FLSM)
- Variable Length Subnet Mask (VLSM)

VLSM

In VLSM to allocate IP addresses to subnets depending upon the no. of hosts. The network having more no of hosts is given priority and the one having least no of host comes at last and for each network the subnet is assigned separately. As in the scenario given:

7.2.4 Advantages of subnetting

- Size of the physical networks is reduced and hence easy to manage.
- Reduce network traffic.
- Easy to troubleshoot.
- Reduce the wastage of IP address.

7.3 LAN Switching

Types of switching

- Layer-2 switching
- Layer-3 switching

7.3.1 Layer-2 Switching

Layer-2 switching is hardware based, which means it uses the MAC address from the host NIC card to filter the network traffic. Layer-2 switch can be considered as multi- port bridge.

Layer 2 switches are fast because they do not look at the network layer header information, instead it looks at the frames hardware address before deciding to either forward the frame or drop it.

Limitations of Layer 2 Switching

With bridge the connected networks are still one large broadcast domain. Layer 2 switch cannot break the broadcast domain, this cause performance issue which limits the size of your network. For this one reason the switch cannot completely replace routers in the internetwork.

7.3.2 Switching methods

There are three types of switching method:

(i) Store-and-forward switching

The entire frame is received and the CRC is computed and verified before forwarding the frame. If the frame is too short (i.e. less than 64 bytes including the CRC), too long (i.e. more than 1518 bytes including the CRC), or has CRC error, it will be discarded. It has the lowest error rate but the longest latency for switching. However, for high-speed network (e.g. Fast Ethernet or Gigabit Ethernet network), the latency is not significant. It is the most commonly used switching method, and is supported by most switches.

(ii) Cut-through switching

It is also known as Fast Forward switching. A frame is forwarded as soon as the destination MAC address in the header has been received (the 1st 6 bytes following the preamble). It has the highest error rate (because a frame is forwarded without verifying the CRC and confirming there is no collision) but the shortest latency for switching.

(iii) Fragment-free switching (Modified Cut-through switching)

A frame is forwarded after the first 64 bytes of the frame have been received. Since a collision can be detected within the first 64 bytes of a frame, fragment-free switching can detect a frame corrupted by a collision and drop it. Therefore, fragment-free switching provides better error checking than cutthrough switching. The error rate of fragment-free switching is above store and-forward switching and below cut-through switching. The latency of fragment-free switching is shorter than store-and- forward switching and longer than cut through switching.

7.4 RIP (Routing Information Protocol)

Routing Information Protocol is a true distance-vector routing protocol. It is an IGP (Inter Gateway Protocol). It sends the complete routing table out to all active interfaces every 30 seconds to its immediate neighbour. This slow convergence means that one router sends a request to other about its route or network get networks which are not assigned to it after all three routers have same networks, this process is repeated to send and receive request so it is called slow convergence. RIP only uses hop count to determine the best way to remote network, but it has a maximum allowable hop count of 0-15 by default, meaning that 16 is deemed unreachable.

RIP version 1 uses only class full routing, which means that all devices in the network must use the same subnet mask. RIP version 2 provides something called prefix routing, and does send subnet mask information with the route updates. This is called classless routing.

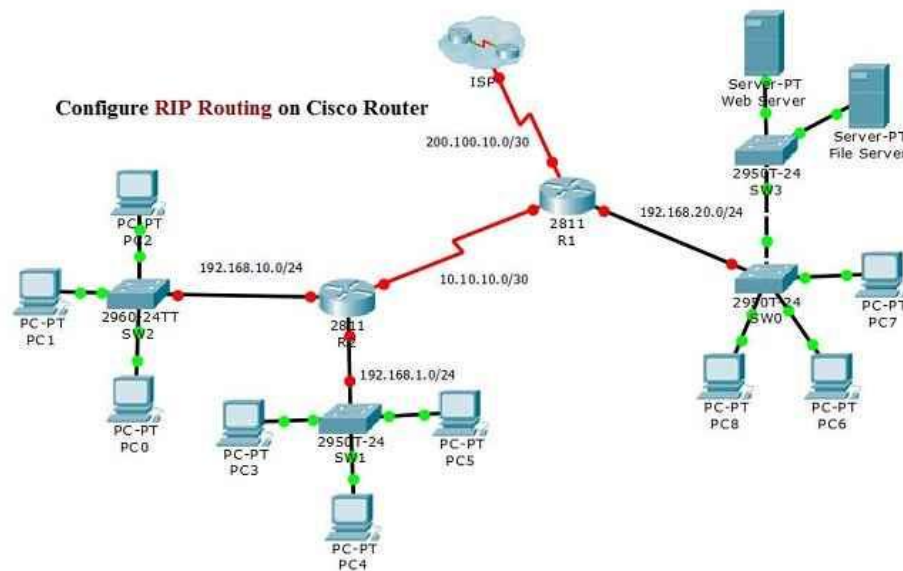


Fig. 7.2 : Configuration example of RIP routing

Hop Count

It is a way of measurement. Hop count limit is 15. This routing supports only 15 routers, if there is one more router in the network then this routing will fail.

7.4.1 Features

- RIP version1 and version2, with the ability to configure individual network cards with separate versions.
- Calculations used to avoid routing loops and speed recovery of the network whenever topology changes occur.
- Route filters; you can configure RIP to except information from only certain networks, and also choose which routes will be shared with RIP routers.
- Peer filters, which allow control over which router announcements are accepted.
- Default administrative distance is 120.
- Simple password authentication support. But there are significant drawbacks, which makes RIP a poor, if not unusable solution for large networks.
- For example, the maximum hop count used for RIP routers is15, making network 16 hops away (or more) unreachable where RIP is concerned.

7.5 IGRP (Interior Gateway Protocol)

Interior Gateway Routing Protocol (IGRP) is a Cisco-proprietary distance-vector routing protocol. To use IGRP, all your routers must be Cisco routers. IGRP has a maximum hop count of 255 with a default of 100. IGRP uses bandwidth and delay of the line by default as a metric for determining the best route to an internetwork. Reliability, load, and maximum transmission unit (MTU) can also be used, although they are not used by default.

7.6 EIGRP (Enhanced Interior Routing Protocol)

Enhanced IGRP (EIGRP) is a classless, enhanced distance-vector protocol that gives us a real edge over IGRP. Like IGRP, EIGRP uses the concept of an autonomous system to describe the set of contiguous routers that run the same routing protocol and share routing information. But unlike IGRP, EIGRP includes the subnet mask in its route

updates. The advertisement of subnet information allows us to use VLSM and summarization when designing our networks.

EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. It sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router. EIGRP has a maximum hop count of 255.

7.6.1 Features

Powerful features that make EIGRP a real standout from IGRP.

- Support for IP, IPX, and AppleTalk via protocol-dependent modules. Considered classless (same as RIPv2 and OSPF).
- Support for VLSM/CIDR.
- Support for summaries and discontinuous networks.
- Efficient neighbor discovery.
- Communication via Reliable Transport Protocol (RTP).
- Best path selection via Diffusing Update Algorithm (DUAL).
- Cisco calls EIGRP a distance vector routing protocol, or sometimes an advanced distance vector or even a hybrid routing protocol.
- EIGRP supports different Network layer protocols through the use of protocol-dependent modules (PDMs).
- Each EIGRP PDM will maintain a separate series of tables containing the routing information that applies to a specific protocol. It means that there will be IP/EIGRP tables, IPX/EIGRP tables, and AppleTalk/EIGRP tables.

7.6.2 Neighbor Discovery

Before EIGRP routers are willing to exchange routes with each other, they must become neighbors. To maintain the neighborhood relationship, EIGRP routers must also continue receiving Hellos from their neighbors. EIGRP routers that belong to different autonomous systems (ASes) don't automatically share routing information and

they don't become neighbors. There are three conditions that must be met for neighborship establishment:

- Hello or ACK received
- AS numbers match
- Identical metrics (K values)

7.7 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is an open standards routing protocol that's been implemented by a wide variety of network vendors, including Cisco. This works by using the Dijkstra algorithm. First, a shortest path tree is constructed, and then the routing table is populated with the resulting best paths. OSPF converges quickly, although perhaps not as quickly as EIGRP, and it supports multiple, equal-cost routes to the same destination. But unlike EIGRP, it only supports IP routing. OSPF is an IGP protocol.

It is a link state routing protocol. It is supported by many operating systems. Its default AD is 110, hop count limit is unlimited. It is classless routing protocol, supports VLSM/CIDR. By default the highest IP address of interface will be elected as Router id. The biggest reason OSPF is the choice in large networks is its efficiency; instead of changing routing table via broadcast the way RIP does, OSPF configured routers maintain a map of the network. The mapping is called the link state database, OSPF routers keep the link state database up to date. Once changes have been made to link state database, an OSPF router's link state database is recalculated.

As the networks start to multiply, the size of the link state database increases, and a corresponding hit on router performance results. Areas are connected to each other through a backbone area, with each router only responsible for the link state database for those areas connected to the routers. Area Border Routers (ABRs) then connect one backbone area to another. The biggest drawback of OSPF is its complexity; OSPF requires proper planning and is more difficult to configure and administer.

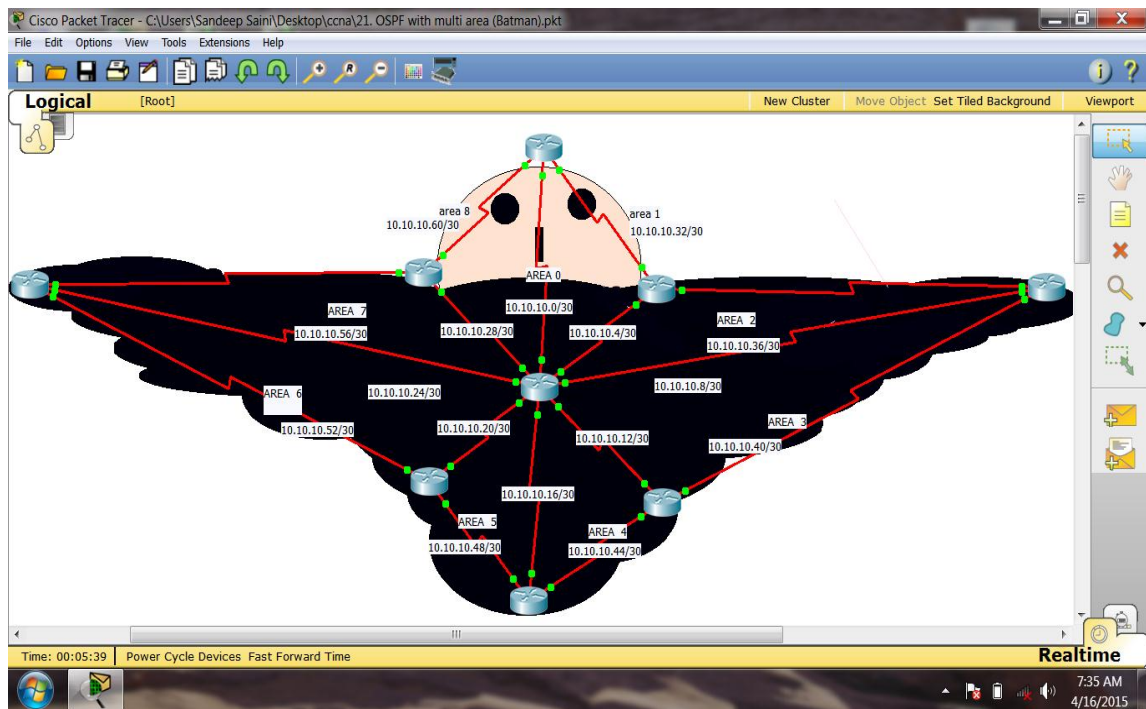


Fig. 7.3 : Configuration example of OSPF

7.7.1 Features

- Consists of areas and autonomous systems
- Minimizes routing update traffic
- Allows scalability
- Supports VLSM/CIDR
- Has unlimited hop count
- Allows multi-vendor deployment (open standard)

7.7.2 Advantages

- Routes calculated with OSPF are always loop free.
- OSPF can scale much more easily than RIP.
- Reconfiguration for network topology changes is faster.
- To decrease routing overhead
- To speed up convergence
- To confine network instability to single areas of the network

- (i) Minimum routing updates.
- (ii) Priorities on all the CISCO routers the priority is 1.
- (iii) The routers having highest IP address become BRD(Border Destination Router).

7.7.3 OSPF Terminology

- **Link**

A link is a network or router interface assigned to any given network. When an interface is added to the OSPF process, it's considered by OSPF to be a link.

- **Router ID**

The Router ID (RID) is an IP address used to identify the router. Cisco chooses the Router ID by using the highest IP address of all configured loopback interfaces. If no loopback interfaces are configured with addresses, OSPF will choose the highest IP address of all active physical interfaces.

- **Neighbors**

Neighbors are two or more routers that have an interface on a common network, such as two routers connected on a point-to-point serial link.

- **Adjacency**

An adjacency is a relationship between two OSPF routers that permits the direct exchange of route updates. OSPF is really picky about sharing routing information—unlike EIGRP, which directly shares routes with all of its neighbors. Instead, OSPF directly shares routes only with neighbors that have also established adjacencies. And not all neighbors will become adjacent—this depends upon both the type of network and the configuration of the routers.

7.7.4 OSPF areas

An OSPF area is a grouping of contiguous networks and routers. All routers in the same area share a common Area ID.

Broadcast (multi-access)

Broadcast (multi-access) networks such as Ethernet allow multiple devices to connect to (or access) the same network, as well as provide a *broadcast* ability in which a single packet is delivered to all nodes on the network. In OSPF, a DR and a BDR must be elected for each broadcast multi-access network.

Non-broadcast multi-access

Non-Broadcast Multi-Access (NBMA) networks are types such as Frame Relay, X.25, and Asynchronous Transfer Mode (ATM). These networks allow for multi-access, but have no broadcast ability like Ethernet. So, NBMA networks require special OSPF configuration to function properly and neighbor relationships must be defined.

- **Point-to-point**

Point-to-point refers to a type of network topology consisting of a direct connection between two routers that provides a single communication path. The point-to-point connection can be physical, as in a serial cable directly connecting two routers, or it can be logical.

- **Point-to-multipoint**

Point-to-multipoint refers to a type of network topology consisting of a series of connections between a single interface on one router and multiple destination routers.

7.7.5 Steps to apply OSPF

Syntax:

```
Router(config)#router ospf <ospf process id>
```

```
Router(config-router)#network <network address> <wild card mask> area<area  
++number>
```

7.8 NAT (Network Address Translation)

If we have to connect many computers with a single IP address then we will use NAT. NAT exchange IP packet between local network and internet. The routing and remote access server of window 2K3 server provide us with a component known as NAT. By enabling NAT on a Server 2003 system, you allow connected users on a private system to share a single connection to access a public network such as the internet i.e. NAT enable multiple client computer to connect the internet through a single publicly registered IP address. A NAT server translate private IP address to public addresses. NAT eliminates the need for large number of IP addresses by mapping externally assigned IP addresses. When deploying NAT, it is needed to configure setting on both the client side and the server side. On the server side of NAT fill the IP address statically.

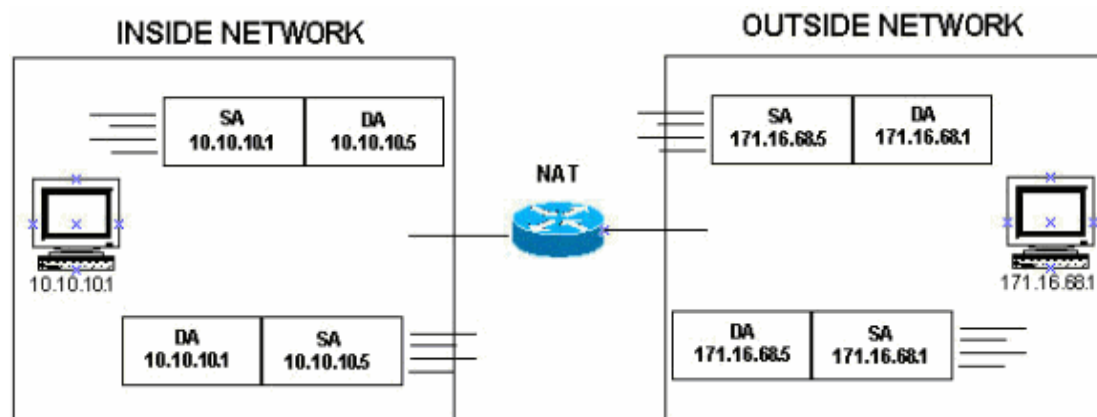


Fig.7.4: Configuration example of NAT

7.8.1 Steps to enable NAT server

- Open **internet** → **Tools** → **Internet options**
 - **Connections** → **LAN settings**
 - Untick the **IP and port address**
 - **Ok** → **Ok** → give site name
-

With the client side configured, there are few things to do on NAT server.

- **Start**→ **administrator tools**→ **Routing & Remote Access**
- Right click on **My Computer**→ right click on **computer name**
- Select option **Configure and enable routing & remote access**
- **Welcome to routing** → **next**→ **next**
- Select **NAT**→ **next**
- Select **LAN card** which is to be connected to internet
- **Next**→ **next**

7.8.2 Advantages of NAT

- It can prevent the depletion of IPv4 addresses.
- NAT (Network Address Translation) can provide an additional layer of security by making the original source and destination addresses hidden.
- NAT (Network Address Translation) provides increased flexibility when connecting to the public Internet.
- NAT (Network Address Translation) allows to use your own private IPv4 addressing system and prevent the internal address changes if you change the service provider.

7.8.3 Disadvantages of NAT

- NAT (Network Address Translation) is a processor and memory resource consuming technology, since NAT (Network Address Translation) need to translate IPv4 addresses for all incoming and outgoing IPv4 datagrams and to keep the translation details in memory.
 - NAT (Network Address Translation) may cause delay in IPv4 communication.
 - NAT (Network Address Translation) cause loss of end-device to end-device IP traceability.
 - Some technologies and network applications will not function as expected in a NAT (Network Address Translation) configured network.
-

7.9 PAT (Port Address Translation)

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Port address translation (PAT) is a function that allows multiple users within a private network to make use of a minimal number of IP addresses. Its basic function is to share a single IP public address between multiple clients who need to use the Internet publicly. It is an extension of network address translation (NAT). Port address translation is also known as overload or port overload.

An example of PAT is a home network that is connected to the Internet. Within this setup, the system's router is assigned a discrete IP address. Multiple users can access the Internet over the router, and are each assigned a port number as they do so. PAT is used to give internal network hosts access to external network hosts. In a local area network (LAN) environment, many clients are accessing the Internet via the LAN's router.

Configuring PAT: Address Pool

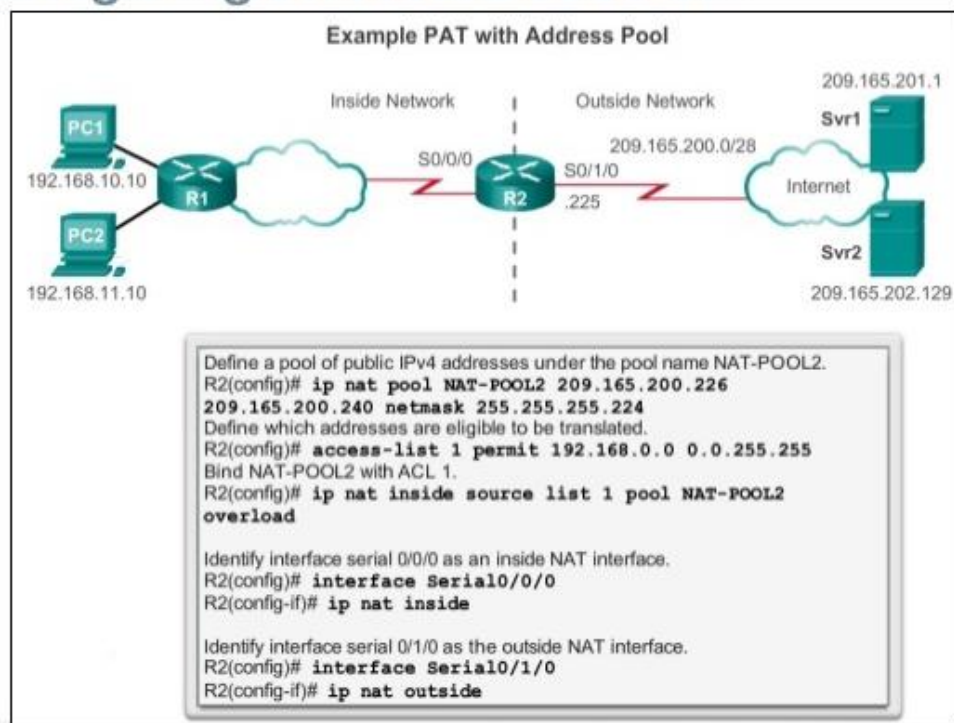


Fig. 7.5 : PAT example & configuration

7.10 TELNET

Telnet stands for terminal network, telephone network, terminal encapsulation on the network. Purpose of Telnet is to access the remote device in order to configure it. It provides textual access of the remote device. It uses the services of TCP. Telnet service is used where small bandwidth is low. It provides textual access of the remote device.

7.10.1 To Access the Device Remotely

For this purpose we have to assign the IP addresses to the PCs and the interfaces. For Telnet the Routers are to be configured with RIP version1 , so that the device can ping each other. Also DCE cable is used to connect the Routers. The serial link should have the speed of 64K also apply vty password and enable secret password. Set up the Routers so that they can manage via Telnet.

First of all select the PCs and the routers connect the ports to the router, double click on router, switch off the router if it is on. Then select the serial port according to the routers, switch on the router. Select the cable to connect the Routers. Router to Router connections are made by the serial cable, so go on first Router select the serial port as s0/1/0 in the scenario, then go to the other Router and connect the serial cable at interface s1/0. Accordingly connect the third Router with interfaces s1/1 and s1/2.

Now connect the PCs to the routers, to do this first select the console cable, click on the PC select RS232 option, then connect it on the Router and select console cable. Now select cross- over cable on the PC select Fast Ethernet option and on the Router select f0/0 option now as the PCs and Routers are connected to each other assign IP addresses to the PCs and the Routers. According to the fig set the IP addresses of the PCs→ double click on the PC→ choose the option of desktop→ IP configuration. Now set the IP address, subnet mask, and the default gateway. Likewise set the IP address of all the PCs. Now set the IP address of the interfaces of router.

7.10.2 To Telnet a device from router

At all the Routers use these commands.

```
Router(config)#line vty 0 4
```

```
Router(config-line)#password cobra
```

```
Router(config-line)#login
```

```
Router(config)#enable password cobra
```

```
Router(config)#enable secret cobra1
```

```
Router#telnet <IP>
```

Or

```
Router>telnet <IP>
```

To exit from telnet session

```
Router#exit
```

To exit from a hanged telnet session

```
Ctrl+shft+6
```

Or

```
Router#disconnect
```

To display connected session

```
Router#show sessions
```

This command shows those sessions, which are created or connected by us. If we want anyone can telnet our router without password then on the line vty type command “No Login”.

7.11 TRUNCKING

Trunking is a technique used in data communications transmission systems to provide many users with access to a network by sharing multiple lines or frequencies. As the name implies, the system is like a tree with one trunk and many branches. Trunking is commonly used in very-high-frequency (VHF) radio and telecommunication systems.

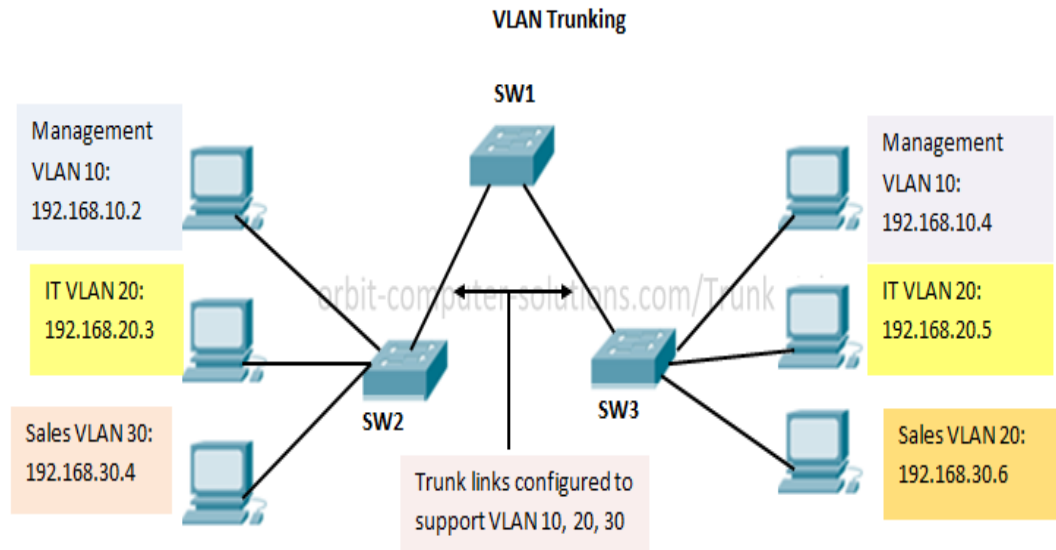


Fig. 7.6 : Truncking

Trunking can also be defined as a network that handles multiple signals simultaneously. The data transmitted through trunking can be audio, video, controlling signals or images. Telecommunication networks all across the globe are based on trunking. Trunking reduces the size of a telecom network and increases bandwidth. VHF radio used by police and control centers is also based on trunking.

7.12 VLAN (Virtual LAN)

VLAN provides Virtual Segmentation of Broadcast Domain in the network. The devices, which are member of same Vlan, are able to communicate with each other. The devices of different Vlan may communicate with each other with routing. So that different Vlan devices will use different n/w addresses.

Vlan provides following advantages: -

- Logical Segmentation of network
- Enhance network security

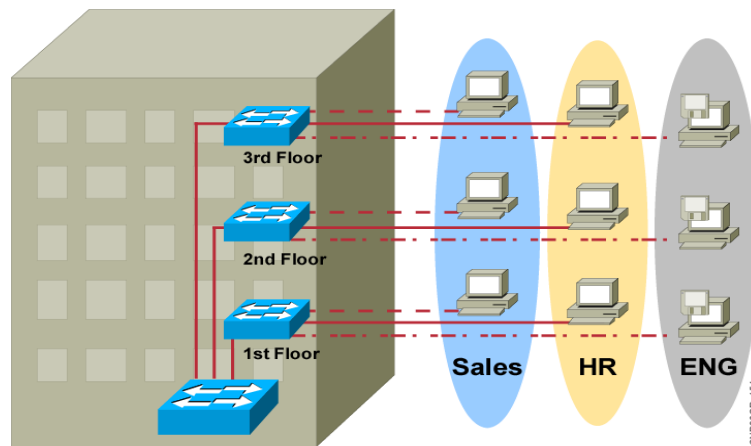


Fig. 7.7 : VLAN

7.12.1 Creating port based Vlan

In port based Vlan, first we have to create a Vlan on manageable switch then we have to add ports to the Vlan. A Virtual LAN (VLAN) is a broadcast domain created based on the functional, security, or other requirements, instead of the physical locations of the devices, on a switch or across switches. With VLANs, a switch can group different interfaces into different broadcast domains. Without VLANs, all interfaces of a switch are in the same broadcast domain; switches connected with each other are also in the same broadcast domain, unless there is a router in between. Different ports of a switch can be assigned to different VLANs.

7.12.2 Advantages of implementing VLAN

- It can group devices based on the requirements other than their physical locations.
 - It breaks broadcast domains and increases network throughput.
 - It provides better security by separating devices into different VLANs.
 - Since each VLAN is a separate broadcast domain, devices in different VLANs cannot listen or respond to the broadcast traffic of each other.
 - Inter-VLAN communication can be controlled by configuring access control lists on the router or Layer 3 switch connecting the VLANs.
-

7.12.3 Types of VLAN

Static VLAN

Assigning VLANs to switch ports based on the port numbers. It is easier to set up and manage.

Dynamic VLAN

Assigning VLANs to switch ports based on the MAC addresses of the devices connected to the ports. A VLAN management application is used to set up a database of MAC addresses, and configure the switches to assign VLANs to the switch ports dynamically based on the MAC addresses of the connected devices. The application used by Cisco switches is called VLAN Management Policy Server (VMPS). Cisco switches support a separate instance of spanning tree and a separate bridge table for each VLAN.

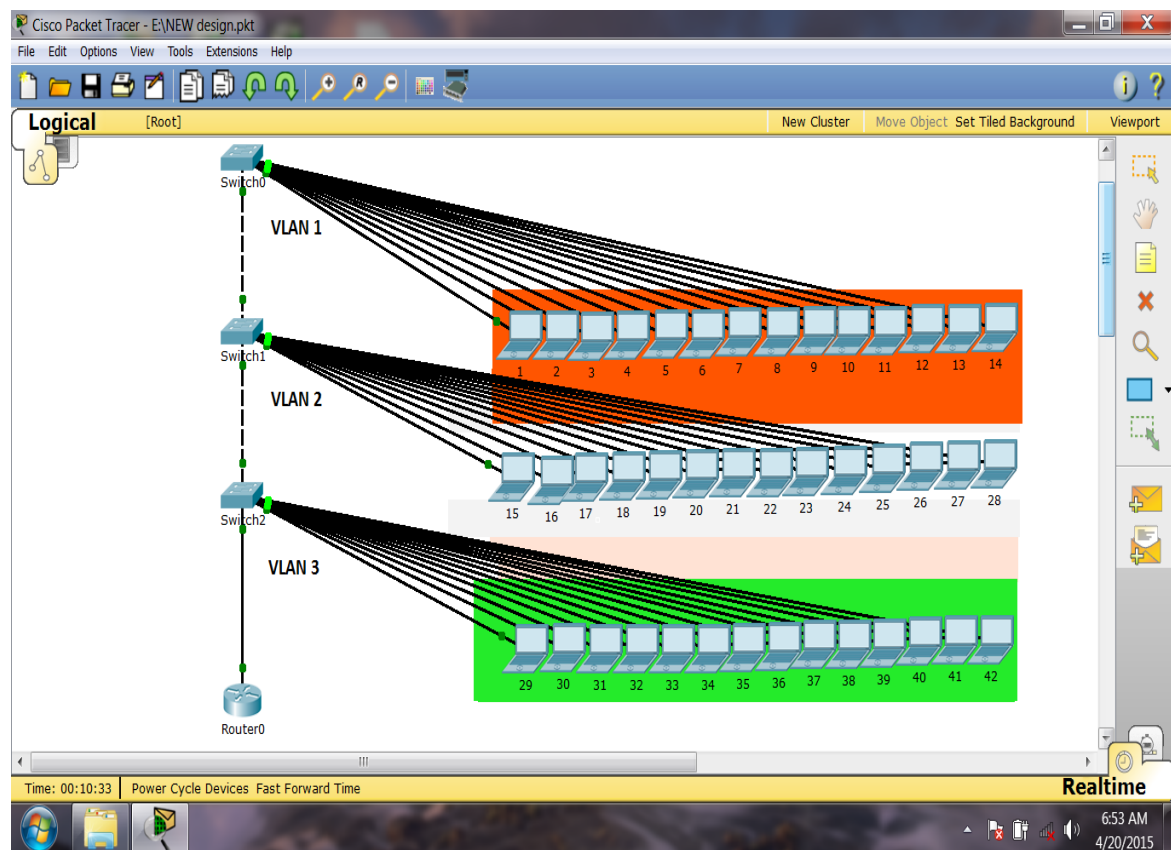


Fig. 7.8 : Configuration example of VLAN

7.12.4 VLAN links

There are two different types of links in a switched network:

Access link

A link from Pc to switch is called as access link or A link that is part of only one VLAN. Therefore, a port connecting to an access link can be a member of only one VLAN. And the mode of port is called as access mode.

Trunk link

A link from switch to switch or switch to router is called as trunk link. A 100 Mbps or 1000 Mbps point-to-point link that connects switches or routers, and carries frames of different VLANs . Therefore, a port connecting to a trunk link can be a member of multiple VLANs. All VLANs are configured on a trunk link by default. VLAN Trunking, by making use of frame tagging, allows traffic from different VLANs to transmit through the same Ethernet link (trunk link) across switches.

7.12.5 VLAN Operation

- Each logical VLAN is like a separate physical bridge.
- VLANs can span across multiple switches.
- Trunks carry traffic for multiple VLANs.
- Trunks use special encapsulation to distinguish between different VLANs.

7.12.6 Commands

Commands to create Vlan

```
Switch#vlan database
```

```
Switch(vlan)#vlan <no.> [name <name of vlan>]
```

```
Switch(vlan)#exit
```

Commands to configure ports for a Vlan

```
Switch(config)#interface <type> <no.>
```

```
Switch(config-if)#switchport access vlan <no.>
```

```
Switch(config-if)#exit
```

Commands to configure multiple ports in a vlan

```
Switch(config)#interface range <type> <slot/port no. (space)–(space) port no.>
```

```
Switch(config-if)#switchport access vlan <no.>
```

```
Switch(config-if)#exit
```

Example: - Suppose we want to add interface fast Ethernet 0/10 to 0/18 in vlan5

```
Switch(config)#interface range fastethernet 0/10 – 18
```

```
Switch(config-if)#switchport access vlan 5
```

```
Switch(config-if)#exit
```

7.13 Access Control Lists (ACLs)

Access Control List (ACL) are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for their networks. This can be applied on routers (Cisco).

ACLs provide a powerful way to control traffic into and out of your network; this control can be as simple as permitting or denying network hosts or addresses. You can configure ACLs for all routed network protocols. The most important reason to configure ACLs is to provide security for your network. However, ACLs can also be configured to control network traffic based on the TCP port being used.

7.13.1 Working of ACLs

A router acts as a packet filter when it forwards or denies packets according to filtering rules. As a Layer 3 device, a packet-filtering router uses rules to determine whether to permit or deny traffic based on source and destination IP addresses, source port and destination port, and the protocol of the packet. These rules are defined using access control lists or ACLs.

To simplify how ACL or a router uses packet filtering work, imagine a guard stationed at a locked door. The guard's instruction is to allow only people whose names appear on a quest list to pass through the door. The guard is filtering people based on the condition of having their names on the authorized list.

When a packet arrives at the router, the router extracts certain information from the packet header and makes decisions according to the filter rules as to whether the packet can pass through or be dropped. Packet filtering process works at the Network layer of the Open Systems Interconnection (OSI) model, or the Internet layer of TCP/IP.

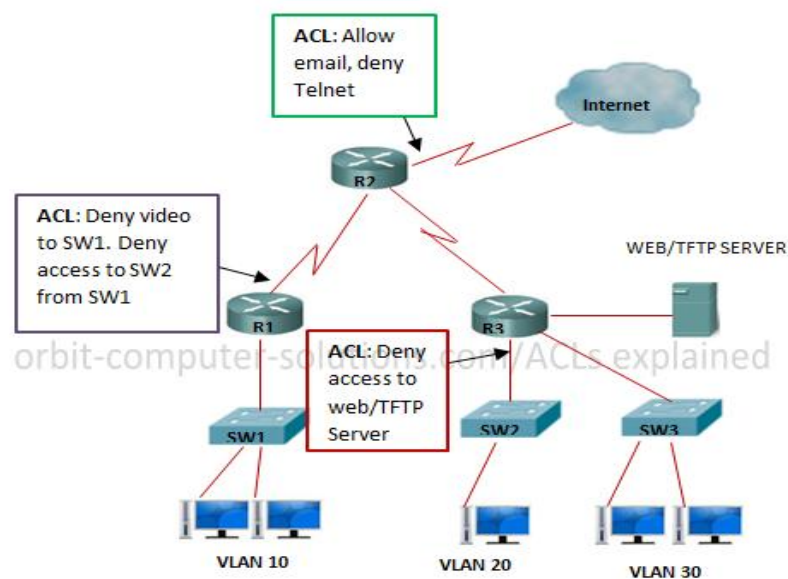


Fig. 7.9 : Access control list

7.13.2 Use of ACLs

- Limits network traffic to increase network performance.
- ACLs provide traffic flow control by restricting the delivery of routing updates.
- It can be used as additional security.
- Controls which type of traffic are forwarded or blocked by the router.
- Ability to control which areas a client access.

7.13.3 Types of Access Control Lists

(i) Standard access-list

Standard access lists create filters based on source addresses and are used for server based filtering. Address based access lists distinguish routes on a network you want to control by using network address number (IP). Address-based access lists consist of a list of addresses or address ranges and a statement as to whether access to or from that address is permitted or denied.

Example of the command syntax for configuring a standard numbered IP ACL:

R1(config)# access-list {1-99} {permit | deny} source-addr [source-wildcard]

(ii) Extended access lists

Extended access lists create filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet based filtering for packets that traverse the network.

Example of the command syntax for configuring an extended numbered IP ACL:

Router(config)# access-list {100-199} {permit | deny} protocol source-addr [source-wildcard] [operator operand] destination-addr [destination-wildcard] [operator operand] [established]

Chapter 8

CODING

8.1 Configuration of Router

Router - R1

```
hostname Router-R1
!
spanning-tree mode pvst
!
interface FastEthernet0/0
noip address
duplex auto
speed auto
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.1.129 255.255.255.192
ip helper-address 10.0.0.2
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.1.1 255.255.255.240
ip helper-address 10.0.0.2
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.1.33 255.255.255.224
ip helper-address 10.0.0.2
!
interface FastEthernet0/0.50
encapsulation dot1Q 50
ip address 192.168.1.65 255.255.255.224
ip helper-address 10.0.0.2
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip access-group 105 out
duplex auto
speed auto
!
interface Serial1/0
ip address 20.10.10.1 255.255.255.0
!
```

```
routerospf 1
log-adjacency-changes
redistribute connected subnets
network 192.168.1.0 0.0.0.255 area 1
network 10.0.0.0 0.0.0.255 area 1
network 20.10.10.0 0.0.0.255 area 0
!
ip classless
!
access-list 105 deny tcp 192.168.1.128 0.0.0.63 host 10.0.0.4 eq www
access-list 105 permit ip any any
!
login
!
end
```

Router - R2

```
interface FastEthernet0/1
noip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
ip address 20.10.10.2 255.255.255.0
!
interface Serial1/1
ip address 30.10.10.1 255.255.255.0
!
routerospf 1
log-adjacency-changes
network 20.10.10.0 0.0.0.255 area 0
network 30.10.10.0 0.0.0.255 area 0
!
login
!
End
```

Router-R3

```
interface Serial1/0
ip address 30.10.10.2 255.255.255.0
!
interface Serial1/1
ip address 40.10.10.1 255.255.255.0
```

```
!  
routerospf 1  
log-adjacency-changes  
network 30.10.10.0 0.0.0.255 area 0  
network 40.10.10.0 0.0.0.255 area 0  
!  
login  
!  
End
```

Router - R4

```
hostname Router-R4  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/0  
noip address  
duplex auto  
speed auto  
shutdown  
!  
interface FastEthernet0/1  
noip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial1/0  
ip address 50.10.10.2 255.255.255.0  
!  
interface Serial1/1  
ip address 60.10.10.1 255.255.255.0  
!  
routerospf 1  
log-adjacency-changes  
network 50.10.10.0 0.0.0.255 area 0  
network 60.10.10.0 0.0.0.255 area 0  
!  
login  
!  
End
```

Router-R5

```
hostname Router-R5
!
ipdhcp pool USER
network 192.168.2.64 255.255.255.224
default-router 192.168.2.65
dns-server 70.10.10.3
ipdhcp pool ACCOUNTANT
network 192.168.2.0 255.255.255.240
default-router 192.168.2.1
dns-server 70.10.10.3
ipdhcp pool STAFF
network 192.168.2.32 255.255.255.224
default-router 192.168.2.33
dns-server 70.10.10.3
ipdhcp pool MANAGEMENT
network 192.168.2.0 255.255.255.224
default-router 192.168.2.17
dns-server 70.10.10.3
!
spanning-tree mode pvst
!
interface FastEthernet0/0
noip address
duplex auto
speed auto
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.2.65 255.255.255.224
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.2.1 255.255.255.240
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.2.17 255.255.255.240
!
interface FastEthernet0/0.50
encapsulation dot1Q 50
ip address 192.168.2.33 255.255.255.224
!
interface FastEthernet0/1
ip address 70.10.10.1 255.255.255.0
```

```
ip access-group 105 out
duplex auto
speed auto
!
interface Serial1/0
ip address 60.10.10.2 255.255.255.0
!
routerospf 1
log-adjacency-changes
network 60.10.10.0 0.0.0.255 area 0
network 70.10.10.0 0.0.0.255 area 2
network 192.168.2.0 0.0.0.255 area 2
!
ip classless
!
access-list 105 deny tcp 192.168.2.64 0.0.0.31 host 70.10.10.2 eq www
access-list 105 permit ip any any
!
login
!
end
```

Router-R6

```
hostname Router-R6
!
spanning-tree mode pvst
!
interface FastEthernet0/0
noip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
noip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
ip address 40.10.10.2 255.255.255.0
!
interface Serial1/1
ip address 50.10.10.1 255.255.255.0
!
```

```
interface Serial1/2
ip address 80.10.10.1 255.255.255.0
!
routerospf 1
log-adjacency-changes
network 40.10.10.0 0.0.0.255 area 0
network 80.10.10.0 0.0.0.255 area 0
network 50.10.10.0 0.0.0.255 area 0
!
login
!
End
```

Router-R7

```
hostname Router-R7
!
spanning-tree mode pvst
!
interface FastEthernet0/0
noip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
noip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
ip address 40.10.10.2 255.255.255.0
!
interface Serial1/1
ip address 50.10.10.1 255.255.255.0
!
interface Serial1/2
ip address 80.10.10.1 255.255.255.0
!
routerospf 1
log-adjacency-changes
network 40.10.10.0 0.0.0.255 area 0
network 80.10.10.0 0.0.0.255 area 0
network 50.10.10.0 0.0.0.255 area 0
!
```

```
login
!  
End
```

Router-R8

```
hostname Router-R8
!  
ipdhcp pool USER
network 192.168.3.64 255.255.255.224
default-router 192.168.3.65
dns-server 100.10.10.2
ipdhcp pool ACCOUNTANT
network 192.168.3.0 255.255.255.240
default-router 192.168.3.1
dns-server 100.10.10.2
ipdhcp pool MANAGEMENT
network 192.168.3.16 255.255.255.240
default-router 192.168.3.17
dns-server 100.10.10.2
ipdhcp pool STAFF
network 192.168.3.32 255.255.255.240
default-router 192.168.3.33
dns-server 100.10.10.2
!  
spanning-tree mode pvst
!  
interface FastEthernet0/0
noip address
duplex auto
speed auto
!  
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.3.65 255.255.255.224
!  
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.3.1 255.255.255.240
!  
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.3.17 255.255.255.240
!  
interface FastEthernet0/0.50
```

```
encapsulation dot1Q 50
ip address 192.168.3.33 255.255.255.240
!
interface FastEthernet0/1
ip address 100.10.10.1 255.255.255.0
ip access-group 105 out
duplex auto
speed auto
!
interface Serial1/0
ip address 90.10.10.2 255.255.255.0
!
routerospf 1
log-adjacency-changes
network 90.10.10.0 0.0.0.255 area 6
network 100.10.10.0 0.0.0.255 area 6
network 192.168.3.0 0.0.0.15 area 6
network 192.168.3.16 0.0.0.15 area 6
network 192.168.3.32 0.0.0.15 area 6
network 192.168.3.64 0.0.0.31 area 6
network 192.168.3.0 0.0.0.255 area 7
!
ip classless
!
access-list 105 deny tcp 192.168.3.64 0.0.0.31 host 100.10.10.3 eq www
access-list 105 permit ip any any
!
login
!
end
```

8.2 Configuration of Switch

```
hostname Switch
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/3
```

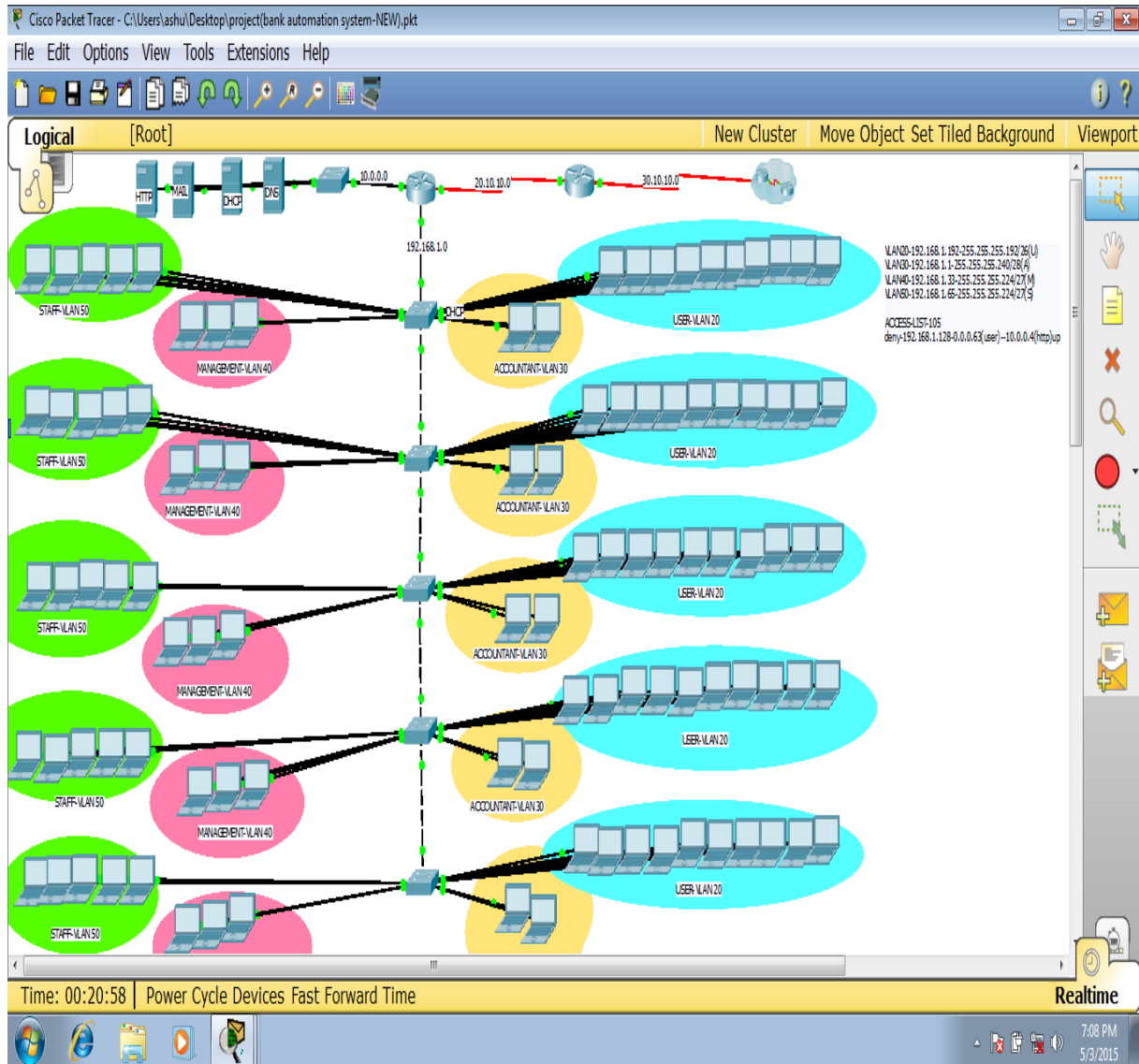
```
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 40
switchport mode access
```

```
!  
interface FastEthernet0/15  
switchport access vlan 40  
switchport mode access  
!  
interface FastEthernet0/16  
switchport access vlan 50  
switchport mode access  
!  
interface FastEthernet0/17  
switchport access vlan 50  
switchport mode access  
!  
interface FastEthernet0/18  
switchport access vlan 50  
switchport mode access  
!  
interface FastEthernet0/19  
switchport access vlan 50  
switchport mode access  
!  
interface FastEthernet0/20  
switchport access vlan 50  
switchport mode access  
!  
interface FastEthernet0/21  
switchport mode trunk  
!  
interface FastEthernet0/22  
switchport mode trunk  
!  
interface FastEthernet0/23  
switchport mode trunk  
!  
interface FastEthernet0/24  
switchport mode trunk  
!  
interface GigabitEthernet1/1  
!  
interface GigabitEthernet1/2  
!  
interface Vlan1  
no ip address  
shutdown  
!  
login  !! End
```

CHAPTER 9

RESULT

9.1 Project view



9.2 Communication between two pc

```
Ping statistics for 192.168.1.86:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.1.86

Pinging 192.168.1.86 with 32 bytes of data:

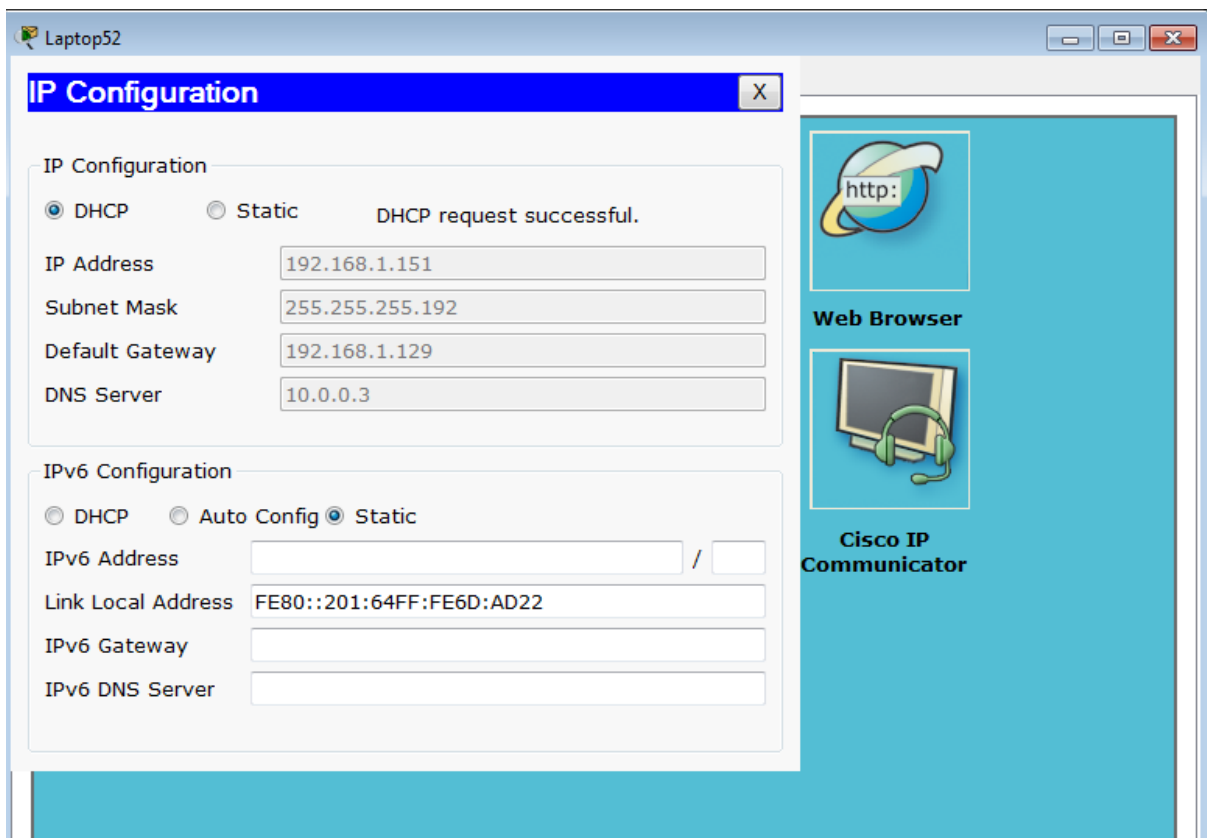
Reply from 192.168.1.86: bytes=32 time=2ms TTL=127
Reply from 192.168.1.86: bytes=32 time=0ms TTL=127
Reply from 192.168.1.86: bytes=32 time=0ms TTL=127
Reply from 192.168.1.86: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.1.86:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

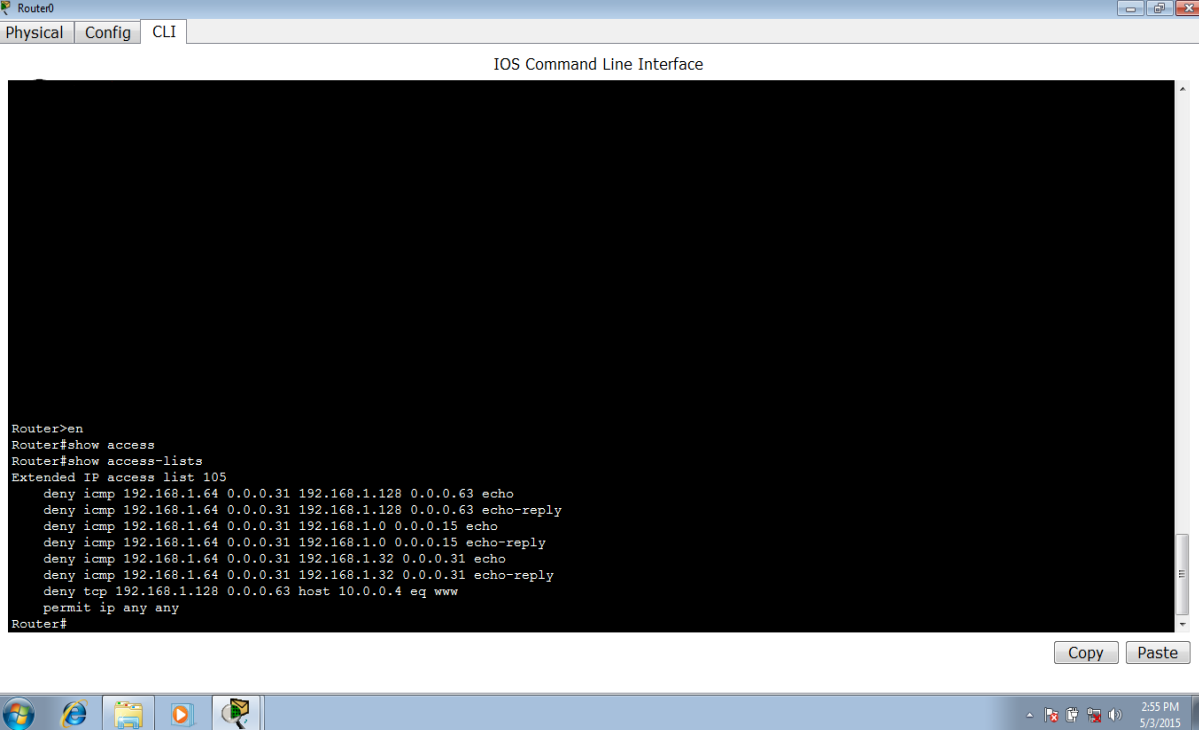
PC>
```



9.3 DHCP



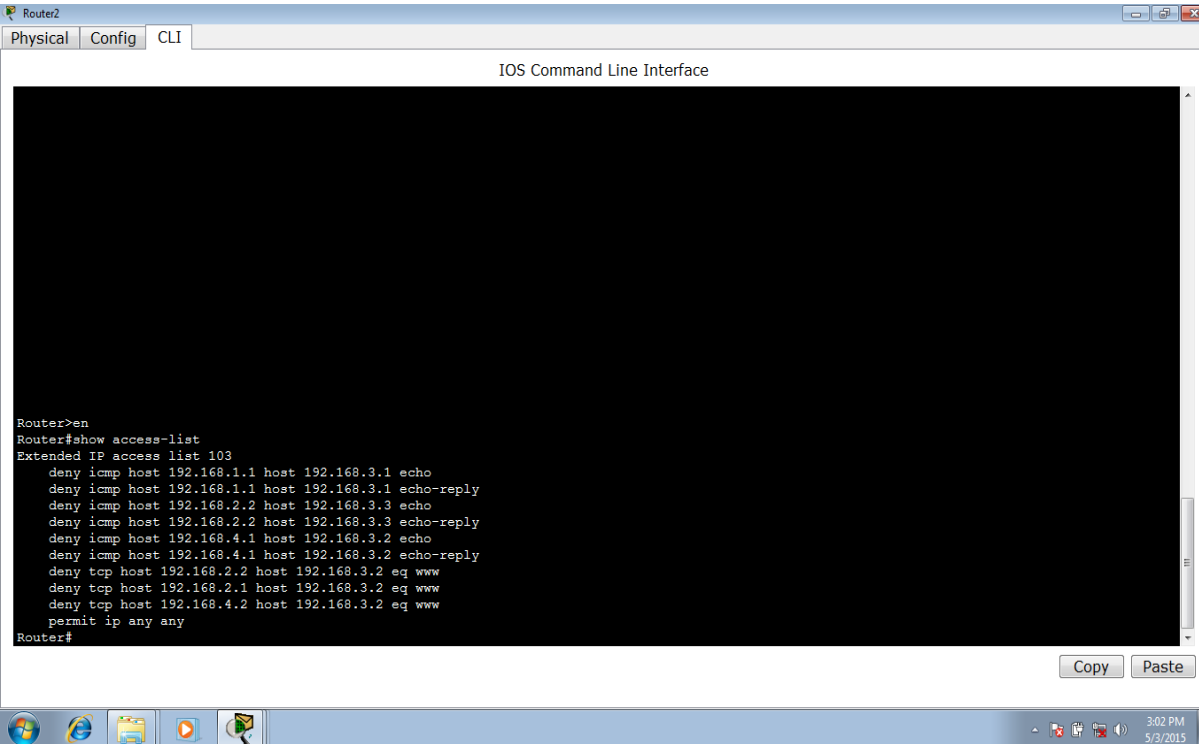
9.4 Access list



The screenshot shows the CLI of Router0. The tabs at the top are Physical, Config, and CLI. The title bar says "IOS Command Line Interface". The command prompt is "Router#". The user has entered the following commands:

```
Router>en
Router#show access
Router#show access-lists
Extended IP access list 105
deny icmp 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.63 echo
deny icmp 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.63 echo-reply
deny icmp 192.168.1.64 0.0.0.31 192.168.1.0 0.0.0.15 echo
deny icmp 192.168.1.64 0.0.0.31 192.168.1.0 0.0.0.15 echo-reply
deny icmp 192.168.1.64 0.0.0.31 192.168.1.32 0.0.0.31 echo
deny icmp 192.168.1.64 0.0.0.31 192.168.1.32 0.0.0.31 echo-reply
deny tcp 192.168.1.128 0.0.0.63 host 10.0.0.4 eq www
permit ip any any
Router#
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons. The taskbar at the bottom shows the Windows Start button, several application icons, and the system clock displaying 2:55 PM on 5/9/2015.

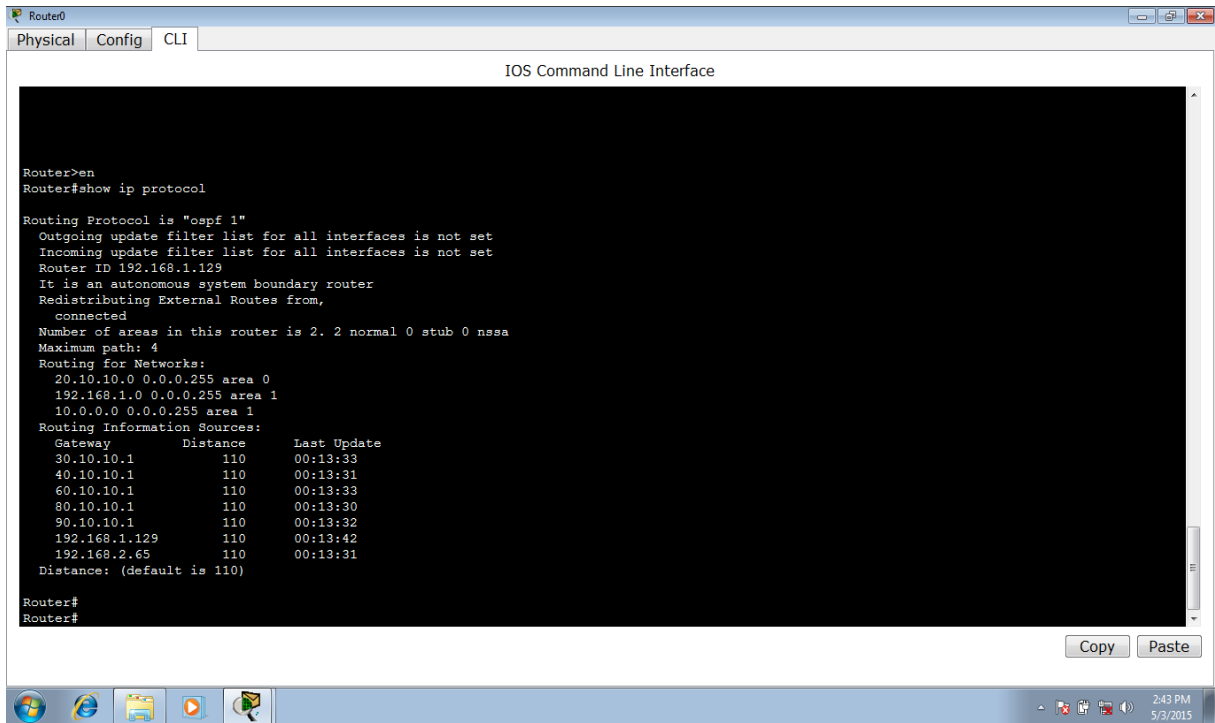


The screenshot shows the CLI of Router2. The tabs at the top are Physical, Config, and CLI. The title bar says "IOS Command Line Interface". The command prompt is "Router#". The user has entered the following commands:

```
Router>en
Router#show access-list
Extended IP access list 103
deny icmp host 192.168.1.1 host 192.168.3.1 echo
deny icmp host 192.168.1.1 host 192.168.3.1 echo-reply
deny icmp host 192.168.2.2 host 192.168.3.3 echo
deny icmp host 192.168.2.2 host 192.168.3.3 echo-reply
deny icmp host 192.168.4.1 host 192.168.3.2 echo
deny icmp host 192.168.4.1 host 192.168.3.2 echo-reply
deny tcp host 192.168.2.2 host 192.168.3.2 eq www
deny tcp host 192.168.2.1 host 192.168.3.2 eq www
deny tcp host 192.168.4.2 host 192.168.3.2 eq www
permit ip any any
Router#
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons. The taskbar at the bottom shows the Windows Start button, several application icons, and the system clock displaying 3:02 PM on 5/9/2015.

9.5 OSPF

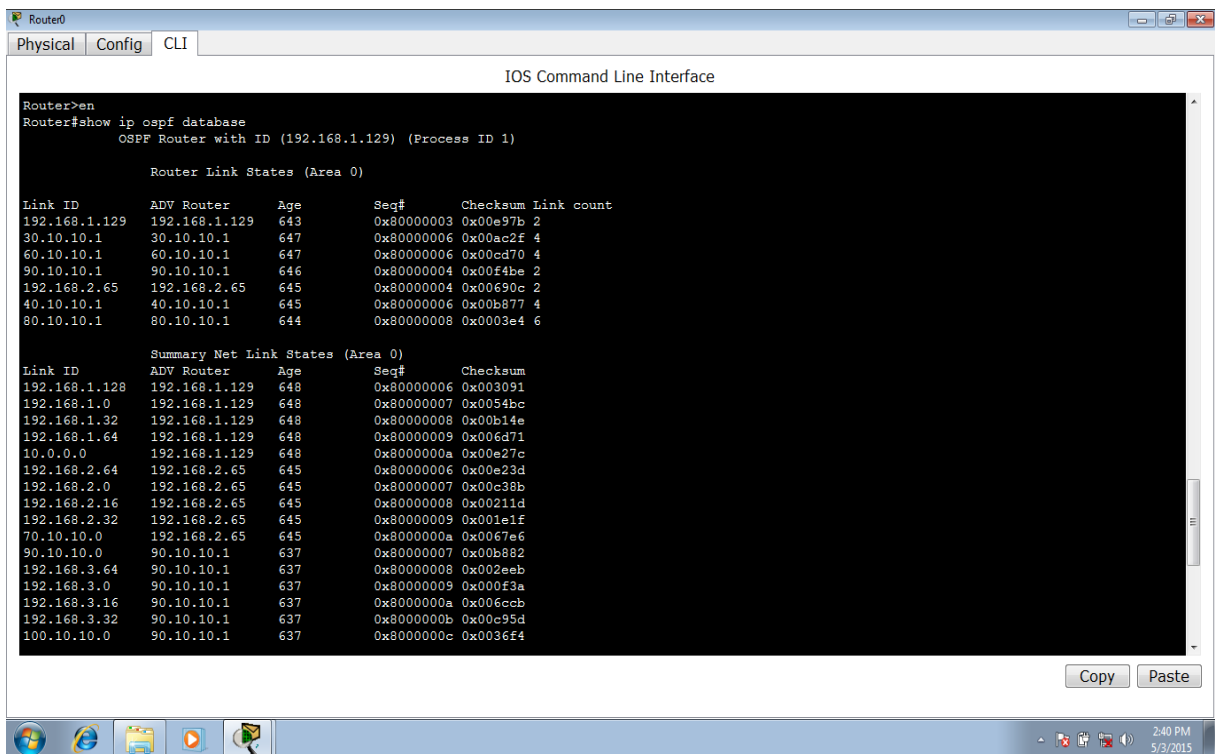


The screenshot shows a Cisco IOS CLI window titled "Router0" with tabs for "Physical", "Config", and "CLI". The main window displays the "IOS Command Line Interface". The user has entered the command "show ip protocol", and the output shows that OSPF is configured as "ospf 1". The output also displays the router ID (192.168.1.129), the number of areas (2), and the maximum path (4). The routing information sources are listed, showing the gateway, distance, and last update for each source.

```
Router>en
Router#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.129
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    20.10.10.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.255 area 1
    10.0.0.0 0.0.0.255 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    30.10.10.1       110          00:13:33
    40.10.10.1       110          00:13:31
    60.10.10.1       110          00:13:33
    80.10.10.1       110          00:13:30
    90.10.10.1       110          00:13:32
    192.168.1.129    110          00:13:42
    192.168.2.65     110          00:13:31
  Distance: (default is 110)

Router#
Router#
```



The screenshot shows a Cisco IOS CLI window titled "Router0" with tabs for "Physical", "Config", and "CLI". The main window displays the "IOS Command Line Interface". The user has entered the command "show ip ospf database", and the output shows the OSPF Router with ID (192.168.1.129) (Process ID 1). The output displays the Router Link States (Area 0) and the Summary Net Link States (Area 0).

```
Router>en
Router#show ip ospf database
  OSPF Router with ID (192.168.1.129) (Process ID 1)

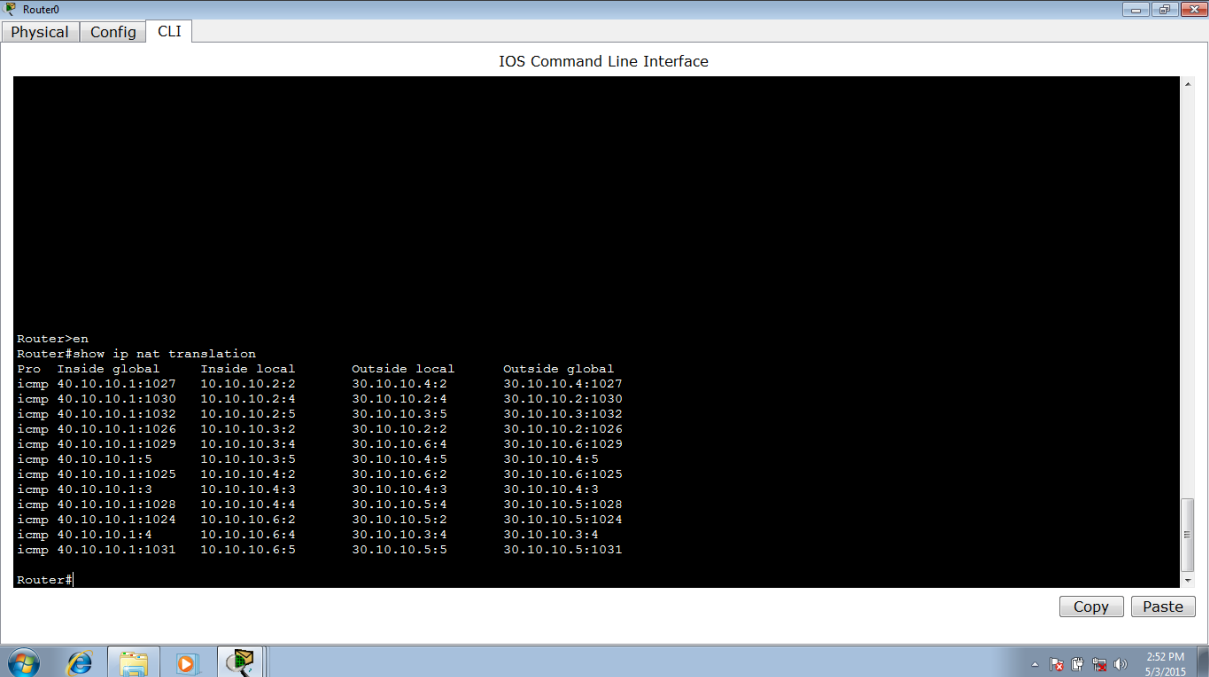
  Router Link States (Area 0)

Link ID        ADV Router    Age         Seq#          Checksum Link count
192.168.1.129  192.168.1.129 643         0x80000003   0x00e97b 2
30.10.10.1     30.10.10.1    647         0x80000006   0x00ac2f 4
60.10.10.1     60.10.10.1    647         0x80000006   0x00cd70 4
90.10.10.1     90.10.10.1    646         0x80000004   0x00f4be 2
192.168.2.65   192.168.2.65  645         0x80000004   0x00690c 2
40.10.10.1     40.10.10.1    645         0x80000006   0x00b877 4
80.10.10.1     80.10.10.1    644         0x80000008   0x0003e4 6

  Summary Net Link States (Area 0)

Link ID        ADV Router    Age         Seq#          Checksum
192.168.1.128  192.168.1.129 648         0x80000006   0x003091
192.168.1.0     192.168.1.129 648         0x80000007   0x0054bc
192.168.1.32    192.168.1.129 648         0x80000008   0x00b14e
192.168.1.64    192.168.1.129 648         0x80000009   0x006d71
10.0.0.0        192.168.1.129 648         0x8000000a   0x00e27c
192.168.2.64    192.168.2.65 645         0x80000006   0x00e23d
192.168.2.0     192.168.2.65 645         0x80000007   0x00c38b
192.168.2.16    192.168.2.65 645         0x80000008   0x00211d
192.168.2.32    192.168.2.65 645         0x80000009   0x001e1f
70.10.10.0      192.168.2.65 645         0x8000000a   0x0067e6
90.10.10.0      90.10.10.1    637         0x80000007   0x00b882
192.168.3.64    90.10.10.1    637         0x80000008   0x002eeb
192.168.3.0     90.10.10.1    637         0x80000009   0x000f3a
192.168.3.16    90.10.10.1    637         0x8000000a   0x006ecb
192.168.3.32    90.10.10.1    637         0x8000000b   0x00c95d
100.10.10.0     90.10.10.1    637         0x8000000c   0x0036f4
```

9.6 PAT



Router0

Physical Config CLI

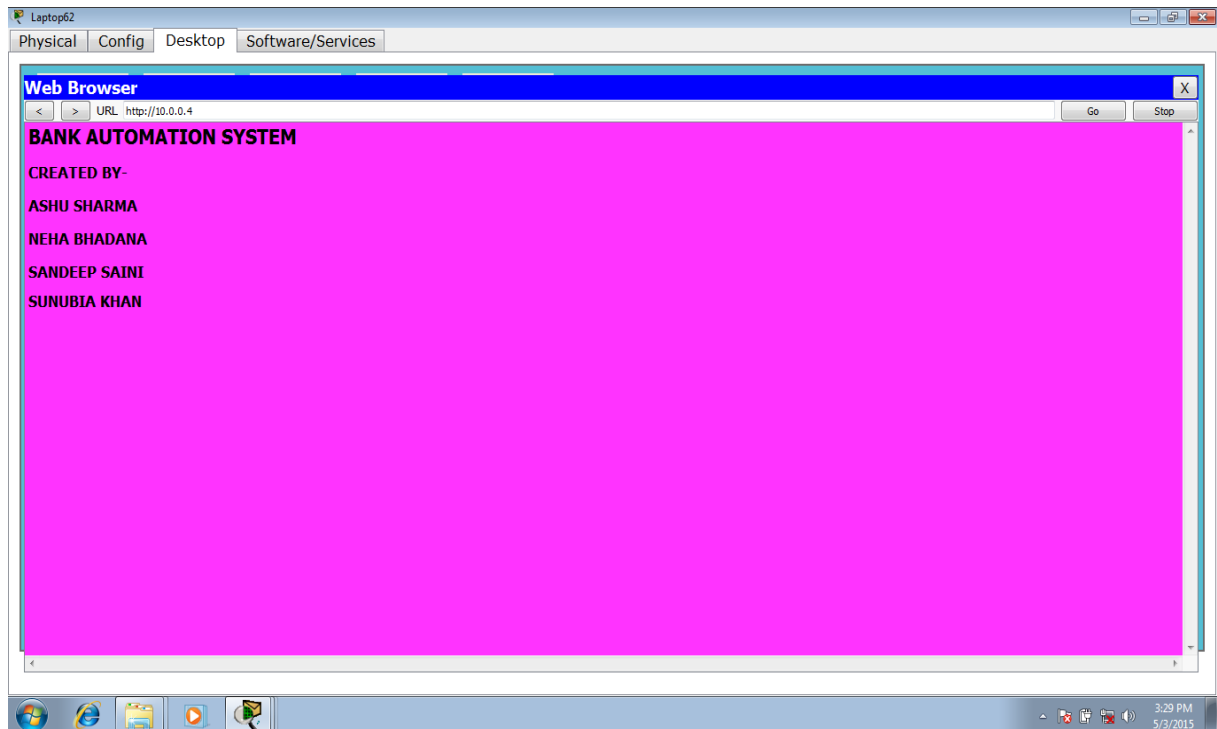
IOS Command Line Interface

```
Router>en
Router#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 40.10.10.1:1027    10.10.10.2:2      30.10.10.4:2      30.10.10.4:1027
icmp 40.10.10.1:1030    10.10.10.2:4      30.10.10.2:4      30.10.10.2:1030
icmp 40.10.10.1:1032    10.10.10.2:5      30.10.10.3:5      30.10.10.3:1032
icmp 40.10.10.1:1026    10.10.10.3:2      30.10.10.2:2      30.10.10.2:1026
icmp 40.10.10.1:1029    10.10.10.3:4      30.10.10.6:4      30.10.10.6:1029
icmp 40.10.10.1:5       10.10.10.3:5      30.10.10.4:5      30.10.10.4:5
icmp 40.10.10.1:1025    10.10.10.4:2      30.10.10.6:2      30.10.10.6:1025
icmp 40.10.10.1:3       10.10.10.4:3      30.10.10.4:3      30.10.10.4:3
icmp 40.10.10.1:1028    10.10.10.4:4      30.10.10.5:4      30.10.10.5:1028
icmp 40.10.10.1:1024    10.10.10.6:2      30.10.10.5:2      30.10.10.5:1024
icmp 40.10.10.1:4       10.10.10.6:4      30.10.10.3:4      30.10.10.3:4
icmp 40.10.10.1:1031    10.10.10.6:5      30.10.10.5:5      30.10.10.5:1031
Router#
```

Copy Paste

2:52 PM 5/3/2015

9.7 Web browsing



CHAPTER 10

REFERENCES

- CCNA study guide seventh edition Todd Laemmle
- CISCO study material www.cisco.com
- www.networks.com
- Midas Logix InfoTech Pvt. Ltd.
- C.S.E Department of Translam Institute of Technology & Management Meerut

LIST OF FIGURES

Figure	Page no.
3.1 Local Area Network	3
3.2 Metropolitan Area Network	4
3.3 Wide Area Network	5
6.1 Real Router	12
6.2 Router in packet tracer	12
6.3 Real Switch	17
6.4 Switch in packet tracer	17
6.5 Lan Cards	19
6.6 Hub	19
6.7 Hub in packet tracer	19
6.8 Modem	20
6.9 Network Repeater	20
6.10 DNS Server in packet tracer	22
6.11 DHCP Server in packet tracer	24
7.1 Configuration example of subnetting	29
7.2 Configuration example of RIP routing	32
7.3 Configuration example of OSPF	36
7.4 Configuration example of NAT	39
7.5 PAT example & configuration	41
7.6 Truncking	44
7.7 VLAN	45
7.8 Configuration example of VLAN	46
7.9 Access control list	49
9.1 Project view	61
9.2 Communication between two pc	62
9.3 DHCP	62
9.4 Access list	63

9.5 OSPF	64
9.6 PAT	65
9.7 Web browsing	65