A

Minor Project Report

On

"Enterprise Network Management System"

Submitted

In partial fulfillment

For the award of the Degree of

Bachelor of Technology

In Department of Information Technology

Submitted To

Mrs.Neha Janu

Reader

Department of Information Technology

Submitted By

Jatin Patni(12ESKIT035)

Hitesh Jaisinghani(12ESKIT032)

Kisan Chaurasiya(12ESKIT039)

V11 Semester, IT

Guided by

Mr. Sunil Dhankar

(Reader)

Department Of Information Technology

Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur

Rajasthan Technical University, Kota

CERTIFICATE

I hereby declare that the work, which is being presented in the Minor Project Report, entitled **"Enterprise Network Management System",** in partial fulfilment for the award of Degree of Bachelor of Technology in Department of Information Technology submitted to the Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, Rajasthan Technical University is a record of my own investigations carried under the Guidance of Mr Sunil Dhankar, Proffesor, Department of Information Technology, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur.

I have not submitted the matter presented in this report elsewhere for the award of any other degree.

Hitesh Jaisinghani(12ESKIT032)

Jatin Patni (12ESKIT035)

Kisan Chaurasiya(12ESKIT039)

B.Tech. (Information Technology)
Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur

Counter Signed by

Mr Sunil Dhankar
Reader

ACKNOWLEDGEMENT

We feel immense pleasure in expressing our regards to the Chairman **Mr. Surja Ram Meel,** Director **Mr. Jaipal Meel,** Registrar **Mrs. Rachana Meel,** Director (Academics) **Prof.** (**Dr.) S. L. Surana,** Principal & Director (D&W) Prof. (Dr.) **Ramesh Pachar** of Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur for providing me necessary facilities during the various stages of this work.

We would like to thank **Dr. Anil Choudhary,** HOD, Department of Information Technology and **Mrs. Neha Janu**, Dept. HOD, Information Technology for providing us an opportunity to work in the right direction and providing their valuable suggestions to improve.

We would like to thank our mentor **Mr. Sunil Dhankar**, Prof., Department of Information Technology, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur for his valuable guidance, keen interest, constant encouragement, incessant inspiration and continuous help throughout this work. His vast experience and realistic approach have been of great help to us.

We would also like to express our gratitude to our parents for their support and blessings. In addition, a very special thanks to all our colleagues and friends for their support in the completion of this work.

Regards,

Hitesh Jaisinghani (12ESKIT032)

Jatin Patni(12ESKIT035)

Kisan Chaurasiya(12ESKIT039)

CONTENTS

Chapter -1

INTRODUCTION

1.1 NETWORKING

A networking is a collection of individual networks, connected by intermediate networking devices such as hubs, switches and routers that functions as a single large network. Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks. All sorts of technologies can actually be employed to move data from one place to another using wires, radio waves and even microwaves.

1.2 TYPES OF NETWORK

There are different types of network such as:

- On the basis of area
- On the basis of connection

1.2.1 On the basis of area

- On the basis of area there are five types of network.
- Local area networks (LANs):- The computers are geographically close together that is in the same building.
- Wide area networks (WANs):- The computers are farther apart and are connected by telephone lines or radio waves.
- Campus area networks (CANs):- The computers are in a limited geographical area, such as campus or military base.
- Metropolitan area network (MANs):- A data network designed for a city or town.

1.2.2 On the basis of connection

On the basis of connection there are two types of network.

- Wired networks
- Wireless networks

Addition to these types the networks can also be distinguished on the basis of different topologies.

1.3 NETWORKTOPOLOGIES

The geometric arrangement of any network is known as its topology. Some of the common topologies are:-

1.3.1 BUS TOPOLOGY

A network in which all the nodes are connected to a single wire which has two end points is known as bus topologies.

1.3.2 STAR TOPOLOGY

A Local area network uses a star topology in which all nodes are connected to a central computer. The main advantage of star topology is that one malfunctioning node doesn't affect the whole network and it's easy to remove nodes. The main disadvantage is that they require more cables.

1.3.3 RING TOPOLOGY

In ring topology, all the nodes are connected in a closed loop. Message travel around the ring, with each reading those messages address to it. One of the advantages of ring topology is that they can span a larger area.

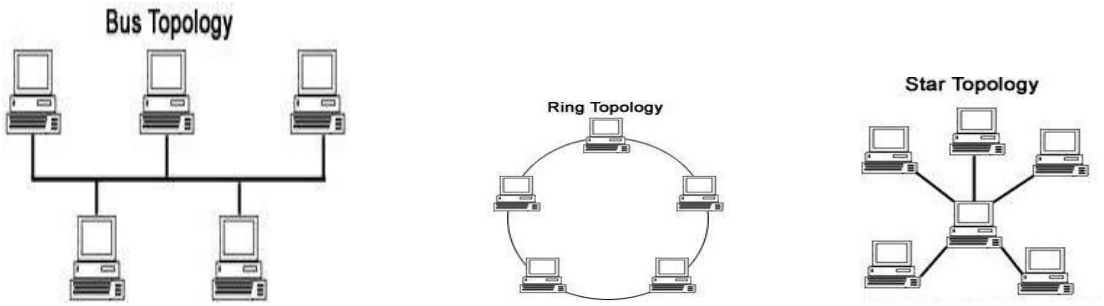


Fig. 1.1: Network Topologies

Chapter - 2

OSI AND TCP/IP REFERENCE MODEL

2.1 INTRODUCTION

The OSI (Open system interconnection) model provides a framework for creating and implementing networking standards, devices and internetworking schemes. Open System Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in1984, and it is now considered the primary architectural model for inter computer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

2.2 LAYERS OF OSI MODEL

The following list details these even layers of the Open System Interconnection (OSI):-

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer

- Physical layer

These layers are divided into two groups. The top three layers define how the application within the end stations will communicate with each other and with users. The bottom four layers define how data is transmitted end–to–end.

2.2.1 APPLICATION LAYER

It is the top most layer of OSI model. The application layer of the OSI model marks the spot where user actually communicates to the computer. This layer comes into play when it's apparent that access to the network is going to be needed. It provides a user interface.

2.2.2 PRESENTATION LAYER

The presentation layer gets its name from its purpose. It presents data to the application layer and is responsible for data transportation and code formatting. This layer is essentially a translator and provides coding and conversion functions. It handles functions such as encryption.

2.2.3 SESSION LAYER

The session layer establishes, manages, and terminates communication sessions. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocol implemented at the session layer.

2.2.4 TRANSPORT LAYER

The transport layer accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer. Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process.

2.2.5 NETWORK LAYER

The network layer defines the network address, which differs from the MAC address. Some network layer implementations, such as the Internet Protocol (IP), define network addresses in a way that route selection can be determined systematically by comparing the source network address with the destination network address and applying the subnet mask. Because this layer defines the logical network layout, routers can use this layer to determine how to forward packets. Because of this, much of the design and configuration work for internetworks happens at Layer 3, the network layer.

2.2.6 DATA LINK LAYER

The data link layer provides the physical transmission of the data and handles error notification, network topology and flow control. This means that data link layer will ensure that messages are delivered to the proper device on LAN using hardware address and translate messages from the network layer into bits for the physical layer to transmit.

The data link layer formats the message into pieces each called a data frame and adds a customized header containing the hardware destination and source address.

2.2.7 PHYSICAL LAYER

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors.

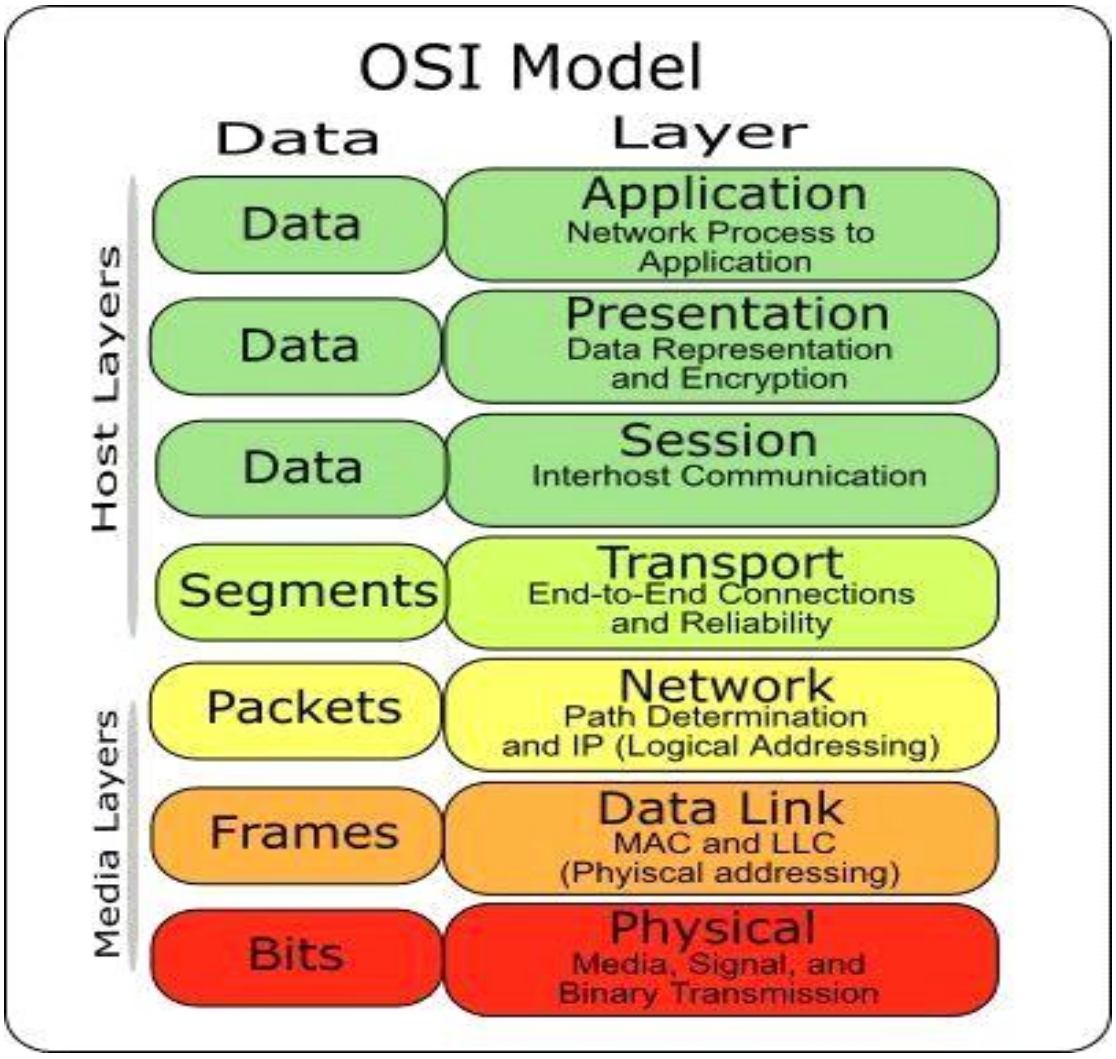


Fig. 2.1 OSI/TCP-IP Reference Model

Chapter - 3

NETWORK PROTOCOLS

The different internet protocols are as follows:

3.1 TELNET

Telnet is the chameleon of protocols- its specialty is terminal emulation. It allows a user on a remote client machine, called the Telnet Client, to access the resources of another machine, the Telnet Server. Telnet achieves this by pulling a fast one on the Telnet Server and making the client machine appears as though it were a terminal directly attached to a local network.

3.2 FILE TRANSFER PROTOCOL (FTP)

File Transfer Protocol (FTP) is the protocol that actually lets us transfer files and it can accomplish this between any two machines using it. As a program, it's employed by users to perform file tasks by hand. FTP teams up with Telnet to transparently log you into theFTP server and then provides for the transfer of files.

3.3 TRIVIAL FILE TRANSFER PROTOCOL (TFTP)

Trivial File Transfer Protocol (TFTP) is the stripped down stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it, plus it's so easy to use and it's fast too. TFTP has no directory-browsing abilities; it can do nothing but send and receive files.

3.4 NETWORK FILE SYSTEM (NFS)

Network file system is a jewel of a protocol specializing in file sharing. It allows two different file Systems to incorporate.

3.5 SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

SMTP answering our ubiquitous call to e-mail, uses a spooled, or queued method of mail delivery. Once a message has been sent to a destination, the message is spooled to a device-usually a disk. SMTP is used to send mails; POP3 is used to receive mails.

3.6 X WINDOWS

Designed for client-server operation, X-Windows defines for a protocol for writing client/server applications based on a graphical user interface. The idea is to allow a program, called a client to run on one computer and have it display thing through a window server on another computer.

3.7 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple network management protocol collects and manipulates this valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals; SNMP receives something called a baseline.

3.8 DOMAIN NAME SERVER(DNS)

DNS is used to resolve a fully qualified domain name. DNS allows you to use a domain name to specify an address. You can change an IP address as often as you want, and no one will know the difference.

3.9 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dynamic host configuration gives ip address to hosts. It allows easier administration and works well in small-to-even-very-large network environment.

Chapter – 4

DEVICES AND TERMINOLOGIES

4.1 DEVICES

There are many devices used in networking such as listed below:-

4.1.1 SERVER

A computer system used primarily to provide one or more network services, or a hardware or software product developed for such usage Role.

Fig 4.1 Server

4.1.2 SWITCHES

In network, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched.

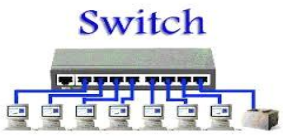


Fig. 4.2 Switch

4.1.3 HUBS

Common connection points for devices in a network, Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. 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.

Fig. 4.3 Hub

4.1.4 ROUTERS

A device that forwards data packets along networks; 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. 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.

(a) (b)

Fig. 4.4 Router

4.1.5 ETHERNET

If we plan to connect only two computers, all we'll need is a network interface card (NIC) in each computer and a cable to run between them. If you want to connect several computers or other devices, you'll need an additional piece of equipment: an Ethernet router. You'll also need a cable to connect each computer or device to the router.

The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.

A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second.

Fig.4.5 Ethernet

4.2 NETWORK TERMINOLOGIES

4.2.1 MEDIA ACCESS CONTROL (MAC)

The addresses consist of a subset of data link layer addresses. MAC addresses identify network entities in LANs that implement the IEEE MAC addresses of the data link layer. As with most data-link addresses, MAC addresses are unique for each LAN interface. MAC addresses are 48 bits in length and are expressed as 12 hexadecimal digits. The first 6

hexadecimal digits, which are administered by the IEEE, identify the manufacturer or vendor and thus comprise the Organizationally Unique Identifier (OUI). The last 6 hexadecimal digits comprise the interface number, or another value administered by the specific vendor. MAC addresses sometimes are called burned-in addresses (BIAs) because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the interface card initializes.

4.2.2 IP ADDRESS

As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagram through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnet works, each host on a TCP/IP network is assigned a unique 32bit logical address that is divided into two main parts: the network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (Inter NIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the Inter NIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.

4.2.2.1 IPV4

Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet. IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model; in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol. IPv4 uses 32-bit (fourbyte) addresses, which limits the address space to4294967296 (2^{32}) addresses. As addresses were assigned to users, the number of unassigned addresses decreased

4.2.2.2 IP Address Format

The 32-bit IP address is grouped eight bits at a time, separated by dots, and represented in decimal format (known as dotted decimal notation). Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, and 1). The minimum value for an octet is 0, and the maximum value for an octet is 255.Figure 30-3 illustrates the basic format of an IP address.

4.2.2.3 IP Address Classes

IP addressing supports five different address classes: A, B, C, D, and E. only classes A, B, and C are available for commercial use. The left-most (high-order) bits indicate the network class. The class of address can be determined easily by examining the first octet of the address and mapping that value to a class range in the following table. In an IP address of 172.31.1.2, for example, the first octet is 172. Because 172 fall between 128 and 191, 172.31.1.2 is a Class Baddress.

4.2.2.4 IP Subnet Addressing

IP networks can be divided into smaller networks called sub networks (or subnets). Subnetting provides the network administrator with several benefits, including extra flexibility, more efficient use of network addresses, and the capability to contain broadcast traffic (a broadcast will not cross router).Subnets are under local administration. As such, the outside world sees an organization as a single network and has no detailed knowledge of the organization's internal structure. A given network address can be broken up into many sub networks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0 are all subnets within network 171.16.0.0. (All 0s in the host portion of an address specifies the entire network.)

4.2.2.5 IP Subnet Mask

A subnet address is created by ―borrowing‖ bits from the host field and designating them as the subnet field. The number of borrowed bits varies and is specified by the subnet mask. The default subnet mask for a Class B address that has no subletting is 255.255.0.0, while the subnet mask for a Class B address 171.16.0.0 that specifies eight bits of subletting is

255.255.255.0. The reason for this is that eight bits of subletting or 28 – 2 (1 for the network address and 1 for the broadcast address) = 254 subnets possible, with 28 – 2 = 254 hosts per subnet. The subnet mask for a Class C address 192.168.2.0 that specifies five bits of subletting is255.255.255.248.With five bits available for sub netting, 25 – 2 = 30 subnets possible, with 23 – 2 = 6 hosts per subnet. The reference charts shown in table 30–2 and table 30–3 can be used when planning Class B and Cnetworks to determine the required number of subnets and hosts, and the appropriate subnet mask.

4.2.3 ETHERCHANNEL

It is a port link aggregation technology or port-channel architecture used primarily on Ciscoswitches. It allows grouping of several physical Ethernetlinks to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers. An Ether Channel can be created from between two and eight active Fast, Gigabit or 10-Gigabit Ethernet ports, with an additional one to eight inactive (failover) ports which become active as the other active ports fail. Ether Channel is primarily used in the backbone network, but can also be used to connect end user machines.

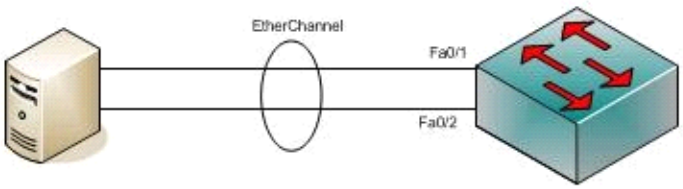


Fig. 4.6 Ether channel

4.2.4 PINGING

Ping is a basic internet program that allows a user to verify that a particular IP address exits and can accept requests. Ping can be used for troubleshooting to test connectivity and determine response time.

4.2.5 TRUNKING

Trunking is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually.

4.2.6 FRAME RELAY

Frame Relay is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame Relay originally was designed for use across Integrated Services Digital Network (ISDN) interfaces. Today, it is used over a variety of other network interfaces as well. This chapter focuses on Frame Relay's specifications and applications in the context of WAN services. Frame Relay is an example of a packetswitched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. The following two techniques are used in packet-switching technology Variable-length packets. Statistical multiplexing Variablelength packets are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached. Statistical multiplexing techniques control network access in a packet-switched network. The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today's popular LANs, such as Ethernet and Token Ring, are packet-switched are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached. Statistical multiplexing techniques control network access in a packet-switched network. The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today's popular LANs, such as Ethernet and Token Ring, are packet-switched networks.

4.2.6.1 Switched virtual circuits (SVCs)

They are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A communication session across an SVC consists of the following four operational states:-

Call setup- The virtual circuit between two Frame Relay DTE devices is established.

Data transfer —Data is transmitted between the DTE devices over the virtual circuit.

Idle—the connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.

Call termination—the virtual circuit between DTE devices is terminated. After the virtual circuit is terminated, the DTE devices must establish a new SVC if there is additional data to be exchanged. It is expected that SVCs will be established, maintained, and terminated using the same signaling protocols used in ISDN.Few manufacturers of Frame Relay DCE equipment support switched virtual circuit connections. Therefore, their actual deployment is minimal in today's Frame Relay networks. Previously not widely supported by Frame Relay equipment, SVCs are now the norm. Companies have found that SVCssave money in the end because the circuit is not open all the time.

4.2.6.2 Permanent virtual circuits (PVCs)

They are permanently established connections that are used for frequent and consistent data transfers between DTE devices across the Frame Relay network. Communication across PVC does not require the call setup and termination states that are used with SVCs.

PVCs always operate in one of the following two operational states:

Data transfer —Data is transmitted between the DTE devices over the virtual circuit.

Idle —the connection between DTE devices is active, but no data is transferred. Unlike SVCs, PVCswill not be terminated under any circumstances when in an idle state.DTE devices can begin transferring data whenever they are ready because the circuit is permanently established.

4.2.6.3 Frame Relay Network Implementation

A common private Frame Relay network implementation is to equip a T1 multiplexer with both FrameRelay and non-Frame Relay interfaces. Frame Relay traffic is forwarded out the Frame and onto the data network. Non-Frame Relay traffic is forwarded to the appropriate application or service,such as a private branch exchange (PBX) for telephone service or to a video-teleconferencing application.

4.2.7 FRAMES

A frame is composed of the data link layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the data link layer -

entity in the destination system. Data from upper-layer entities is encapsulated in the data link layer header and trailer.

4.2.8 PACKET

It is an information unit whose source and destination are network layer entities. A packet is composed of the network layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the network layer entity in the destination system. Data from upper-layer entities is encapsulated in the network layer header and trailer.

Chapter - 5

ROUTERS AND ROUTING

5.1 DEFINITION

A device that forwards data packets along networks; 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. 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.

5.2 TYPES OF ROUTING

- Static routing
- Dynamic routing
- OSPF routing
- IGRP/EIGRP routing
- Routing information protocol (RIP)
- Default routing

5.2.1 STATIC ROUTING

Static routing is a concept describing one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network. This is achieved by manually adding routes to the routing table. The opposite of static routing is dynamic routing, sometimes also referred to as adaptive routing.

In these systems, router (config)# ip route 10.10.20.0 255.255.255.0 192.168.100.1

5.2.2 DYNAMIC ROUTING

Dynamic Routing describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change. People using a transport system can display dynamic routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination. Another example of adaptive routing can be seen within financial markets. For example, ASOR or Adaptive Smart Order Router (developed by Quod Financial), takes routing decisions dynamically and based on real-time market events. The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available.

5.2.2.1 ROUTING INTERNET PROTOCOL (RIP)

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable.RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the Routing Information Protocol with Metric-Based Topology (RMTI) algorithm to cope with the count-to-infinity problem. With RMTI, it is possible to detect every possible loop with a very small computation effort. Originally, each RIP router transmitted full updates every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. It was thought, as a result of random initialization, the routing updates would

spread out in time, but this was not true in practice. Sally Floyd and Van Jacobson showed in 1994 that, without slight randomization of the update timer, the timers synchronized over time. In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS (the latter two being link-state routing protocols), and (without RMTI) a hop limit severely limits the size of network it can be used in. However, it is easy to configure, because RIP does not require any parameters on a router unlike other. RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

In these systems, lab A (config)# router rip: Lab A(config-router)#network 192.168.10.0

5.2.2.2 OPEN SHORTEST PATH FIRST (OSPF)

Open Shortest Path First (OSPF) is a link-state routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4.The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks.

5.2.2.3 INTERIOR GATEWAY ROUTING PROTOCOL

Another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

In these systems,

Lab_A #config t

Lab_A (config)#router igrp 10

Lab_A (config-router)# network 192.168.10.0

5.2.2.4 ENHANCED INTERIOR GATEWAY (EIGRP) ROUTING

Enhanced Interior Gateway Routing Protocol (EIGRP) is a distance-vector routing protocol designed by Cisco Systems. It is an enhanced version of Cisco's earlier Interior Gateway Routing Protocol (IGRP). In March 2013, Cisco claimed that EIGRP would be made an open standard. EIGRP differs from many other distance-vector routing protocols by providing incremental routing updates and backwards compatibility with Cisco's IGRP. It is optimized to reduce routing instability (this often occurs after topology changes), the amount of bandwidth consumed by routing updates and the processing power used by the router. Most of the routing optimizations are based on the Diffusing Update Algorithm (DUAL) work from SRI, which guarantees loop-free operation and provides mechanisms for fast convergence. Dynamic routes using internal EIGRP have a default administrative distance of 90 and external EIGRP routes have a default administrative distance of 170.

5.3 DEFAULT ROUTING

A default route of a computer that is participating in computer networking is the packet forwarding rule (route) taking effect when no other route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default route. This route generally points to another router, which treats the packet the same way: If a route matches, the packet is forwarded accordingly; otherwise the packet is forwarded to the default route of that router. The process repeats until a packet is delivered to the destination. Each router traversal counts as one hop in the distance calculation for the transmission path. The route evaluation process in each router uses the longest prefix match method to obtain the most specific route. The network with the longest subnet mask that matches the destination IP address is the next-hop network gateway. The default route in Internet Protocol Version 4 (IPv4) is designated as the zero-address 0.0.0.0/0 in CIDR notation, often called the quad-zero route. The subnet mask is given as /0, which effectively specifies all networks, and is the shortest match possible. A route lookup that does not match any other route, falls back to this route,similarly, in IPv6, the default route is specified by: /0.

In the highest-level segment of a network, administrators generally point the default route for a given host towards the router that has a connection to a network service provider. Therefore, packets with destinations outside the organization's local area network, typically destinations on the Internet or a wide area network, are forwarded to the router with the connection to that provider. The device to which the default route points is often called the default gateway, and it often carries out other functions such as packet filtering, firewalling, or proxy server operations.

In these systems, router (config)#ip route 0.0.0.0.0.0.0.0

Chapter - 6

NETWORK SWITCHES AND SWITCHING

6.1 DEFINITION

In networks, a device that filters and forwards packets between LAN segments, Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

6.2 TYPES OF SWITCHING

There are two types of switching

- Packet switching
- Circuit switching

6.2.1 PACKET SWITCHING

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud. Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS), and X.25The virtual connections between customer sites are often referred to as a virtual circuit Information Formats. The data and control information that is transmitted through internetworks takes a variety of forms. The terms

used to refer to these information formats are not used consistently in the internetworking industry but sometimes are used interchangeably. Common information formats include frames, packets, datagram, segments, and message, cells, and data units.

6.2.2 CIRCUIT SWITCHING

Switched circuit sallow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit. When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated. A frame is an information unit whose source and destination are data link layer entities.

Chapter - 7

VIRTUAL LANs (VLANs)

7.1 INTRODUCTION

A VLAN is a logical grouping of network users and resources connected to administratively define ports on a switch. By default no host in a specific VLAN can communicate with hosts of another VLAN. We need a router. Router allows broadcast only within the originating network, but switches forwards to all segments. The reason is called flat networking.

7.2 VLAN TRUNKING PROTOCOL

The basic goal of VLAN trunking protocol is to manage all configured VLANs across a switched internetwork and to maintain consistency throughout the network. VTP allows an administration to add, delete and rename VLAN information that is then propagated to all other switches in the VTP domain.

7.3 VTP MODES OF OPERATION

There are three different modes of operation:

7.3.1 SERVER

You need at least one server in your VTP domain to propagate VLAN information in whole domain. The switch must be in server mode to able to create, add. Delete VLAN in a VTP domain.

7.3.2 CLIENT

In client mode switches receives information from VTP servers, and they also send and receive updates.

7.3.3 TRANSPARENT

Switches in transparent mode don't participate in VTP domain, but they will still forward VTP adds though any configured trunk links.

7.4 TYPES OF VLAN

Types of VLAN are as follow.

7.4.1 STATIC VLAN

These are most secured VLANs. The switch ports that you assign a VLAN association to always maintain that association until an administrator manually changes port assignment .this type of VLAN is easy to set up and monitor.

7.4.2 DYNAMIC VLAN

It determines a node's VLAN assignment automatically. Using intelligent management software, you can base VLAN assignment on hardware (MAC) address, protocols and even application to create dynamic VLAN.

7.5ADVANTAGES OF VLAN

- Network ads and changes are achieved by configuring a port into appropriate VLAN.
- A group of users needing high security can be put into a VLAN so that no user outside of VLAN can communicate with them.
- VLAN can enhance network security.
- VLAN increases the no. of broadcast domain.

Chapter- 8

WIRED AND WIRELESS NETWORKS

8.1WIRED NETWORKS

There are three basic systems people use to set up wired networks. An Ethernet system uses either a twisted copper-pair or coaxial-based transport system. The most commonly used cable for Ethernet is a category 5 unshielded twisted pair (UTP) cable -- it's useful for businesses who want to connect several devices together, such as computers and printers, but it's bulky and expensive, making it less practical for home use. A phone line, on the other hand, simply uses existing phone wiring found in most homes, and can provide fast services such as DSL. Finally, broadband systems provide cable Internet and use the same type of coaxial cable that gives us cable television.

8.1.1WORKING

If you plan to connect only two computers, all you'll need is a network interface card (NIC) in each computer and a cable to run between them. If you want to connect several computers or other devices, you'll need an additional piece of equipment: an Ethernet router. You'll also need a cable to connect each computer or device to the router. Once you have all of your equipment, all you need to do is install it and configure your computers so they can talk to one another. Exactly what you need to do depends on the type of network and your existing hardware. For example, if your computers came with network cards already installed, all you'll need to do is buy a router and cables and configure your computers to use them. Regardless of which type you select, the routers, adapters and other hardware you buy should come with complete setup instructions.

The steps you'll need to take to configure your computers will also vary based on your hardware and your operating system. User manuals usually provide the necessary information, and Web sites dedicated to specific operating systems often have helpful tips on getting several different computers to talk to each other. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers.

Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.

A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1gigabit (1,000 megabits) per second.

8.2 WIRELESS NETWORKS

A wireless network or Wireless Local Area Network (WLAN) serves the same purpose as a wired one to link a group of computers. Because "wireless" doesn't require costly wiring, the main benefit is that it's generally easier, faster and cheaper to set up.

By comparison, creating a network by pulling wires throughout the walls and ceilings of an office can be labor-intensive and thus expensive. But even when you have a wired network already in place, a wireless network can be a cost-effective way to expand or augment it. In fact, there's really no such thing as a purely wireless network, because most link back to a wired network at some point.

8.2.1 WORKING

The Basics Wireless networks operate using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space.

The cornerstone of a wireless network is a device known as an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. Since wireless networks are usually connected to wired ones, an access point also often serves as a link to the resources available on the a wired network, such as an Internet connection. In order to connect to an access point and join a wireless network, computers must be equipped with wireless network adapters. These are often built right into the computer, but if not, just about any computer or notebook can be made wirelesscapable through the use of an add-on adapter plugged into an empty expansion slot, USB port, or in

the case of notebooks, a PC Card slot. Ethernet and wireless networks each have advantages and disadvantages; depending on your needs, one may serve you better than the other. Wired networks provide users with plenty of security and the ability to move lots of data very quickly. Wired networks are typically faster than wireless networks, and they can be very affordable. However, the cost of Ethernet cable can add up -- the more computers on your network and the farther apart they are, the more expensive your network will be. In addition, unless you're building a new house and installing Ethernet cable in the walls, you'll be able to see the cables running from place to place around your home, and wires can greatly limit your mobility. A laptop owner, for example, won't be able to move around easily if his computer is tethered to the wall.

8.3 IPV6

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

IPv6 is intended to replace IPv4, which still carries more than 96% of Internet traffic worldwide as of May 2014.IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. Device mobility, security, and configuration aspects have been considered in the design of the protocol.

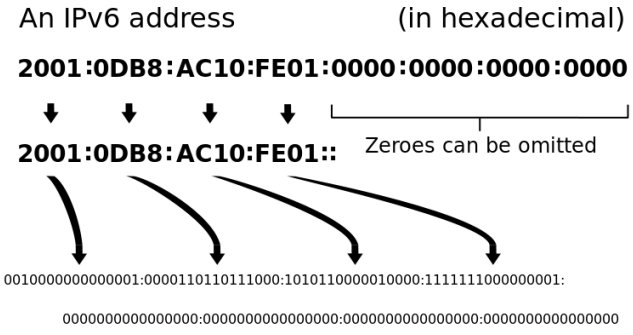


Fig. 8.1 IPV6

8.4 Introduction to Packet Tracer

What is Packet Tracer?

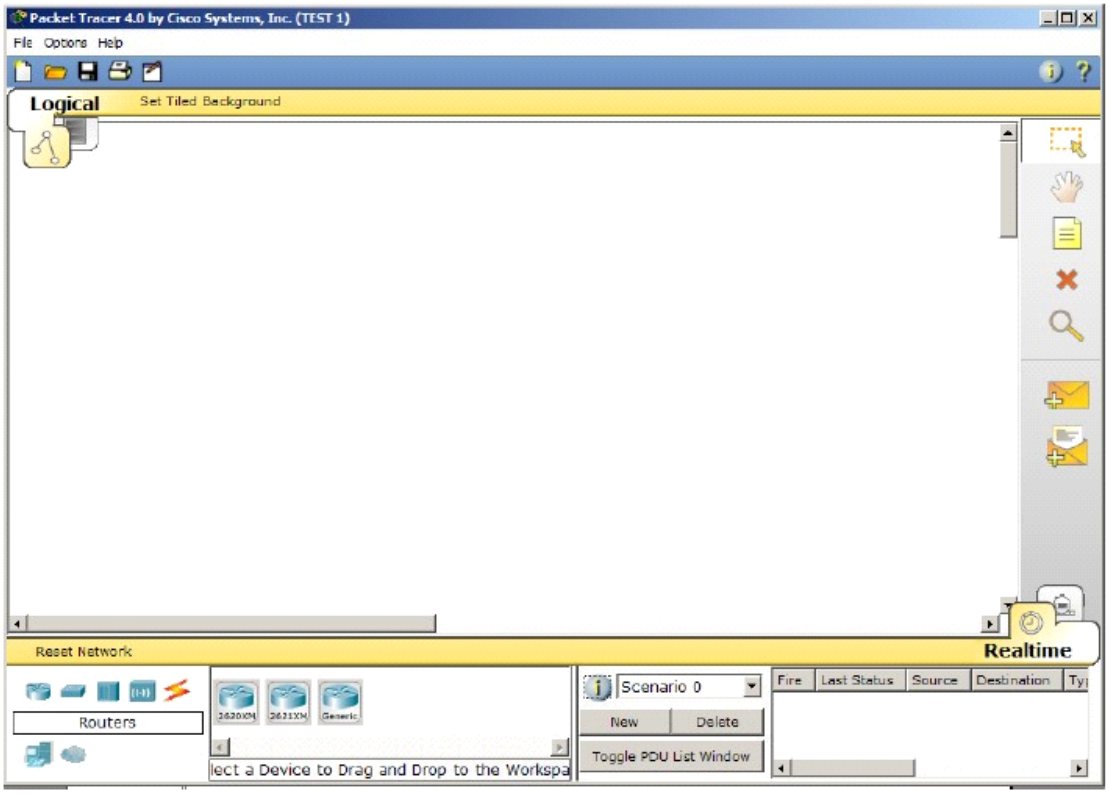
Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer

3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.

Purpose: The purpose of this lab is to become familiar with the Packet Tracer interface. Learn how to use existing topologies and build your own.

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 6.4 Student.



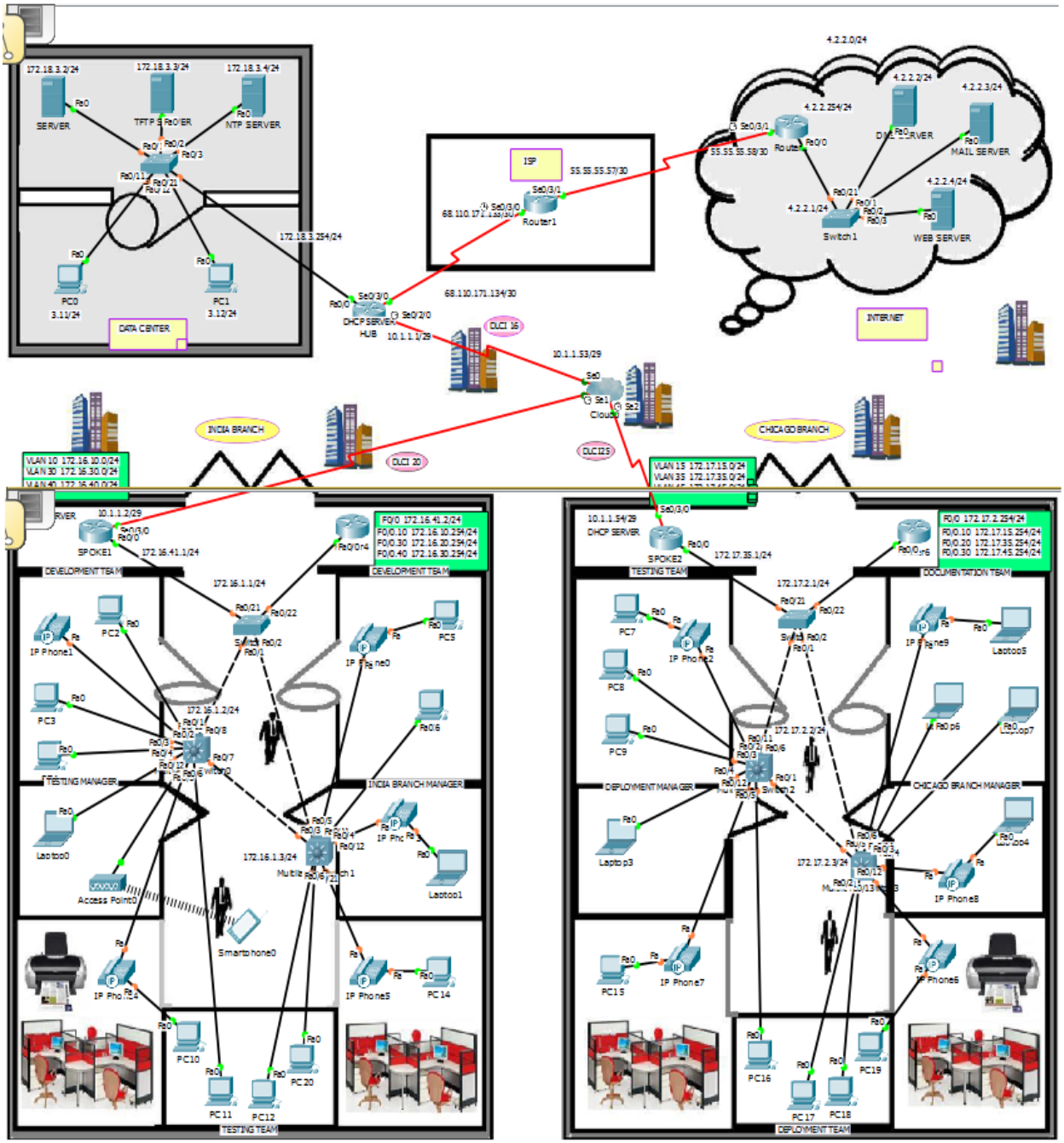
Step 2: Choosing Devices and Connections

We will begin building our network topology by selecting devices and the media in which to connect them.

Several types of devices and network connections can be used. For this lab we will keep it simple by using End Devices, Switches, Hubs, and Connections. Single click on each group of devices and connections to display the various choices.

PROJECT SCENARIO

- **Enterprise Network Management System is the practical implementation of the connectivity between the 2 branches of a company with its DATA centre , connected to ISP using the Simulator Cisco Packet Tracer.**



Configuration on Routers:

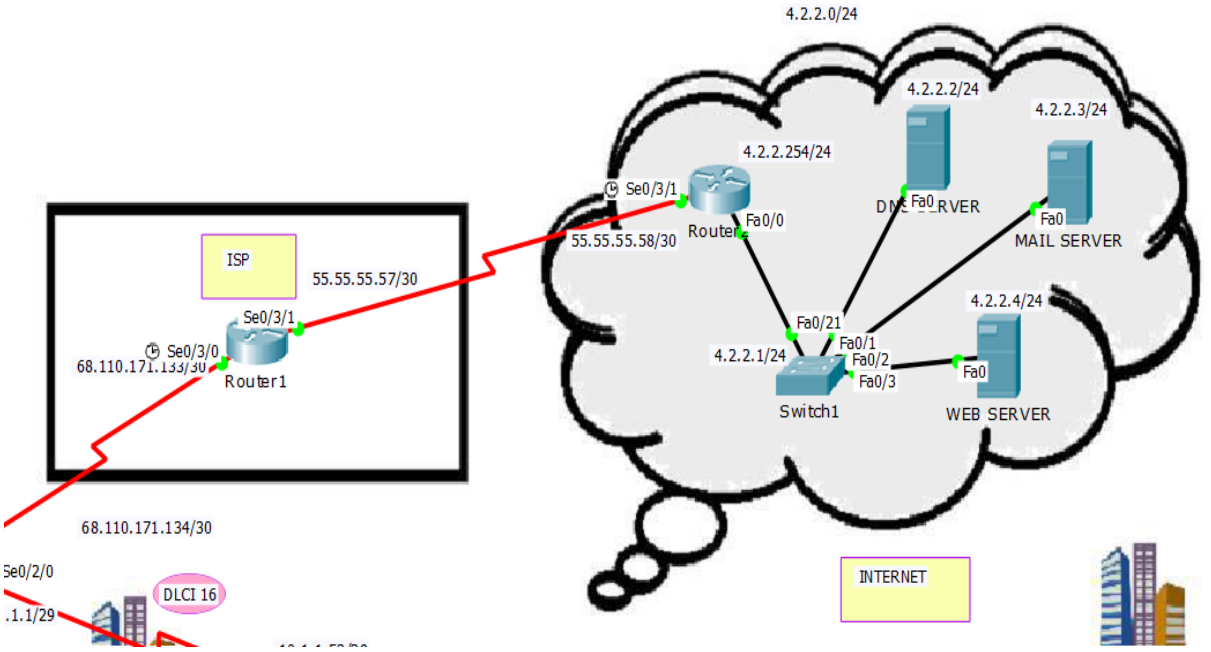
The screenshot shows the configurations on the routers of the company.

```
interface FastEthernet0/0
 ip address 172.16.41.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/3/0
 no ip address
 encapsulation frame-relay
!
interface Serial0/3/0.1 point-to-point
 ip address 10.1.1.2 255.255.255.248
 frame-relay interface-dlci 20
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.7 area 0
 network 172.16.30.0 0.0.0.255 area 0
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.41.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
```

Configuration of DHCP pool.

```
Current configuration : 2041 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
ip dhcp excluded-address 172.16.10.1 172.16.10.100
ip dhcp excluded-address 172.16.10.240 172.16.10.254
ip dhcp excluded-address 172.16.30.1 172.16.10.100
ip dhcp excluded-address 172.16.30.240 172.16.10.254
ip dhcp excluded-address 172.16.40.1 172.16.40.100
ip dhcp excluded-address 172.16.40.240 172.16.40.254
ip dhcp excluded-address 172.16.1.1 172.16.1.100
ip dhcp excluded-address 172.16.1.240 172.16.1.254
!
ip dhcp pool FORVLAN30
 network 172.16.30.0 255.255.255.0
 default-router 172.16.30.254
 dns-server 4.2.2.2
ip dhcp pool FORVLAN40
 network 172.16.40.0 255.255.255.0
 default-router 172.16.40.254
 dns-server 4.2.2.2
ip dhcp pool FORVLAN_VOICE
 network 172.16.10.0 255.255.255.0
 default-router 172.16.10.254
 option 150 ip 172.16.10.254
!
!
```

Topology at ISP(internet service provider)



Configuration at ISP

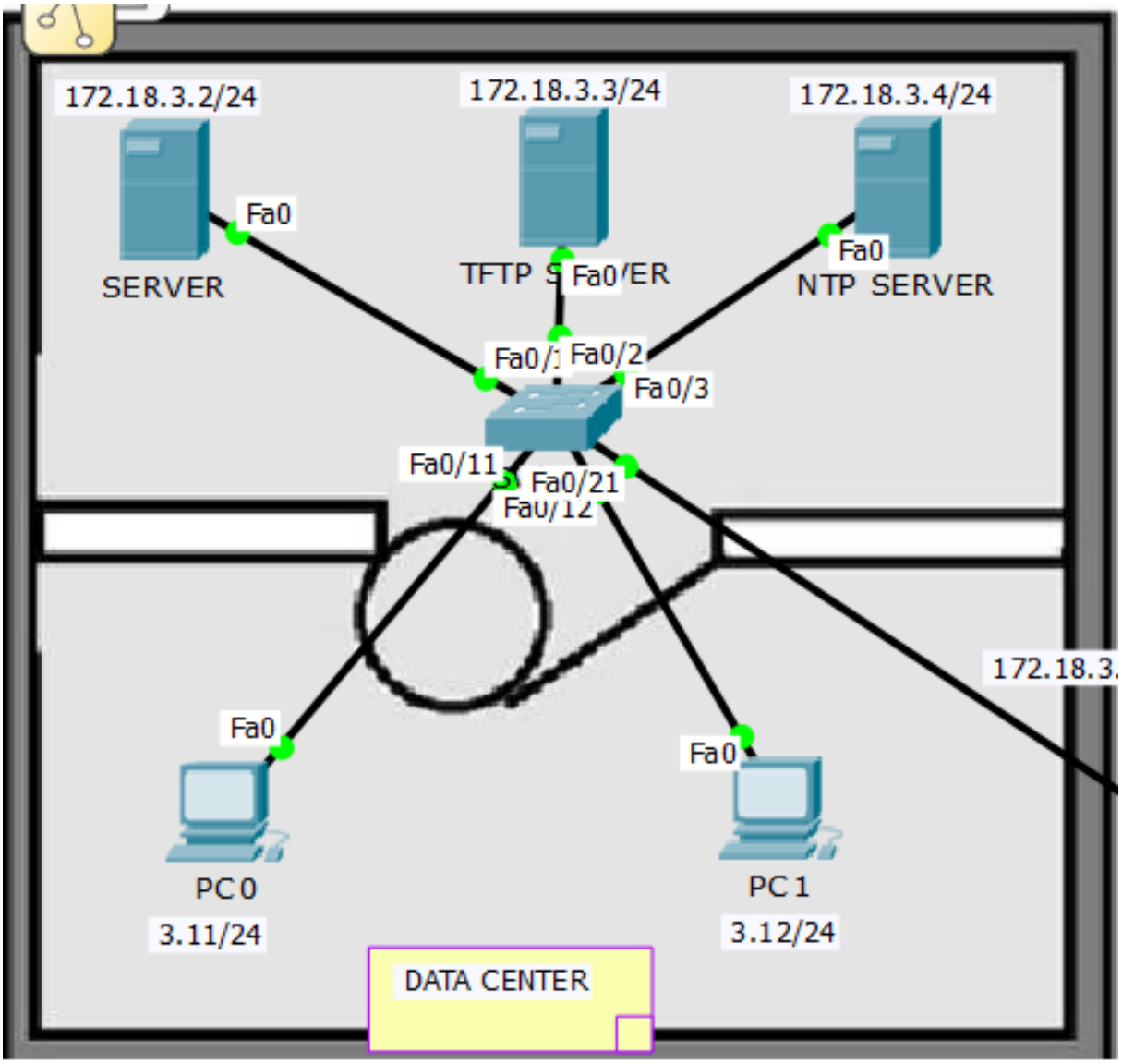
```
Router1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES unset  administratively down down

FastEthernet1/0        unassigned      YES unset  administratively down down

Serial2/0              196.0.0.17      YES manual up                    up

Serial3/0              196.0.0.2       YES manual up                    up

FastEthernet4/0        unassigned      YES unset  administratively down down

FastEthernet5/0        unassigned      YES unset  administratively down down

Serial6/0              unassigned      YES unset  administratively down down

Serial7/0              unassigned      YES unset  administratively down down
Router1#
```

Route Information at ISP

```
ISP_Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.0.0.0/32 is subnetted, 20 subnets
S       192.0.0.1 [1/0] via 196.0.0.2
S       192.0.0.2 [1/0] via 196.0.0.2
S       192.0.0.3 [1/0] via 196.0.0.2
S       192.0.0.4 [1/0] via 196.0.0.2
S       192.0.0.5 [1/0] via 196.0.0.2
S       192.0.0.6 [1/0] via 196.0.0.6
S       192.0.0.7 [1/0] via 196.0.0.6
S       192.0.0.8 [1/0] via 196.0.0.6
S       192.0.0.9 [1/0] via 196.0.0.6
S       192.0.0.10 [1/0] via 196.0.0.6
S       192.0.0.11 [1/0] via 196.0.0.10
S       192.0.0.12 [1/0] via 196.0.0.10
S       192.0.0.13 [1/0] via 196.0.0.10
S       192.0.0.14 [1/0] via 196.0.0.10
S       192.0.0.15 [1/0] via 196.0.0.10
S       192.0.0.16 [1/0] via 196.0.0.14
S       192.0.0.17 [1/0] via 196.0.0.14
S       192.0.0.18 [1/0] via 196.0.0.14
S       192.0.0.19 [1/0] via 196.0.0.14
S       192.0.0.20 [1/0] via 196.0.0.14
     196.0.0.0/30 is subnetted, 8 subnets
C       196.0.0.0 is directly connected, Serial2/0
C       196.0.0.4 is directly connected, Serial7/0
C       196.0.0.8 is directly connected, Serial3/0
C       196.0.0.12 is directly connected, Serial6/0
S       196.0.0.16 [1/0] via 196.0.0.2
S       196.0.0.20 [1/0] via 196.0.0.6
S       196.0.0.24 [1/0] via 196.0.0.10
```

DATA Center

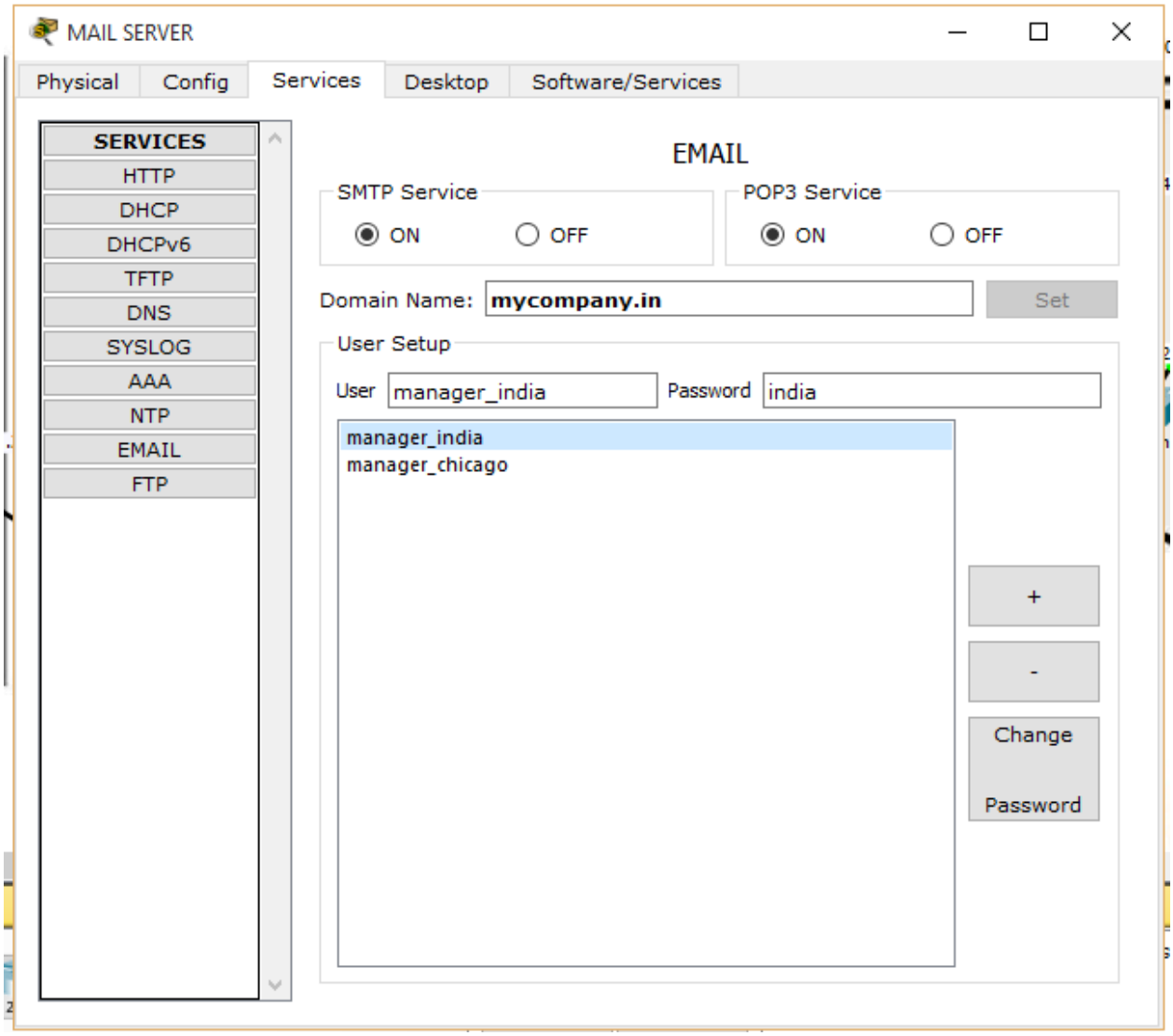
A **data center** (sometimes spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of **data** and information organized around a particular body of knowledge or pertaining to a particular business.



Configurations at various Servers

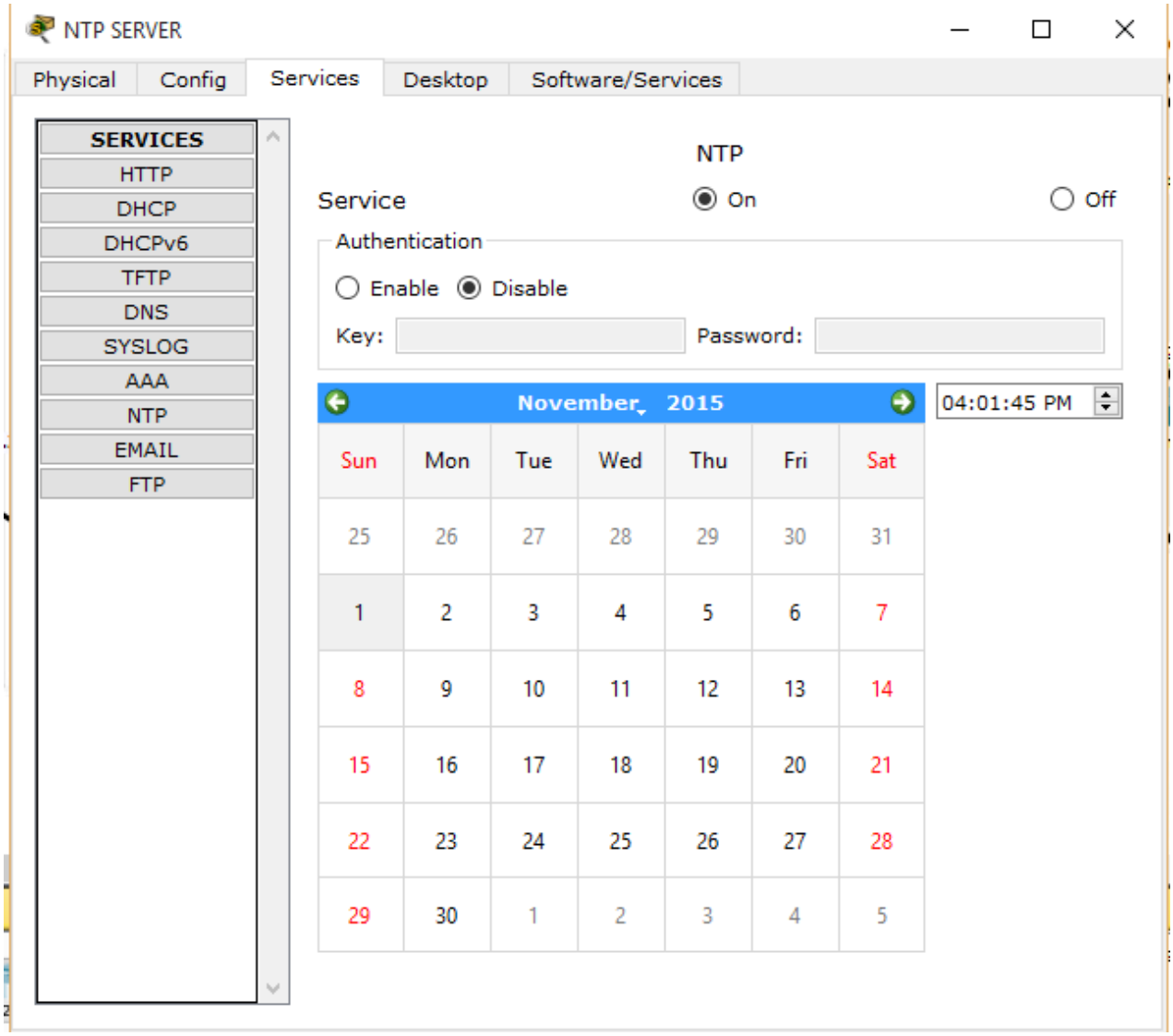
1. SMTP Server (mail server)

Although electronic mail **servers** and other mail transfer agents use **SMTP** to send and receive mail messages, user-level client mail applications typically use **SMTP** only for sending messages to a mail **server** for relaying. For receiving messages, client applications usually use either POP3 or IMAP.



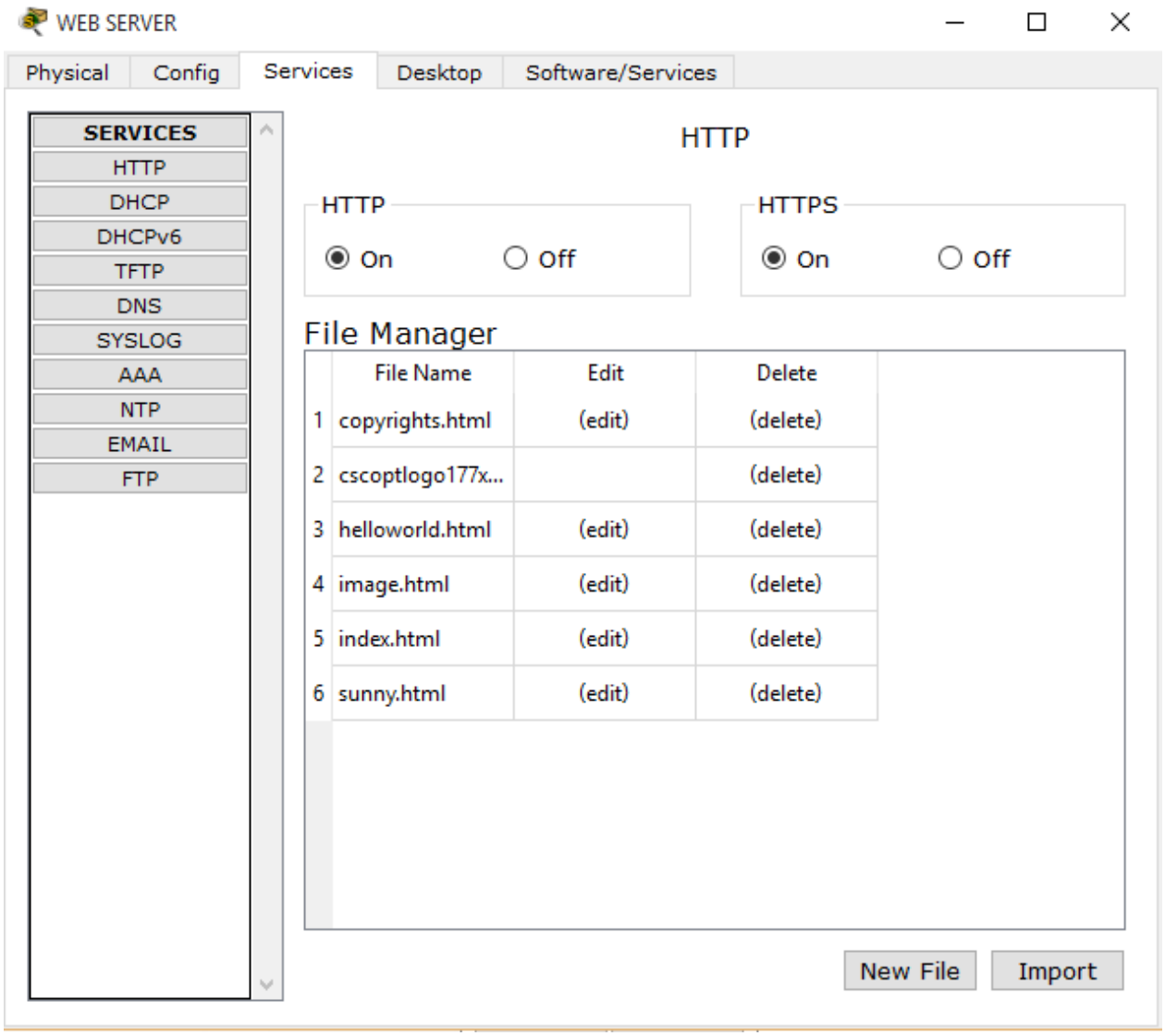
2. NTP Server

NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses a modified version of Marzullo's algorithm to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more



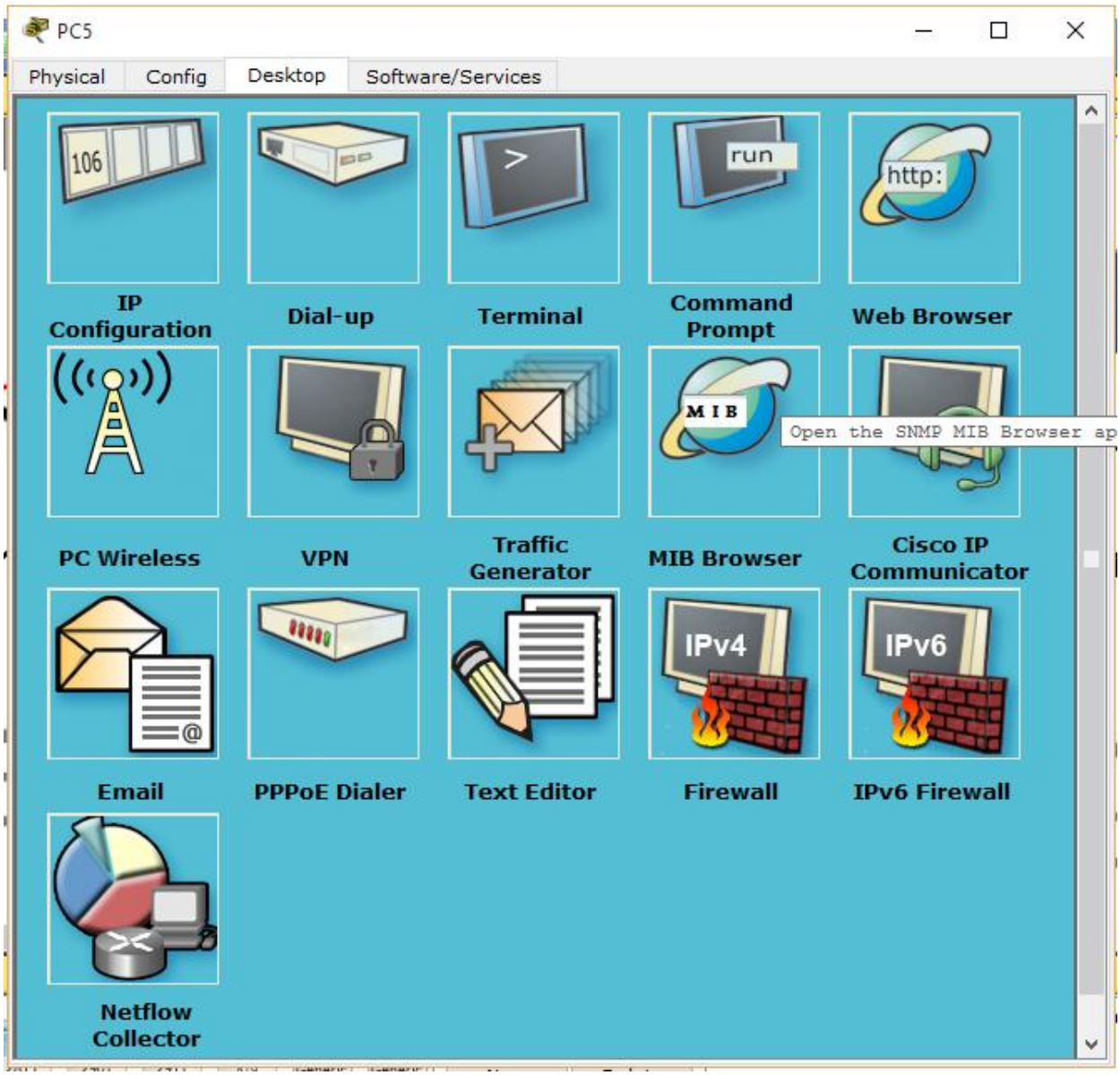
3. WEB Server

A **web server** is a computer system that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide **Web**. The term can refer either to the entire system, or specifically to the software that accepts and supervises the HTTP requests.



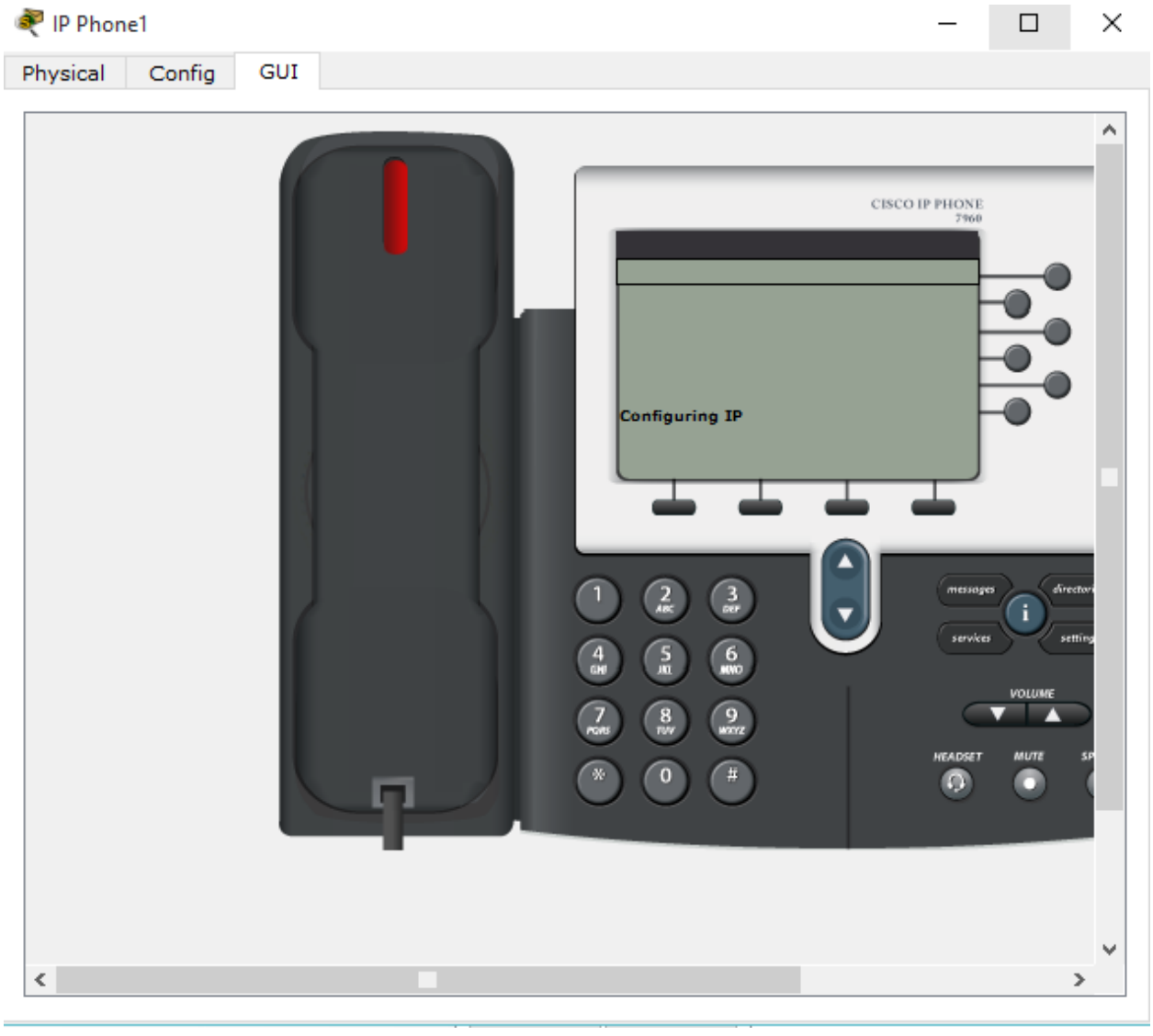
Interface of PC

A **personal computer** is a general-purpose computer whose size, capabilities and original sale price make it useful for individuals, and is intended to be operated directly by an end-user with no intervening computer operator. This contrasts with the batch processing or time-sharing models that allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time.



IP Phone

A VoIP **phone** or **IP phone** uses Voice over **IP**technologies for placing and transmitting **telephone**calls over an **IP** network, such as the Internet, instead of the traditional public switched **telephone**network (PSTN).



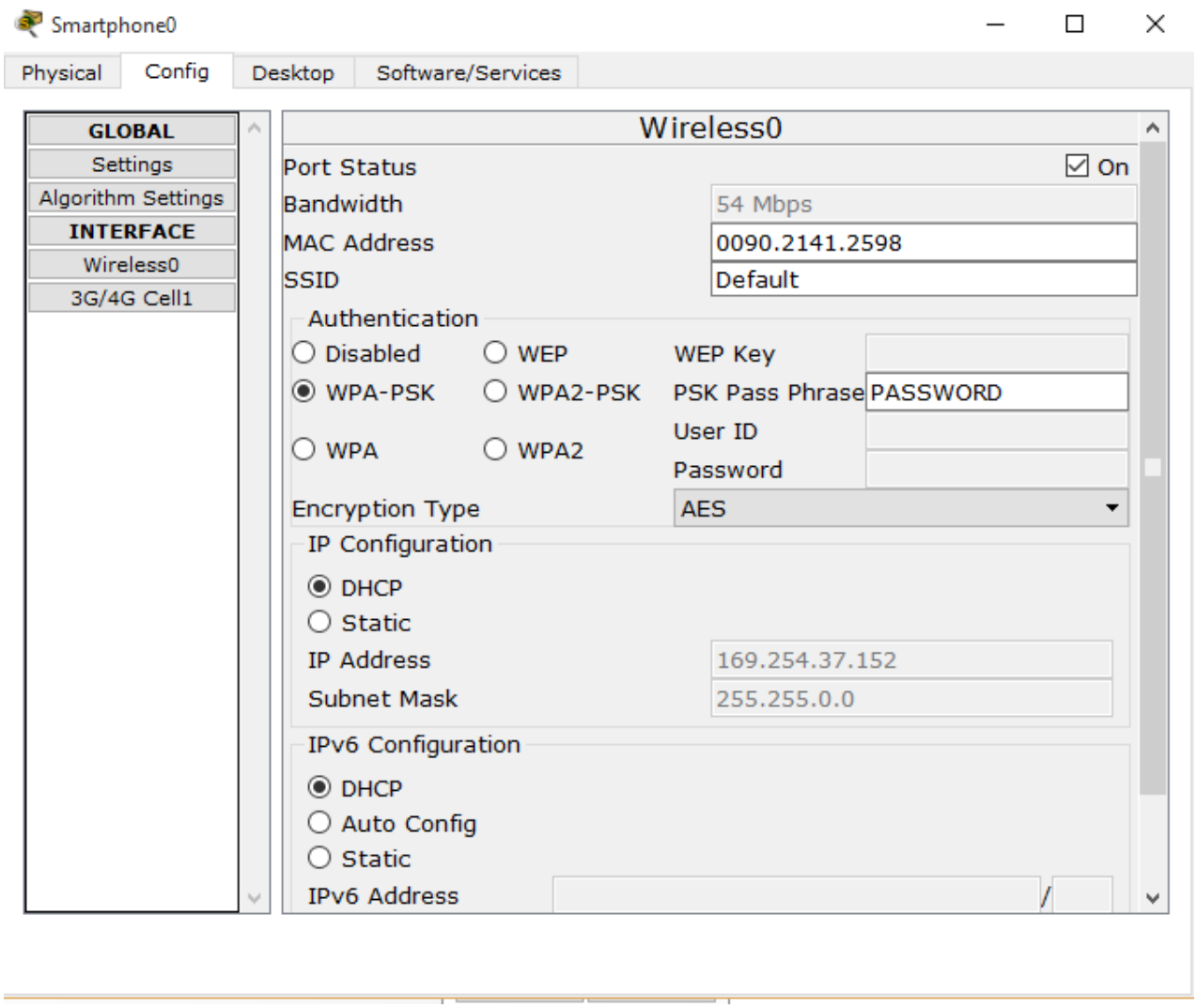
IP Phone configuration

```
logging 172.18.3.2
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 172.16.10.254 port 2000
 auto assign 4 to 6
 auto assign 1 to 5
!
ephone-dn 1
 number 1101
!
ephone-dn 2
 number 1201
!
ephone-dn 3
 number 1301
!
ephone-dn 4
 number 1401
!
ephone-dn 5
 number 1501
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
ntp server 172.18.3.4 key 0
!
end
```

```
Router2(config)#do show ip int brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES unset  administratively down down

FastEthernet1/0        unassigned      YES unset  administratively down down

Serial2/0              196.0.0.29      YES manual up                    up

Serial3/0              196.0.0.14      YES manual up                    up

FastEthernet4/0        unassigned      YES unset  administratively down down

FastEthernet5/0        unassigned      YES unset  administratively down down

Serial6/0              unassigned      YES unset  administratively down down

Serial7/0              unassigned      YES unset  administratively down down
Router2(config)#
```

Smartphone Interface

A smartphone or smart phone is a mobile phone with an advanced mobile operating system which combines features of a personal computer operating system with other features useful for mobile or handheld use.[1][2][3] They typically combine the features of a cell phone with those of other popular mobile devices, such as personal digital assistant (PDA), media player and GPS navigation unit. Most smartphones can access the Internet, have a touchscreen user interface, can run third-party apps, music players and are camera phones. Most Smartphones produced from 2012 onwards also have high-speed mobile broadband 4G LTE internet, motion sensors, and mobile payment mechanisms.



Configuration on Switch

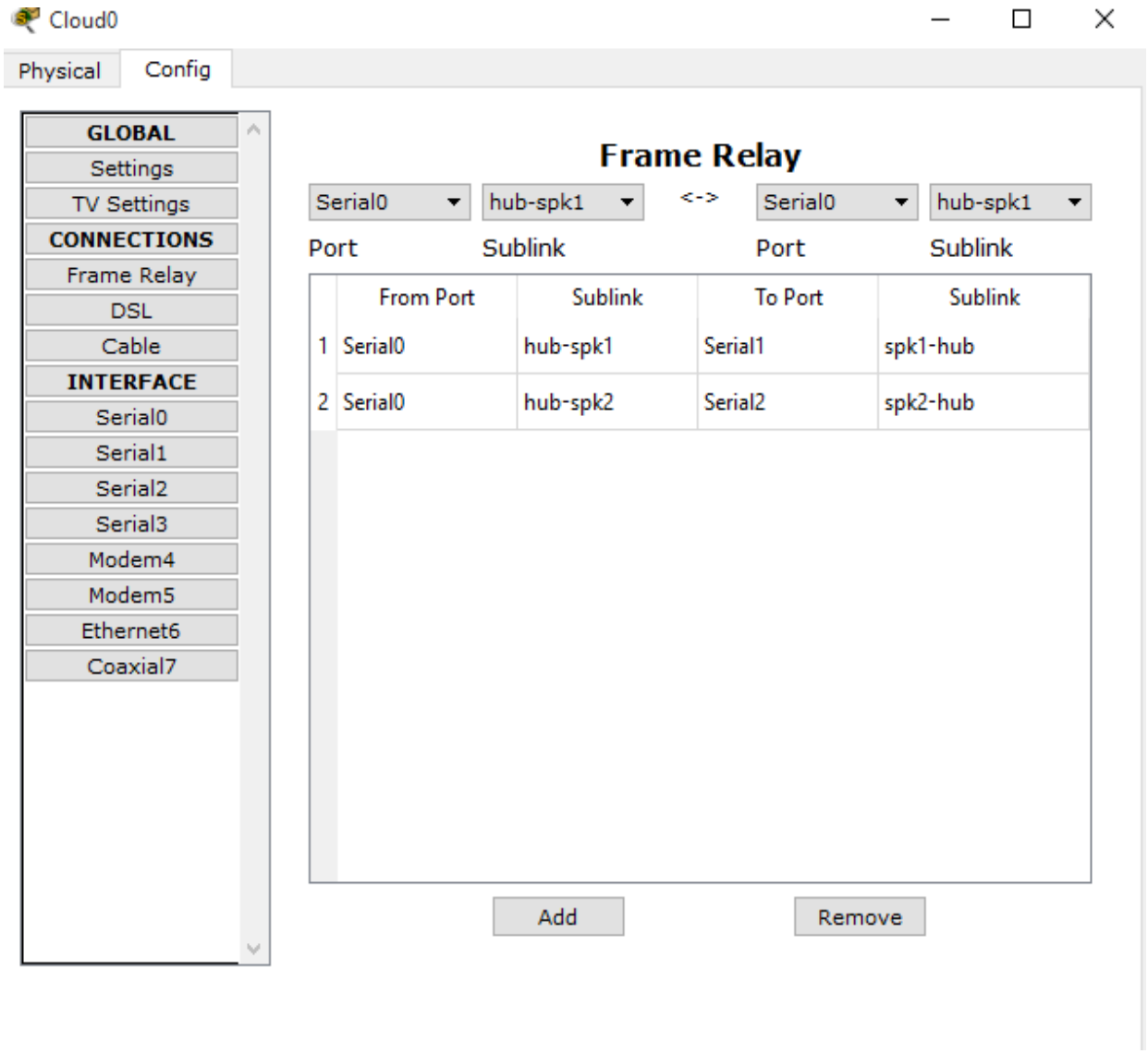
```
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 --More--
```

FastEthernet0/1	unassigned	YES unset	up	up
FastEthernet0/2	unassigned	YES unset	up	up
FastEthernet0/3	unassigned	YES unset	up	up
FastEthernet0/4	unassigned	YES unset	up	up
FastEthernet0/5	unassigned	YES unset	up	up
FastEthernet0/6	unassigned	YES unset	up	up
FastEthernet0/7	unassigned	YES unset	up	up
FastEthernet0/8	unassigned	YES unset	up	up
FastEthernet0/9	unassigned	YES unset	down	down
FastEthernet0/10	unassigned	YES unset	down	down
FastEthernet0/11	unassigned	YES unset	up	up
FastEthernet0/12	unassigned	YES unset	up	up
FastEthernet0/13	unassigned	YES unset	down	down
FastEthernet0/14	unassigned	YES unset	down	down
FastEthernet0/15	unassigned	YES unset	down	down
FastEthernet0/16	unassigned	YES unset	down	down
FastEthernet0/17	unassigned	YES unset	down	down
FastEthernet0/18	unassigned	YES unset	down	down
FastEthernet0/19	unassigned	YES unset	down	down
FastEthernet0/20	unassigned	YES unset	down	down
FastEthernet0/21	unassigned	YES unset	down	down

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/9, Fa0/10, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   VOICE                             active    Fa0/11
30   VLAN0030                          active    Fa0/1, Fa0/2, Fa0/3
40   VLAN0040                          active    Fa0/4, Fa0/5, Fa0/12
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

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


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

CLOUD(frame relay)

Frame relay is a packet-switching telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in wide area networks (WANs).



CONCLUSION

In the age of pre-modernization era all the communication were based on wires and cables. But after a certain period of time as world moved towards the pedestal of technical modernization specially in the field of communication and networking the use of so called networking devices such as hubs, routers, switches has given a soft turn in the field of fast exchange of information and ideas . The day is not far-off,that thing which we can't imagine also that is with a certain click we will get an interface being produced in front of us and the communication and networking process will be dependent on a single click. But neverthelessThe communication will be at that stage when the information gap will not imaginebeing a path of hindrance between individuals.

Future Scope

The work examines perspectives from the inclusion of the autonomicity and self-manageability features in the scope of Future Internet's (FI) deployment. Apart from the strategic importance for further evolution, we also discuss some major future challenges among which is the option for an effective network management (NM), as FI should possess a considerably enhanced network manageability capability. We examine a new network manageability paradigm that allows network elements (NEs) to: be autonomously interrelated/controlled; be dynamically adapted to changing environments, and; learn the desired behaviour over time, based on the original context of the Self-NET research project effort. As self-organizing and self-managing systems have a considerable market impact, we identify benefits for all market actors involved. In addition, we incorporate some recent, but very promising experimental findings, mainly based on the context of a specific use-case for network coverage and capacity optimization, highlighting the way towards developing specific NM-related solutions, able to be adopted by the real market sector. We conclude with some essential arising issues.

REFRENCES

- James F. Kurose , ―Networking : A Top Down Approach ― vol -1 ,1 Jan 2002
- Narasimha Karumanchi, Dr Damodaram & Dr Sreenevas Rao, ― Elements of Computer Networking : An Integrated Approach ― , 20 February 2014
- Thom Singer , ― ABC's of Networking ― , 1 August 2012
- John T.Chambers , ―Ciscopress‖ , vol -21 , 3 March 2013
- T. Socolofsky and C. Kale, ―A TCP/IP Tutorial‖, Jan 1991
- S. Keshav, ―An Engineering Approach to Computer Networking‖