

DESIGN AND DEVELOPMENT OF GENERIC NETWORK ARCHITECTURE USING STATE-OF-THE-ART TECHNOLOGIES

Submitted in partial fulfillment of the Degree of

Bachelor of Technology

In

Electronics and Communication Engineering



May, 2014

By

ADITYA AHUJA (101041)

KAMAL DEWAN (101054)

NIKITA GUPTA (101060)

Under the supervision of

Ms. MEENAKSHI SOOD

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT, HIMACHAL PRADESH

ACKNOWLEDGEMENT

We take this opportunity to express our profound gratitude and deep regards to Prof. S. K. Kak (Vice Chancellor, Jaypee University of Information Technology), Prof. Dr. T. S. Lamba (Dean, Academic and Research, Jaypee University of Information Technology) and Prof. Dr. S. Bhooshan (Head of Department, ECE, Jaypee University of Information Technology), for their exemplary guidance, monitoring and constant encouragement throughout the course of our project.

We would like to thank our project mentor, Mrs. Meenakshi Sood (Asst. Professor, Jaypee University of Information Technology), for offering invaluable assistance, support and guidance at every threshold. The knowledge and blessing given by her from time to time shall carry us a long way in the journey of life on which we are about to embark.

We are greatly indebted to Mr. Sanjay Jain (Network Manager, Jaypee University of Information Technology), for sharing immense amount of knowledge and upgrading us to a level where we could understand and relate to each and every aspect of the existing network architecture of Jaypee University of Information Technology.

Date: 24.05.2014



ADITYA AHUJA (101041)



KAMAL DEWAN (101054)



NIKITA GUPTA (101060)

Certificate

This is to certify that the project report entitled “**DESIGN AND DEVELOPMENT OF GENERIC NETWORK ARCHITECTURE USING STATE-OF-THE-ART TECHNOLOGIES**”, submitted by Aditya Ahuja (101041), Kamal Dewan (101054) and Nikita Gupta (101060) in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date: 24.05.2014



Meenakshi Sood

Assistant Professor,

Jaypee University of Information Technology

CERTIFICATE

This is to certify that the project report entitled “**DESIGN AND DEVELOPMENT OF GENERIC NETWORK ARCHITECTURE USING STATE-OF-THE-ART TECHNOLOGIES**”, submitted by Aditya Ahuja (101041), Kamal Dewan (101054) and Nikita Gupta (101060) in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date:

Meenakshi Sood
Assistant Professor,
Jaypee University of Information Technology

ACKNOWLEDGEMENT

We take this opportunity to express our profound gratitude and deep regards to Prof. S. K. Kak (Vice Chancellor, Jaypee University of Information Technology), Prof. Dr. T. S. Lamba (Dean, Academic and Research, Jaypee University of Information Technology) and Prof. Dr. S. Bhooshan (Head of Department, ECE, Jaypee University of Information Technology), for their exemplary guidance, monitoring and constant encouragement throughout the course of our project.

We would like to thank our project mentor, Mrs. Meenakshi Sood (Asst. Professor, Jaypee University of Information Technology), for offering invaluable assistance, support and guidance at every threshold. The knowledge and blessing given by her from time to time shall carry us a long way in the journey of life on which we are about to embark.

We are greatly indebted to Mr. Sanjay Jain (Network Manager, Jaypee University of Information Technology), for sharing immense amount of knowledge and upgrading us to a level where we could understand and relate to each and every aspect of the existing network architecture of Jaypee University of Information Technology.

Date:

ADITYA AHUJA (101041)

KAMAL DEWAN (101054)

NIKITA GUPTA (101060)

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	1
1.1 OSI and TCP/IP Models	2
1.2 Network Topologies	5
1.3 Internetworking Protocol.....	6
1.4 Network Devices	9
1.5 Transmission Media	9
1.6 Subnetting.....	10
1.7 Supernetting	11
1.8 Network Address Translation.....	11
CHAPTER 2: TECHNOLOGIES EMPLOYED	13
2.1 Routing	13
2.2 Routing Protocols	13
2.3 Virtual Local Area Network.....	14
2.4 Inter-VLAN Communication	15
2.5 Voice over IP.....	16
2.6 Virtual Private Network	16
2.7 Frame Relay	18
2.8 Port Security	19
2.9 EtherChannel.....	19
2.10 Firewall.....	20
2.11 Access Control List	21
2.12 LAN Design	22
CHAPTER 3: CAMPUS NETWORK	
ARCHITECTURE DESIGN	25
3.1 Proposed network architecture	25
3.2 Demonstration of network.....	37
3.3 Conclusion.....	43
CHAPTER 4: ENTERPRISE NETWORK	
ARCHITECTURE DESIGN	44
4.1 Proposed network architecture.....	44
4.2 Demonstration of network	52
4.3 Conclusion	53

PUBLICATION 54
 Deploying Pragmatic Techniques for Campus Network Design.....54

REFERENCES.....67

LIST OF FIGURES

Chapter 1

Figure 1.1	The OSI Reference Model.....	3
Figure 1.2	Comparison of TCP/IP and OSI model.....	5
Figure 1.3	Classful addressing in IPv4.....	7
Figure 1.4	IPv4 Header.....	8
Figure 1.5	IPv6 Header.....	8

Chapter 2

Figure 2.1	Virtual Private Network.....	17
Figure 2.2	Basic Frame Relay Structure.....	19
Figure 2.3	Connected Switches With Or Without Ether Channels.....	20
Figure 2.4	Basic functionality of a Firewall.....	21
Figure 2.5	Basic LAN Framework.....	23

Chapter 3

Figure 3.1	Network Architecture proposed as an enhancement to the existing network of Jaypee University of Information Technology	25
Figure 3.2	Academic Area.....	26
Figure 3.3	Configuration for VLAN and Trunk Port.....	27
Figure 3.4	Configuration for Sub-interface.....	27
Figure 3.5	Configuration for DHCP.....	28
Figure 3.6	Configuration for OSPF.....	28
Figure 3.7	VoIP : Configuration for VLAN and Trunk Port.....	28
Figure 3.8	VoIP : Configuration for Sub-interfaces.....	29
Figure 3.9	VoIP : Configuration for DHCP Pool.....	29
Figure 3.10	VoIP : Configuration for registration of IP Phone.....	29
Figure 3.11	VoIP : Configuration for enabling inter-network IP Phone calling.....	29
Figure 3.12	VoIP : Configuration for OSPF.....	30

Figure 3.13	Wireless Router : Configuration for LAN side of the router.....	30
Figure 3.14	Wireless Router : Configuration for the link connecting to WAN.....	30
Figure 3.15	Laboratory Block.....	31
Figure 3.16	Configuration for EIGRP on laboratory router.....	31
Figure 3.17	Server Room.....	31
Figure 3.18	Configuration for HTTP server.....	32
Figure 3.19	Configuration for FTP server.....	32
Figure 3.20	Configuration for DNS server.....	32
Figure 3.21	Configuration for RIP v2 on Server Router.....	33
Figure 3.22	Edge Router and its connections to different areas.....	33
Figure 3.23	Configuration for redistribution on central router.....	33
Figure 3.24	Redundant ISP Block.....	34
Figure 3.25	Configuration for NAT.....	34
Figure 3.26	Area showing connection of ISP router and Edge router.....	35
Figure 3.27	Configuration for Google Server and routing.....	35
Figure 3.28	Private Home Network.....	36
Figure 3.29	PDU at Multilayer switch2.....	36
Figure 3.30	PDU at Academic Block Switch.....	37
Figure 3.31	PDU on Academic Router.....	37
Figure 3.32	PDU at Edge Router.....	38
Figure 3.33	PDU at Laboratory Router.....	38
Figure 3.34	PDU at Laboratory Switch.....	39
Figure 3.35	PDU at Laboratory 2 switch.....	39
Figure 3.36	PDU at PC10.....	40
Figure 3.37	Accessing Students' Resource.....	41
Figure 3.38	Ring going out from the IP Phone with number 1000.....	42
Figure 3.39	IP Phones connected.....	42

Chapter 4

Figure 4.1	Network design proposed for an enterprise.....	44
Figure 4.2	Block 1.....	45
Figure 4.3	Block 2.....	46

Figure 4.4	Block 3.....	46
Figure 4.5	Block 4.....	47
Figure 4.6	Configuration for Port Security in Block 4.....	47
Figure 4.7	Configuration for access control list (ACL) in Block 4.....	48
Figure 4.8	Frame Relay Network.....	48
Figure 4.9	Frame Relay : Configuration for sub-interface.....	48
Figure 4.10	Frame Relay : Configuration for DLCI numbers on serial connection of cloud.....	49
Figure 4.11	Frame Relay : Configuration for Permanent Virtual Circuit.....	49
Figure 4.12	ISPs connecting the network to outside world.....	50
Figure 4.13	Site-to-site VPN	50
Figure 4.14	Configuration for one end of VPN tunnel.....	51
Figure 4.15	Configuration for other end of VPN tunnel.....	51
Figure 4.16	Unsuccessful Ping originating from outside the R&D Department.....	52
Figure 4.17	Unsuccessful Ping originating from inside the R&D Department.....	52

LIST OF ABBREVIATIONS

LAN	Local Area Network
WAN	Wide Area Network
ISO	International Standards Organization
TCP	Transmission Control Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
UTP	Unshielded Twisted Pair
STP	Shielded Twisted Pair
CIDR	Classless Inter-Domain Routing
NAT	Network Address Translation
FTP	File Transfer Protocol
RIP	Routing Information Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
LSA	Link State Advertisement
VLAN	Virtual Local Area Network
PC	Personal Computer
VoIP	Voice Over Internetworking Protocol
VPN	Virtual Private Network
IPsec	Internet Protocol Security
AAA	Authentication, Authorization and Accounting

DTE	Data Terminal Equipment
DCE	Data Circuit Equipment
MAC	Media Access Control
DLCI	Data Link Connection Interface
VC	Virtual Circuit
SVC	Switched Virtual Circuit
PVC	Permanent Virtual Circuit
ATM	Asynchronous Transfer Mode
STP	Spanning Tree Protocol
PAgP	Port Aggregation Protocol
LACP	Link Aggregation Control Protocol
ACL	Access Control List
DHCP	Dynamic Host Configuration Protocol
RIPv2	Routing Information Protocol version 2
HTTP	Hypertext Transfer Protocol
DNS	Domain Name System
PAT	Port Address Translation
ISP	Internet Service Provider
PDU	Protocol Data Unit
IT	Information Technology
CIR	Committed Information Rate

SUMMARY

Networking has traversed from days where networks were considered a background component of businesses to the present electronic age, where networks are an imperative resource, and directly determine revenue generation for an organization. In today's dynamic arena of networking, the crafting of networks has escalated from using just an elemental set of features, to consolidating modernistic technologies and services, in an effort to come up with avant-garde networks which can meet the aim of connectivity, scalability, simplicity of operation, and flexible accommodation of new trends and technologies. When the network is going to interface with the internet, its security is also an important aspect, thus, today's networks must be open and pervasive, yet remain secure and controlled. Moreover, the demand for mobile computing has increased in today's business environment, thus the networks must also be accessible remotely. Therefore, new network designs are needed, as heirloom solutions cannot meet the new requirements, nor reduce the costs and streamline the operations.

Using Cisco's network simulation software, Cisco Packet Tracer, we present two network architectures, the Campus Network Architecture and the Enterprise Network Architecture. The Campus Network Architecture is an enhancement to the existing network architecture of Jaypee University of Information Technology, by the incorporation of new and advanced technologies such as VoIP, VPN, Ether Channels, STP, ISP redundancy. Adhering to the need of the hour in corporate sector, we have proposed the Enterprise Network Architecture, using novel technologies such as Frame Relay, Port Security, Access Control Lists, VoIP, VPN, Redistribution of Routing Protocols and ISP Redundancy.

CHAPTER – 1

INTRODUCTION

Network architecture and designing, which was considered sheer art few decades ago, today, in the contemporary world, is an amalgamation of knowledge and art. In the past, network designers had a very limited number of options in terms of hardware devices, protocols and media, and thus network designing was relatively easier, with very little scope of mistake, but with limited efficiency and flexibility. In the contemporary world, the designing of networks has evolved and matured to the incorporation of multiple technologies and services, in an effort to support the vastly disparate end to end communication requirements. The modern networks are designed to meet security, connectivity, and performance challenges while enabling key IT initiatives. They are based on complex environments, which are an amalgamation of multiple protocols, media and interconnections to networks outside any single organization's dominion of control, thus giving rise to computationally efficient networks, which can scale, and flexibly accommodate upgrades without an entire revamp of the design. Networks are broadly classified as *LAN (Local Area Network)*, and *WAN (Wide Area Network)*. LANs, which persist over a relatively shorter distance are designed to allow personal computers to share resources, which can include hardware (e.g., a printer), software (e.g., an application program), or data. A WAN, which is a geographically dispersed collection of LANs, provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. In networking's early days, networks were not considered a critical resource as they did not directly support revenue generation. Now, the picture has changed radically. As our ability to gather, process, and distribute information grows, the demand for ever more sophisticated information processing grows even faster. The issue here is resource sharing, and the goal is to make all programs, equipments, and especially data available to anyone on the network without regard to the physical location of the resource and the user. In enterprises today, more business is conducted electronically and deals are closed rapidly. In today's digital age, company operations have undergone a sea-change, and 24*7 connectivity has never been more imperative than it is today. Therefore, it is apt to say that the corporate network has matured from an inert business element to a very active and visible asset that today's organizations rely on to support their day-to-day functions. It is seen as a critical resource, which directly supports revenue generation.

The roots of our project lie in two different network architectures. The first architecture serves as an enhancement to the existing network of *Jaypee University of Information Technology (JUIT)*, by the incorporation of new and advanced technologies such as *VoIP (Voice over IP)*, *VPN (Virtual Private Network)*, *Ether Channels*, *STP (Spanning Tree Protocol)* and *ISP (Internet Service Provider) redundancy*. The second network architecture serves as a state-of-the-art enterprise network, consisting of an effective blend of a plethora of new technologies such as *Frame Relay*, *Port Security*, *Access Control Lists (Firewalling)*, *VoIP*, *VPN*, *Redistribution of Routing Protocols* and *ISP Redundancy*. The proposed architectures are generic and can be utilized for any campus, be that of a university, a corporate office, a hospital or myriads of other organizations.

We start with a backdrop of data communications and networking, wherein discussion on the various concepts has been carried out.

1.1) OSI AND TCP/IP MODEL

A) OPEN SYSTEMS INTERCONNECTION (OSI) REFERENCE MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol, it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model is a layered framework for the design of network systems that allow communication between all types of computer systems.

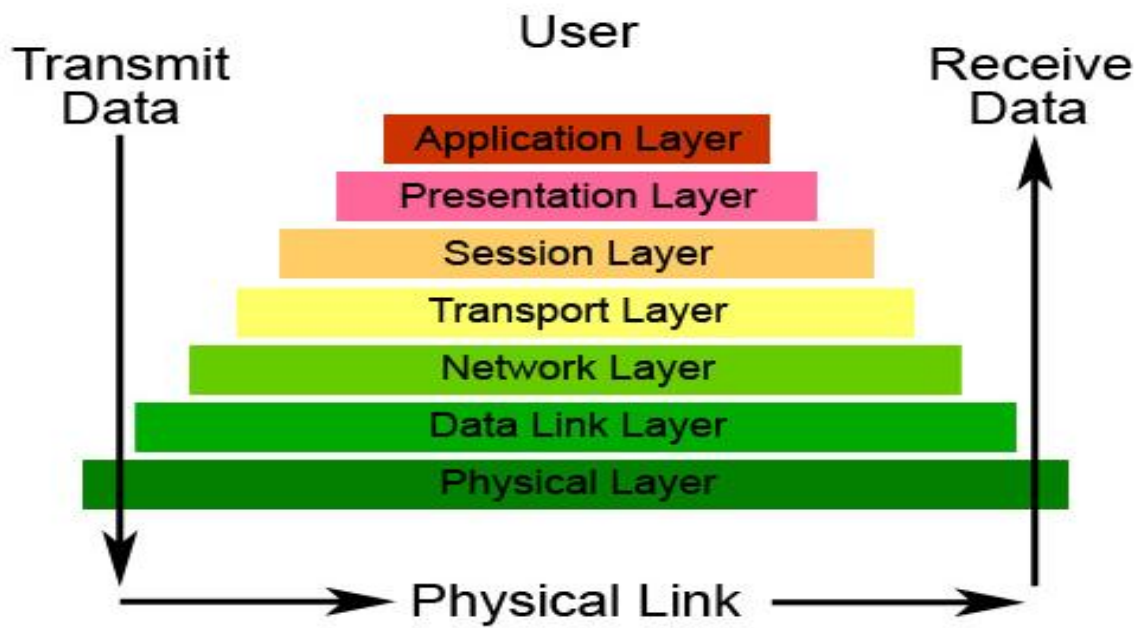


Figure 1.1 - The OSI Reference Model

The layers of OSI model are discussed below:

- **PHYSICAL LAYER (LAYER 1)**

It establishes the actual physical connection between the computer equipment and the network, and provides the transmission of bits from one system to another.

- **DATA LINK LAYER (LAYER 2)**

It provides the transmission of packets, and performs error detection and correction functions to ensure that a packet contains the same information received as sent.

- **NETWORK LAYER (LAYER 3)**

It determines the path that will be taken through the network. The network layer also controls the rate at which the network accepts packets, to avoid and recover from congestion.

- **TRANSPORT LAYER (LAYER 4)**

It provides for the flow of data between sender and receiver, and ensures that the data arrives at the correct destination. Another function of this layer is to ensure that packets are sent at a rate the receiver and the application can cope with. At the receiver, the transport layer reassembles the packets into messages and delivers them to the next highest layer.

- **SESSION LAYER (LAYER 5)**

It allows the setup and termination of a communications path, ensures that the sender is authentic and has access rights to establish a connection, and synchronizes the communication between two systems.

- **PRESENTATION LAYER (LAYER 6)**

It converts outbound data from a machine-specific format to an international standard format. It converts inbound data from international format to a machine-specific format.

- **APPLICATION LAYER (LAYER 7)**

It provides the software for network services, such as file transfer, remote login, remote execution, e-mail, etc. It provides the interface between user programs and the network.

B) TCP/IP (TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL) MODEL

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality, however, the modules are not necessarily interdependent. Where the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term “hierarchical” means that each upper-level protocol is supported by one or more lower-level protocols.

The reference model consists of 5 layers which are dependent on each other for some limited number of functions. These layers are:

- Physical
- Data link
- Network
- Transport
- Application

The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

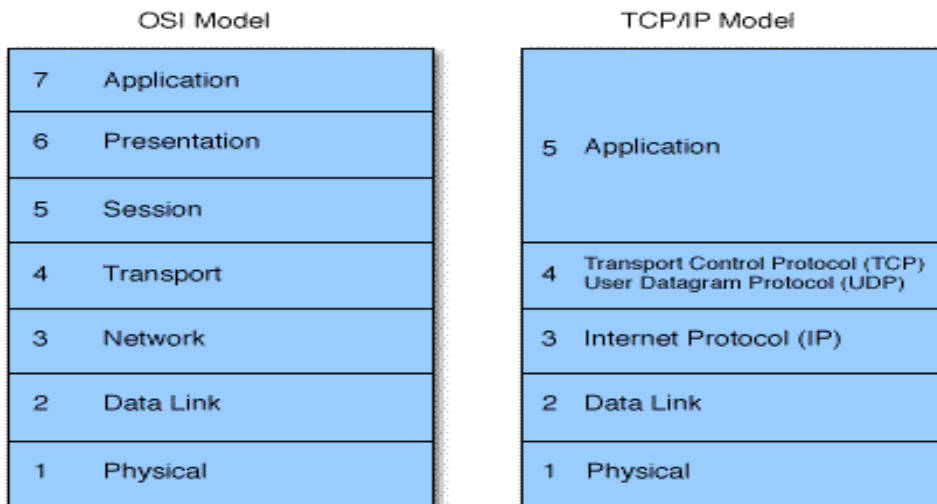


Figure 1.2 – Comparison of TCP/IP and OSI model

1.2) NETWORK TOPOLOGIES

Network topology is the arrangement of the various elements (links, nodes etc.) of a computer network. The transmission of packets through different layouts gives rise to formation of these topologies where efficient delivery, distortion, time to live parameters are given much more importance. The various topologies are discussed below:

BUS TOPOLOGY

All the end devices are attached with a single cable connected throughout the network. It is the most basic architecture where the transmission of packets for a single station restricts all other station from using the cable. Thus, this topology comes with a vast set of limitations.

RING TOPOLOGY

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

STAR TOPOLOGY

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange.

MESH TOPOLOGY

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. Besides being robust, a mesh eliminates the traffic problems that can occur when links must be shared by multiple devices.

1.3) INTERNET PROTOCOL

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. It performs the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. To achieve it, IP defines packet structures that encapsulate the data to be delivered. The data so parted is sent in frames having header which defines its origin. It also defines addressing methods that are used to label the datagram with source and destination information.

Originally, IP was the connectionless datagram service in the primitive Transmission Control Program whereas the other being the connection-oriented Transmission Control Protocol (TCP). So, The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the internet. Its successor, Internet Protocol Version 6 (IPv6) is now getting acclaimed.

A) INTERNET PROTOCOL VERSION 4

IPv4 addresses are 32 bits long. These bits are divided into four octets, each octet have 8 bits. It is profitable to manage IP addresses in a network because changes in the values of the 32 bits indicate either a different IP network address or IP host address.

In order to provide some structure to the way IP addresses are assigned, IP addresses were initially grouped into classes. This architecture is called classful addressing. In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space, ranging from 0.0.0.0 to 255.255.255.255. The addressing of these classes has been depicted in figure 1.3.

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Figure 1.3 - Classful Addressing in IPv4

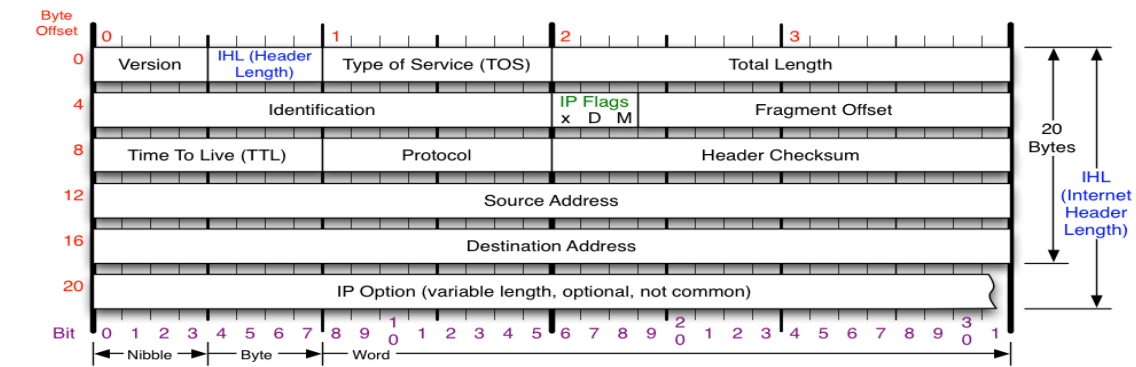
The range of IP addresses in each class is determined by the number of bits allocated to the network section of the 32-bit IP address. The number of bits allocated to the network section is represented by a mask written in dotted decimal or with the abbreviation $/n$ where n = the numbers of bits that are high in the mask.

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks [4].

An IP datagram consists of a header and a text part. The header has a 20 byte fixed part and a variable length optional part. The detailed functioning of IPv4 header is shown in figure 1.4.

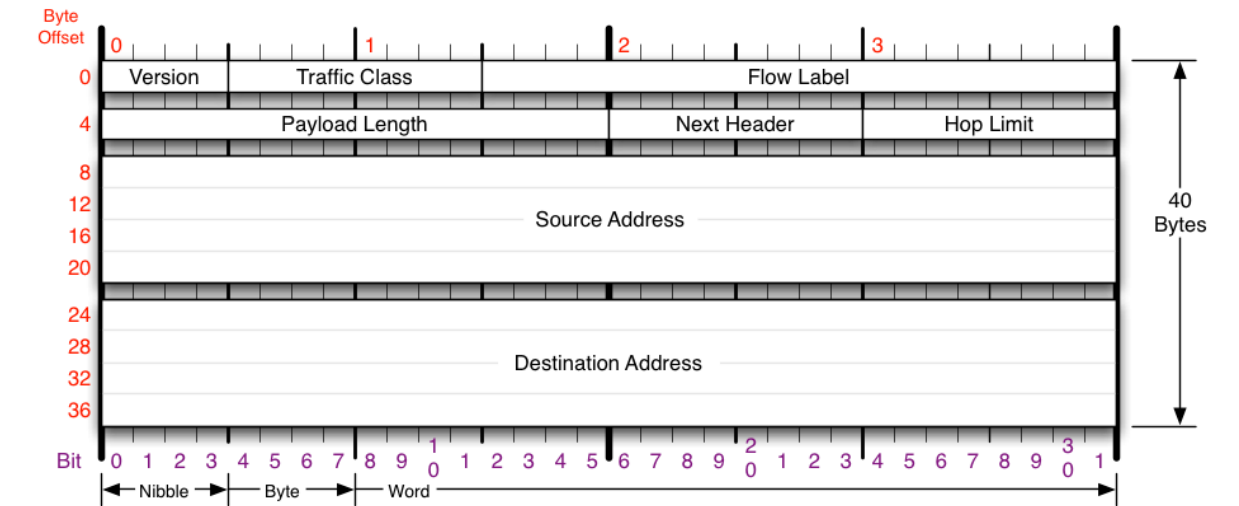
B) INTERNET PROTOCOL VERSION 6

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol. With the ability to meet the ever-increasing number of new devices being connected to the Internet, IPv6 uses a 128-bit address, allowing 2^{128} , or approximately 3.4×10^{38} addresses, or more than 7.9×10^{28} times as many as Ipv4, which uses 32-bit addresses. The two protocols are not designed to be interoperable, complicating the transition to IPv6. An IPv6 datagram is shown in figure 1.5.



Version Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.	Protocol IP Protocol ID. Including (but not limited to): 1 ICMP 17 UDP 57 SKIP 2 IGMP 47 GRE 88 EIGRP 6 TCP 50 ESP 89 OSPF 9 IGRP 51 AH 115 L2TP	Fragment Offset Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.	IP Flags x D M x 0x80 reserved (evil bit) D 0x40 Do Not Fragment M 0x20 More Fragments follow RFC 791
Header Length Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.	Total Length Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.	Header Checksum Checksum of entire IP header	RFC 791 Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Figure 1.4 - IPv4 Header



Version Version of IP Protocol. 4 and 6 are valid. This diagram represents version 6 structure only.	Payload Length 16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. Any extension headers are considered part of the payload.	Next Header 8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.	Hop Limit 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.
Traffic Class 8 bit traffic class field.	Source Address 128-bit address of the originator of the packet.	Destination Address 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).	RFC 2460 Please refer to RFC 2460 for the complete Internet Protocol version 6 (IPv6) Specification.
Flow Label 20 bit flow label.			

Figure 1.5 - IPv6 Header

1.4) NETWORK DEVICES

For a LAN to be able to access the backbone network, special networking devices are required. These devices help in connecting type or types of networks at different layers of the OSI model. Some of the basic networking devices are discussed below:

Hubs are simple devices that direct data packets to all the devices connected to that hub irrespective of the fact that given data packet is destined for that network. Thus, they act as a broadcasting unit and provide a pathway for the electrical signals to travel along. They come with the disadvantage that they can create a performance bottleneck on busy networks [5].

A **Bridge** is a device that connects two or more local area networks, or two or more segments of the same network. Nowadays, multiport bridges allow network managers to connect more than two network segments to each other. It filters network traffic by examining each set of data and transmitting only appropriate data to each connected segment. In this manner, bridges help to reduce overall network traffic.

A **Switch** is a special type of hub that offers an additional layer of intelligence to basic, physical-layer repeater hubs. Switch checks for the destination MAC address and forward it to the relevant port to reach the computer only. In this manner, switches reduce traffic and divide the collision domain into segments. If in case, a destination MAC address is not present in table it forwards it to all except the source segment.

Routers are networking devices used to extend or segment networks by forwarding packets from one logical network to another. It is often used to regulate the flow of information between networks. They are aware of many possible paths across the networks and can choose the best route for each data packet to travel, using different routing algorithms. The so created internal tables of network information that it compiles, a router then determines whether or not it knows how to forward the data packet towards its destination.

1.5) TRANSMISSION MEDIA

The transmission media, used to convey information, can be classified as guided or unguided. Guided media provide a physical path along which the signals are propagated. These include twisted pair, coaxial cable and optical fiber [7]. Unguided media employ an antenna for transmitting through air, vacuum, or water. LAN design mostly relies on guided transmission media for higher efficiency as compared to unguided transmission. The basic features of transmission media is discussed in table 1.

Media Type	Maximum Segment Length	Speed	Cost	Advantages	Disadvantages
UTP	100 m	10 Mbps to 1000 Mbps	Least expensive	Easy to install; widely available and widely used	Susceptible to interference; can cover only a limited distance
STP	100 m	10 Mbps to 100 Mbps	More expensive than UTP	Reduced crosstalk; more resistant to EMI than Thinnet or UTP	Difficult to work with; can cover only a limited distance
Coaxial	500 m (Thicknet) 185 m (Thinnet)	10 Mbps to 100 Mbps	Relatively inexpensive, but more costly than UTP	Less susceptible to EMI interference than other types of copper media	Difficult to work with (Thicknet); limited bandwidth; limited application (Thinnet); damage to cable can bring down entire network
Fiber-Optic	10 km and farther (single-mode) 2 km and farther (multimode)	100 Mbps to 100 Gbps (single mode) 100 Mbps to 9.92 Gbps (multimode)	Expensive	Cannot be tapped, so security is better; can be used over great distances; is not susceptible to EMI; has a higher data rate than coaxial and twisted-pair cable	Difficult to terminate

Table 1 - Guided Transmission Media

1.6) SUBNETTING

Subnetting is the technique which helps to create multiple logical networks that exist within a single Class A, B, or C network.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If a major network (Class A, B, or C) is segmented into smaller subnetworks, a network of interconnecting subnetworks is obtained. Each data link on this network would then have a unique network ID. Any device, or gateway, connecting n subnetworks has n distinct IP addresses, one for each subnetwork that it interconnects.

In order to divide a network into multiple subnetworks, the natural mask is extended and some of the bits from the host ID portion of the address are used to create a subnetwork ID.

1.7) SUPERNETTING

Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. The original Internet Protocol (IP) suite defines IP addresses in four major classes of address structure, Classes A, B, C and D. Each class allocates one portion of the 32-bit IPv4 format to a network address and the remaining portion to the specific host machines within the network [2].

For example, with the employment of supernetting, variant network address 192.168.2.0/24 and an adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses. Supernetting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.

1.8) NETWORK ADDRESS TRANSLATION

Network Address Translation (NAT) is a network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address. It was originally designed in an attempt to help conserve IPv4 addresses, available with the Internet Service Provider. It modifies the IP address information in IPv4 headers while in transit across a traffic routing device.

This translation is performed in two ways, statically and dynamically. Both of these techniques are discussed below:

A) STATIC NAT

A static NAT configuration creates a one-to-one mapping and translates a specific address to another address. This type of configuration creates a permanent entry in the NAT table and hence, the organization is required to purchase as many public IP addresses as the number of users. This is mostly useful for hosts that provide application services like mail, Web, FTP, and so forth [8].

B) DYNAMIC NAT

In dynamic NAT, generally all the private addresses are mapped onto a single or a few number of public addresses. A table is created when the host initiated a connection and generally establishes a one- to-many mapping between the addresses. Dynamic NAT allows session to be

initiated only from inside or outside networks for which it is configured. Dynamic NAT entries are removed from the translation table if the host does not communicate for a specific period of time which is configurable. The address is then assigned to the pool for use by another host.

CHAPTER – 2

TECHNOLOGIES EMPLOYED

2.1) ROUTING

Routing is the act of finding the destination of the data in the network and selecting the best path in the network to forward it. Along the way, at least one router is encountered. In the process, datagram routing tables are built at nodes or routers. Routers are capable of supporting multiple independent routing protocols and maintaining routing tables for delivery of packets over several networks. Routing can be classified in two types:

A) STATIC ROUTING

In static routing, it is possible to route the packets through a specific and manually controlled path. As a result, neighboring routers do not exchange routing information and have no way to communicate any changes in the network topology. This features of static routes increases manageability in small networks and adds some level of security. The disadvantage of this is that maintaining networks manually can be tedious and prone to human error.

B) DYNAMIC ROUTING

Dynamic routing uses algorithm to enable routers to discover routes automatically to different destinations and to share the information with other routers. Its most important is the ability to react to topological changes. Dynamic routing protocols determine the best and the next-best paths to any destination networks. It can ensure load balancing when more than one path exists between the source and the destination [10].

2.2) ROUTING PROTOCOLS

A routing protocol is a network layer protocol that provides enough information in its network layer address to allow a packet to be forwarded from one host to another host based on the addressing scheme, without knowing the entire path from source to destination.

They are used in the implementation of routing algorithms to facilitate the exchange of routing information between networks, allowing routers to build routing tables dynamically.

The routing protocols are further classified as Distance vector routing protocol and Link-state routing protocol. In distance vector routing, each node maintains a table of minimum distances to every node, guides the packets to the desired node by showing the next stop in the route, while in

link-state routing, each node in the domain has the entire topology of the domain, i.e., the list of nodes and links, how they are connected including the type, minimum distance, and condition of the links (up or down). Hence, the routing table for each node is unique because the calculations are based on different interpretations of the topology.

Some of the routing protocols are detailed as follows:

A) ROUTING INFORMATION PROTOCOL (RIP)

It is a standards-based, distance-vector routing protocol used by routers to exchange routing information. RIP uses hop count to determine the best path between two locations. Hop count is the number of routers the packet must go through till it reaches the destination network. The maximum allowable number of hops a packet can traverse in an IP network implementing RIP is 15 hops [11].

B) ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance-vector routing protocol that is used on a computer network to help automate routing decisions and configuration. It is a classless protocol because it includes the subnet mask in its route updates. It synchronizes routing tables between neighbors initially and then sends specific updates only when topology changes occur, thus making it suitable for very large networks, having a maximum hop count of 255.

C) OPEN SHORTEST PATH FIRST (OSPF)

Open Shortest Path First (OSPF) is an open link-state routing protocol that calls for the sending of link-state advertisements (LSAs), which include information on attached interfaces, to all other routers within the same hierarchical area. As the routers accumulate link-state information, they use the Shortest Path First algorithm to calculate the shortest path to each node.

2.3) VIRTUAL LOCAL AREA NETWORK (VLAN)

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN however allowing a special feature of forming group end stations even if they are not located physically on the same LAN segment.

Other features of a VLAN are:

- Broadcast packets sent by one of the workstations will reach all the others in the VLAN, and will remain confined to that particular VLAN only.

- All the workstations can communicate with each other without needing to go through a gateway.

Some of the advantages of Virtual LAN are:

1. Performance

As mentioned above, routers that forward data in software become a bottleneck as LAN data rates increase. Doing away with the routers removes this bottleneck.

2. Greater flexibility

If users move their desks, or just move around the place with their laptops, then, if the VLANs are set up the right way, they can plug their PC in at the new location, and still be within the same VLAN. This is much harder when a network is physically divided up by routers.

3. Ease of partitioning-off resources

If there are servers or other equipment to which the network administrator wishes to limit access, then they can be put off into their own VLAN. Then users in other VLANs can be given access selectively.

2.4) INTER-VLAN COMMUNICATION

Since VLANs are functionally equal to multiple separate switches each with its own subnet, a router is required to route traffic between them. Networks that have multiple switches connected to a router of course need one physical connection from each switch to a separate port on the router. The same would normally be true of VLANs within a single switch, need of a separate physical connection from a port in each VLAN on the switch, to multiple ports on the router. This becomes a problem for a number of reasons, but primarily because most routers don't have more than a few Ethernet ports, and even with enough ports this would be an unnecessary waste of resources on the router. The solution to this multiple connection problem is to use what is called a trunk line.

A trunk line aggregates traffic from multiple independent VLANs into a single physical connection between switches, or between a switch and a router. Within this trunk there is a logical division of the connection, by encapsulating each frame with VLAN information, or by using a special frame header marking each frame as belonging to a specific VLAN. Normally this trunk will carry traffic for each VLAN present on the switch.

A sub interface is a division of one physical interface into multiple logical interfaces depending on the number of networks. Routers commonly employ sub interfaces for routing traffic between virtual LAN (VLAN).

2.5) VOICE OVER INTERNET PROTOCOL

For many people, Internet Protocol (IP) is more than just a way to transport data, it's also a tool that simplifies and streamlines a wide range of business applications. VoIP is the most obvious example. It is a rapidly emerging technology for voice communication that uses the ubiquity of IP-based networks to deploy VoIP client devices, such as desktop IP phones and mobile VoIP-enabled handheld devices and carry phone calls over the data network, whether on the Internet or an organization's own internal network. A primary attraction of VoIP is its ability to help reduce expenses because telephone calls travel over the data network rather than the phone company's network [14].

2.6) VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) is a network that generally uses internet to establish connection to the secured internal network of an organization as shown in figure 2.1. The people working in other offices of the organization and employees like remote desktop engineers need a fast, secure and reliable way to share information across computer networks. The security and protection of the shared information is maintained using special tunneling protocols and complex encryption procedures, hence the new connection so established is virtually a dedicated point-to point connection. Thus, VPN is a cheaper and more secure way to connect as compared to privately owned or lease services. The figure shows the different ways in which the members and different offices of an organization can connect using VPN [15].

VPNs are of two types:

A) REMOTE ACCESS

This is a user to LAN connection used for the employees who need to connect to the internal network of the organization from various remote locations. A remote access VPN allows individual users to establish secure connections with a remote computer network, and access the secure resources on that network as if they were directly plugged in to the network's servers.

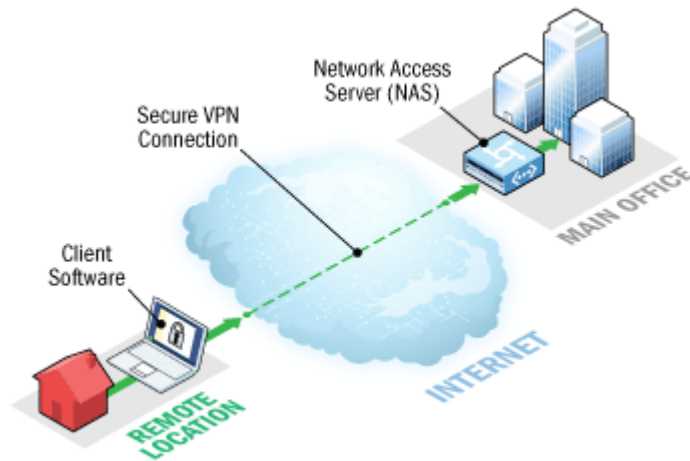


Figure 2.1(a) – Remote Access Virtual Private Network

B) SITE-TO-SITE

A site-to-site VPN allows branches in multiple locations to establish secure connections with each other over a public network, making the resources from one location available to employees at other locations.

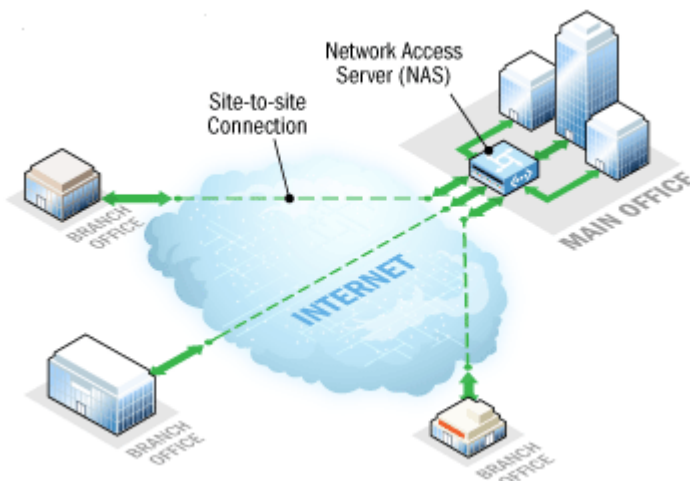


Figure 2.1(b) – Site-to-site Virtual Private Network

The advantages offered by VPN are discussed in the following section:

1) Data Confidentiality

Private data of a network travels over a public network, hence data confidentiality is vital and can be attained by encrypting the data. This is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.

2) Data Integrity

While it is important that data is encrypted over a public network, it is just as important to verify that it has not been changed while in transit. For example, IPsec has a mechanism to ensure that the encrypted portion of the packet, or the entire header and data portion of the packet, has not been tampered with. If tampering is detected, the packet is dropped. Data integrity can also involve authenticating the remote peer.

3) Data Origin Authentication

It is extremely important to verify the identity of the source of the data that is sent. This is necessary to guard against a number of attacks that depend on spoofing the identity of the sender.

4) Data Tunneling / Traffic Flow Confidentiality

Tunneling is the process of encapsulating an entire packet within another packet and sending it over a network. Data tunneling is helpful in cases where it is desirable to hide the identity of the device originating the traffic. Traffic flow confidentiality is the service that conceals source and destination addresses, message length, or frequency of communication.

5) AAA(Authentication, Authorization and Accounting)

With user authentication however, a valid username and password also has to be entered before the connection is completed.

When a request to establish a tunnel comes in from a dial-up client, the VPN device prompts for a username and password. This can then be authenticated locally or sent to the external AAA server, which checks:

Who you are (Authentication)

What you are allowed to do (Authorization)

What you actually do (Accounting)

The Accounting information is especially useful for tracking client use for security auditing, billing or reporting purpose.

2.7) FRAME RELAY

Frame Relay is a packet-switched technology, which allows multiple sites of an organization, located within a few kilometers, to connect. All the locations plug into the frame relay “cloud”, which is usually a conglomeration of dozens or hundreds of Frame-Relay switches and routers. User devices are referred to as data terminal equipment (DTE), and the network equipment in the

cloud that interfaces to DTE is referred to as data circuit-terminating equipment (DCE). Unlike Ethernet switches, which make decisions based on MAC addresses, Frame Relay switches make decisions based on Data Link Connection Interfaces (DLCIs). For communication to occur between locations, virtual circuits (VC) must be created, which is a one-way path through the Frame-Relay cloud. Virtual circuits are identified with DLCIs.

These circuits are of two types:

1) **SWITCHED VIRTUAL CIRCUIT (SVC)**

It is created only when traffic needs to be sent, and is torn down when communication is complete. SVCs are used in situations where data transmission is sporadic and the allocated resources are not intended to be bound for a given virtual circuit.

2) **PERMANENT VIRTUAL CIRCUIT (PVC)**

It is always kept active, and is the most commonly used virtual circuit. The virtual circuit values are manual. The route through the network, link-by-link is also manual. If the equipment happens to fail, the PVC also fails, and the physical network has to be re-routed. The permanent virtual circuit is an efficient circuit for hosts which have to communicate frequently like ATMs [16].

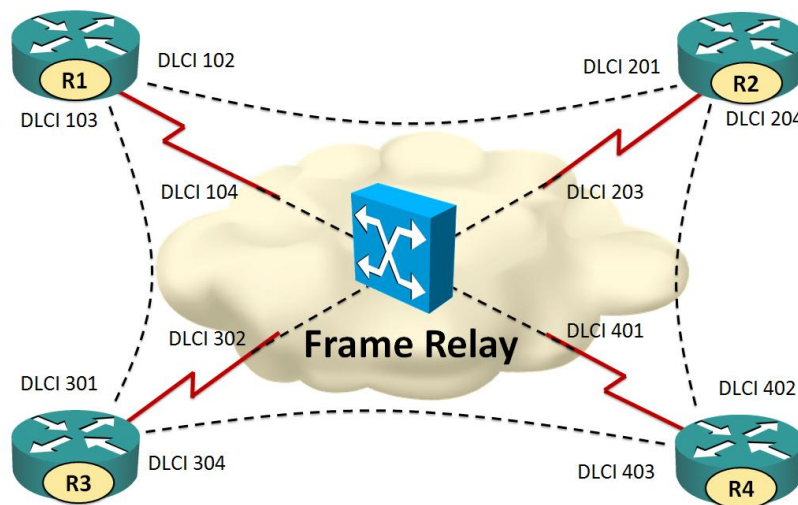


Figure 2.2 – Basic Frame Relay Structure

The extreme simplicity of configuring user equipment in a Frame Relay network is the reason for Frame Relay's popularity.

2.8) PORT SECURITY

Port security is a mechanism available on the switches to restrict the devices that can connect via a particular port of the switch. A port set up for port security only allows machines with a MAC address belonging to the range configured on it to connect to the LAN. The port compares the MAC address of any frame arriving on it with the MAC addresses configured in its allowed list. If the addresses match, it allows the packet to go through. If the MAC address does not belong to the configured list, the port can either simply drop the packet or shut itself down for a configurable amount of time. This feature also lets you specify the number of MAC addresses that can connect to a certain port [1].

2.9) ETHER CHANNEL

Ether Channel technology, built upon 802.3 full-duplex Fast Ethernet standard, allows grouping of multiple ports into a single logical transmission path between a switch and a router, server, or another switch. It provides two advantages in a network, which are described below:

- 1) It makes fair distribution of traffic between the channels, and thus, the data gets transmitted in lesser amount of time.
- 2) The technology provides redundancy in the event of link failure. If a link is cut in an Ether Channel, traffic is rerouted to one of the other links in less than a few milliseconds [1].

Under normal conditions, all but one redundant physical link between two switches will be disabled by STP at one end. With EtherChannel configured, multiple links are grouped into a port-channel, which is assigned its own configurable virtual interface. The bundle is treated as a single link.

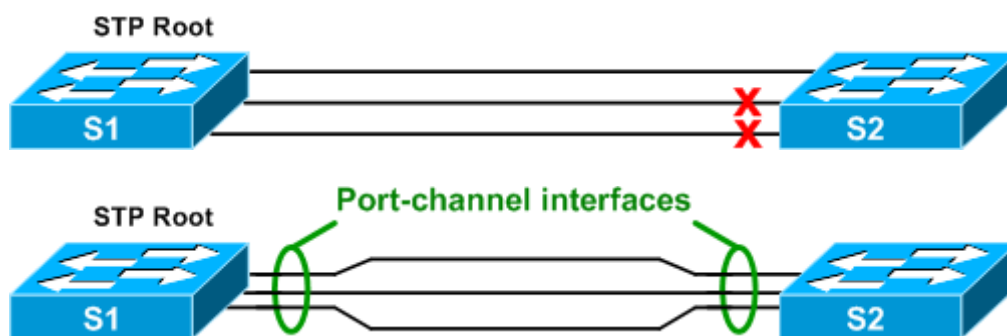


Figure 2.3 – Connected switches without and with Ether Channels

The Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) facilitate the automatic creation of Ether Channels by exchanging packets between Ethernet interfaces.

PAgP is a Cisco-proprietary protocol that can be run only on Cisco switches and on those switches licensed by licensed vendors to support PAgP. LACP is defined in IEEE 802.3AD and allows Cisco switches to manage Ethernet channels between switches that conform to the 802.3AD protocol.

To configure an Ether Channel using LACP negotiation, each side must be set to either active or passive; only interfaces configured in active mode will attempt to negotiate an Ether Channel. Passive interfaces merely respond to LACP requests. PAgP behaves the same, but its two modes are referred to as desirable and auto respectively.

2.10) FIREWALL

Firewall is either hardware or software based security mechanism in a network. As a check point gateway, it analyses the IP packets and decides whether to allow through or not, based on the preconfigured rules. It also determines which information or services to be accessed from outside as well as from inside and by whom. The firewall is helpful for packet inspection, security policy implementation, generation of the audit system and log messages.

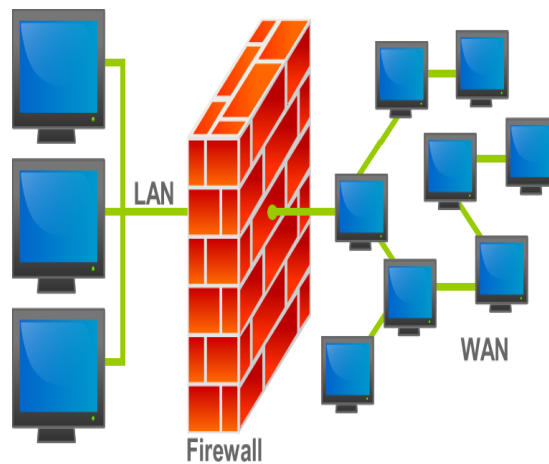


Figure 2.4 – Basic functionality of a Firewall

There exist two types of firewalls, which are discussed below:

1) HARDWARE BASED

It is a dedicated device with its own operating system on a specialized platform. It uses packet filtering to examine the header of a packet to determine its source and destination. They can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers.

2) SOFTWARE BASED

Also known as Access Control List (ACL), it is an additional program loaded on a network device like a router to inspect data or network traffic. It has been discussed in detail in the following section.

2.11) ACCESS CONTROL LIST

As discussed in the previous section, an ACL is a software based firewall. Such a list is capable of filtering network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. The router, with ACL configured on it, examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists.

Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

Some of the universal facts about access control list are:

- ACLs come in two varieties: Numbered and Named
- Each of these references to ACLs supports two types of filtering: **Standard** and **Extended**.
- Standard IP ACLs can filter only on the source IP address inside a packet.
- Whereas an extended IP ACLs can filter on the source and destination IP addresses in the packet.
- There are two actions an ACL can take: **Permit** or **Deny**.
- Once a match is found, no further statements are processed—therefore, order is important.
- If no match is found, the imaginary implicit deny statement at the end of the ACL drops the packet.

An ACL should have at least one permit statement, otherwise, all traffic will be dropped because of the hidden implicit deny statement at the end of every ACL.

2.13) LAN DESIGN

To devise the architecture of a LAN, hierarchical model is employed. This model uses layers, which simplifies the task required for internetworking along with ease of understanding and fault isolation. The Layered Approach stretches up to three layers:

A) **ACCESS LAYER**

The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs,

and wireless access points. The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network.

B) AGGREGATION LAYER

The aggregation layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer.

3) CORE LAYER

The core layer of the hierarchical design is the high-speed backbone of the internetwork. The core layer is critical for interconnectivity between distribution layer devices, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

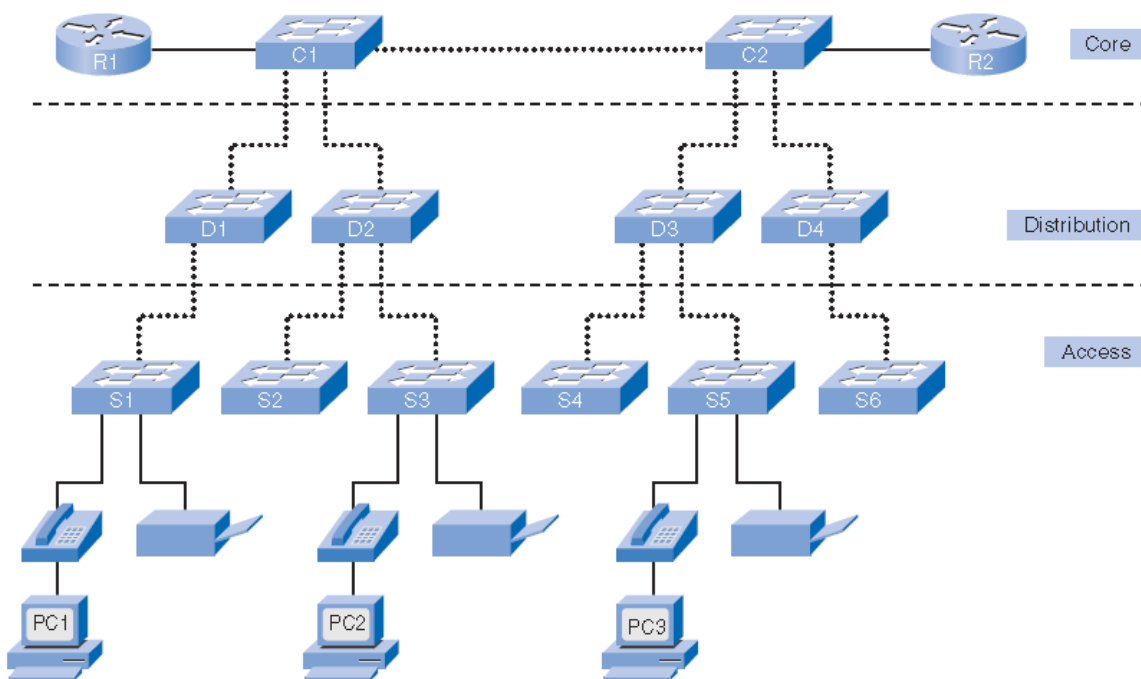


Figure 2.5 - Basic LAN Framework

Some of the benefits associated with hierarchical network design are:

- **Scalability**

Hierarchical networks scale very well. The modularity of the design allows one to replicate design elements as the network grows.

As each instance of the module is consistent, expansion is easy to plan and implement.

- **Redundancy**

As a network grows, availability becomes more important, which can be dramatically increased through easy redundant implementations with hierarchical networks. Access layer switches are connected to two different distribution layer switches to ensure path redundancy. If one of the distribution layer switches fails, the access layer switch can switch to the other distribution layer switch. Additionally, distribution layer switches are connected to two or more core layer switches to ensure path availability if a core switch fails.

- **Performance**

Communication performance is enhanced by avoiding the transmission of data through low performing, intermediary switches. Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases. The distribution layer then uses its high-performance switching capabilities to forward the traffic up to the core, where it is routed to its final destination.

- **Security**

Security is improved and easier to manage. Access layer switches can be configured with various port security options that provide control over which devices are allowed to connect to the network. Some more advanced security policies are available at the distribution layer.

- **Manageability**

Manageability is relatively simple on a hierarchical network. Each layer of the hierarchical design performs specific functions that are consistent throughout that layer. Therefore, if it is required to change the functionality of an access layer switch, the change can be repeated across all access layer switches in the network because they presumably perform the same functions at their layer. Deployment of new switches is also simplified because switch configurations can be copied between devices with very few modifications.

- **Maintainability**

Because hierarchical networks are modular in nature and scale very easily, they are easy to maintain. With other network topology designs, maintainability becomes increasingly complicated as the network grows. Also, in some network design models, there is a finite limit to how large the network can grow before it becomes too complicated and expensive to maintain. In the hierarchical design model, switch functions are defined at each layer, making the selection of the correct switch easier.

CHAPTER – 3

CAMPUS NETWORK ARCHITECTURE DESIGN

3.1) PROPOSED NETWORK ARCHITECTURE

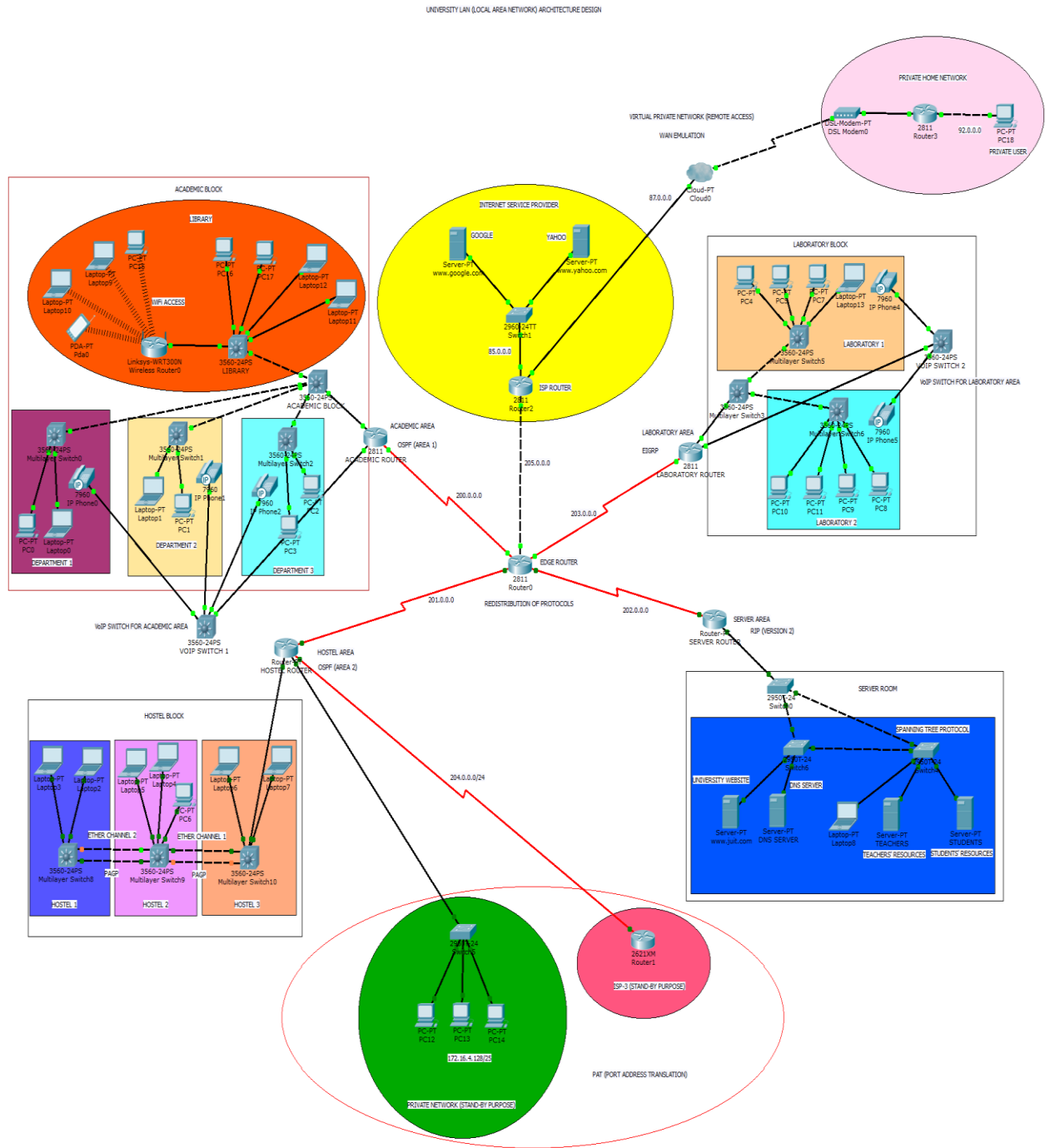


Figure 3.1 – Network Architecture proposed as an enhancement to the existing network of JUIT

A detailed description of the above network design has been presented as follows:

- **ACADEMIC BLOCK AND HOSTEL AREA**

The academic block is the area where all the different departments and the library are located. It has been implemented with the OSPF (Open Shortest Path First) routing protocol. The ACADEMIC BLOCK is under OSPF area 1, and the HOSTEL BLOCK is under OSPF area 2. A separate switch for VoIP facility has been used, to which the IP phones for each department are connected. In the hostel block, Ether Channels have been deployed, i.e., bundling of two individual Ethernet links into a single logical link. If a link within an Ether Channel fails, traffic previously carried over the failed link switches to the second segment within the Ether Channel. The Ether Channels have been configured using the Port Aggregation Control Protocol (PAGP). The Library has been provided with Wi-Fi access.

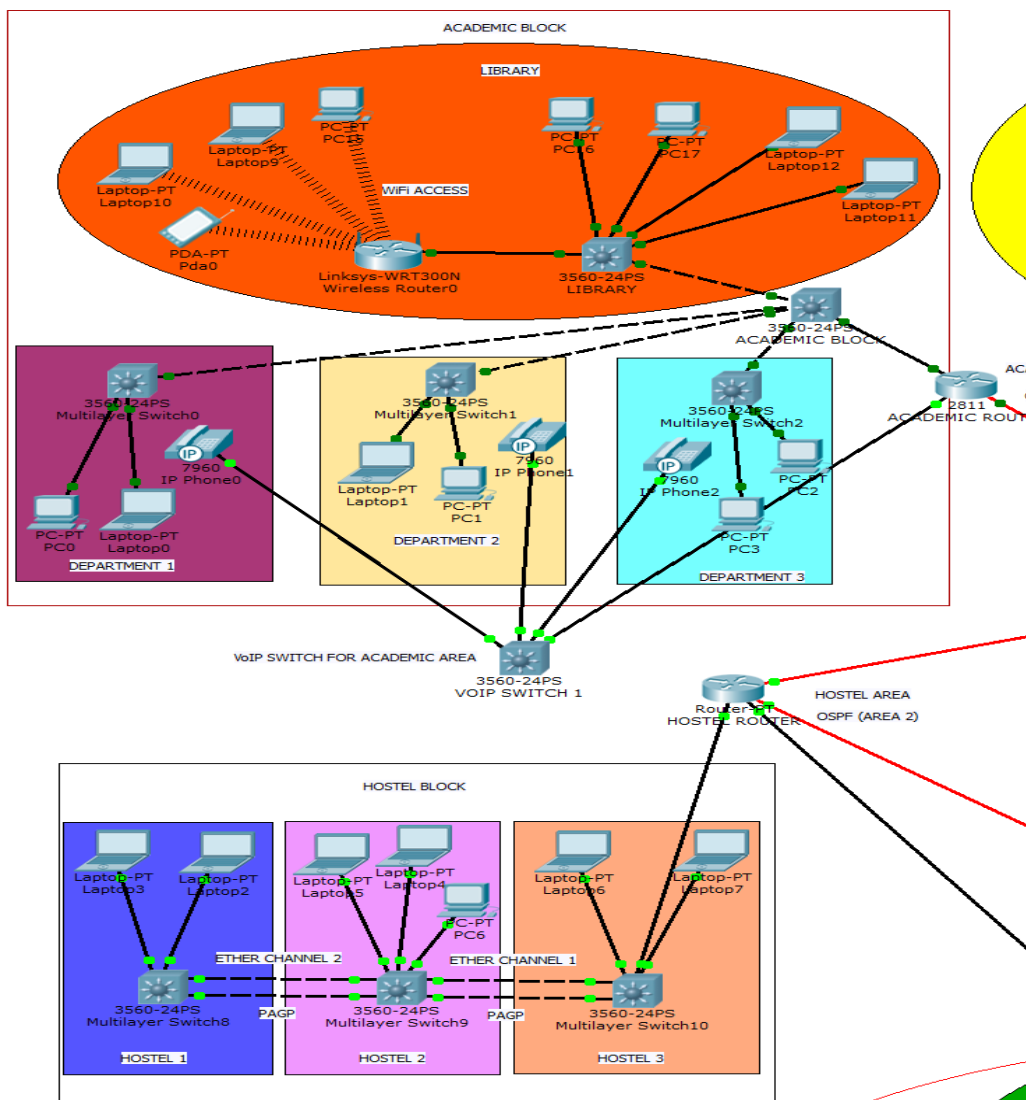


Figure 3.2- Academic block and Hostel Area

PROGRAMMING MODULES FOR ACADEMIC AREA

```
• Creation of VLAN and Trunk Port:  
Switch#configure terminal  
Switch(config)#vlan 2  
Switch(config-vlan)#name DEPARTMENT_1  
Switch(config-vlan)#exit  
Switch(config)#interface range f0/2, f0/24  
Switch(config-if-range)#switchport access vlan 2  
Switch(config-if-range)#exit  
Switch(config)#vlan 3  
Switch(config-vlan)#name DEPARTMENT_2  
Switch(config-vlan)#exit  
Switch(config)#interface range f0/3, f0/23  
Switch(config-if-range)#switchport access vlan 3  
Switch(config-if-range)#exit  
Switch(config)#vlan 4  
Switch(config-vlan)#name DEPARTMENT_3  
Switch(config-vlan)#exit  
Switch(config)#interface range f0/4, f0/22  
Switch(config-if-range)#switchport access vlan 4  
Switch(config-if-range)#exit  
Switch(config)#vlan 10  
Switch(config-vlan)#name LIBRARY  
Switch(config-vlan)#exit  
Switch(config)#interface range f0/5, f0/21  
Switch(config-if-range)#switchport access vlan 10  
Switch(config-if-range)#exit  
Switch(config)#int f0/1  
Switch(config-if)#switchport trunk encapsulation dot1q  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#exit
```

Figure 3.3 – Configuration for VLAN and Trunk Port

```
• Creating sub-interfaces on the router:  
Router#conf t  
Router(config)#int f0/0  
Router(config-if)#no ip address  
Router(config-if)#no shut  
Router(config-if)#exit  
Router(config)#int f0/0.1  
Router(config-subif)#encapsulation dot1q 2  
Router(config-subif)#ip address 172.16.0.1 255.255.255.128  
Router(config-subif)#exit  
Router(config)#int f0/0.2  
Router(config-subif)#encapsulation dot1q 3  
Router(config-subif)#ip address 172.16.0.129 255.255.255.128  
Router(config-subif)#exit  
Router(config)#int f0/0.3  
Router(config-subif)#encapsulation dot1q 4  
Router(config-subif)#ip address 172.16.1.1 255.255.255.128  
Router(config-subif)#exit  
Router(config)#int f0/0.4  
Router(config-subif)#encapsulation dot1q 10  
Router(config-subif)#ip address 172.16.5.1 255.255.255.128  
Router(config-subif)#exit
```

Figure 3.4 – Configuration for Sub-interface

- **Creating DHCP pools:**

```

Router(config)#ip dhcp pool dep1
Router(dhcp-config)#network 172.16.0.0 255.255.255.128
Router(dhcp-config)#default-router 172.16.0.1
Router(dhcp-config)#dns-server 172.16.4.11
Router(dhcp-config)#exit
Router(config)#ip dhcp pool dep2
Router(dhcp-config)#network 172.16.0.128 255.255.255.128
Router(dhcp-config)#default-router 172.16.0.129
Router(dhcp-config)#dns-server 172.16.4.11
Router(dhcp-config)#exit
Router(config)#ip dhcp pool dep3
Router(dhcp-config)#network 172.16.1.0 255.255.255.128
Router(dhcp-config)#default-router 172.16.1.1
Router(dhcp-config)#dns-server 172.16.4.11
Router(dhcp-config)#exit
Router(config)#ip dhcp pool library
Router(dhcp-config)#network 172.16.5.0 255.255.255.128
Router(dhcp-config)#default-router 172.16.5.1
Router(dhcp-config)#dns-server 172.16.4.11
Router(dhcp-config)#exit

```

Figure 3.5 – Configuration for DHCP

- **Routing – OSPF:**

```

Router(config)#router ospf 1
Router(config-router)#network 172.16.0.0.0.0.0.127 area 0
Router(config-router)#network 172.16.0.128 0.0.0.127 area 0
Router(config-router)#network 172.16.1.0.0.0.0.127 area 0
Router(config-router)#exit

```

Figure 3.6 – Configuration for OSPF

- **Creation of VLANs and Trunk Port:**

```

Switch#conf t
Switch(config)#vlan 11
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch(config)#vlan 12
Switch(config-vlan)#name data
Switch(config-vlan)#exit
Switch(config)#interface range f0/2, f0/24
Switch(config-if-range)#switchport voice vlan 11
Switch(config-if-range)#switchport access vlan 12
Switch(config-if-range)#exit
Switch(config)#interface range f0/3-4
Switch(config-if-range)#switchport voice vlan 11
Switch(config-if-range)#switchport access vlan 12
Switch(config-if-range)#exit
Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit

```

Figure 3.7 – VoIP - Configuration for VLAN and Trunk Port

- **Creating sub-interfaces :**

```

Router#conf t
Router(config)#interface f0/1
Router(config-if)#no ip address
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int f0/1.1
Router(config-subif)#encapsulation dot1q 11
Router(config-subif)#ip address 10.0.0.1 255.0.0.0
Router(config-subif)#exit
Router(config)#int f0/1.2
Router(config-subif)#encapsulation dot1q 12
Router(config-subif)#ip address 20.0.0.1 255.0.0.0
Router(config-subif)#exit

```

Figure 3.8 – VoIP – Configuration for Sub-interfaces

- **Creating DHCP Pool:**

```

Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 10.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 10.0.0.1
Router(dhcp-config)#option 150 ip 10.0.0.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 20.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 20.0.0.1
Router(dhcp-config)#exit

```

Figure 3.9 – VoIP – Configuration for DHCP Pool

- **Registration of IP Phones:**

```

Router#conf t
Router(config)#telephony-service
Router(config-telephony)#no auto-reg-ephone
Router(config-telephony)#ip source-address 10.0.0.1 port 2000
Router(config-telephony)#max-ephones 10
Router(config-telephony)#max-dn 100
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 1000
Router(config-ephone-dn)#exit
Router(config)#ephone 1
Router(config-ephone)#mac-address 0009.7C08.C930
Router(config-ephone)#exit

```

Figure 3.10 – VoIP – Configuration for registration of IP Phone

- **Enabling inter-network IP Phone calling:**

```

Router#conf t
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern ....
Router(config-dial-peer)#session target ipv4:200.0.0.1
Router(config-dial-peer)#exit

```

Figure 3.11 – VoIP – Configuration for enabling inter-network IP Phone calling

- **Adding the networks to routing:**
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router(config-router)#network 20.0.0.0 0.0.0.255 area 0
Router(config-router)#exit

Figure 3.12 – VoIP – Configuration for OSPF

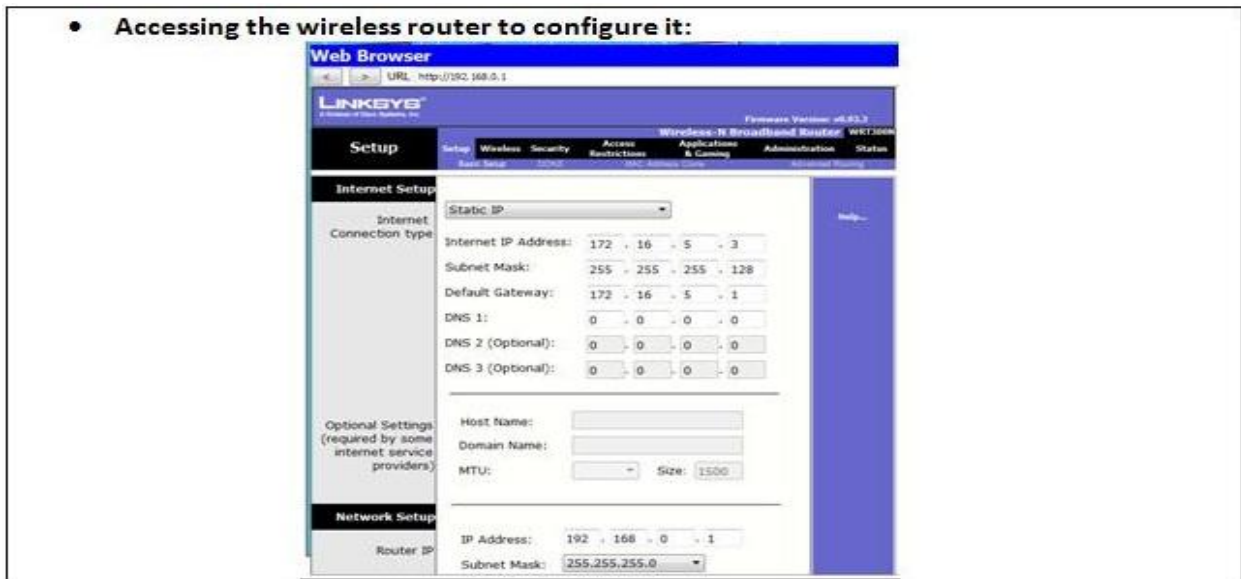


Figure 3.13 – Wireless Router – Configuration for LAN side of the router

- **Turning ON the link to WAN side of the Wireless Router:**
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#exit
- **Adding the network to routing:**
Router(config)#router ospf 1
Router(config-router)#network 172.16.5.0 0.0.0.127 area 0
Router(config-router)#exit

Figure 3.14 – Wireless Router – Configuration for the link connecting to WAN

• **LABORATORY AREA**

The laboratory area is the area where the campus' laboratories are located. It has been kept under EIGRP (Enhanced Interior Gateway Routing Protocol). A separate switch for VoIP facility has been used, to which the IP phones for each laboratory are connected.

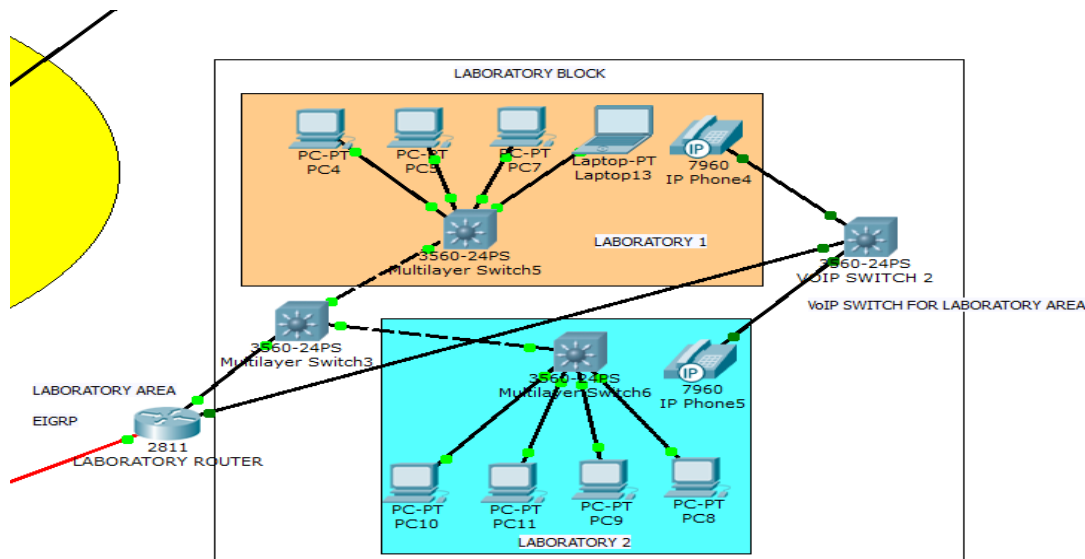


Figure 3.15 – Laboratory Block

PROGRAMMING MODULE FOR LABORATORY AREA

- **Routing – EIGRP:**

```

Router(config)#router eigrp 2
Router(config-router)#network 172.16.1.129
Router(config-router)#network 172.16.2.1
Router(config-router)#network 40.0.0.0
Router(config-router)#network 50.0.0.0
Router(config-router)#no auto-summary

```

Figure 3.16 – Configuration for EIGRP on laboratory router

• SERVER ROOM

The campus' server room is the area where all the servers supporting the campus' network have been placed. It is running on RIPv2 (Routing Information Protocol version 2). The first server is for the university's website (www.juit.com), second is the DNS server, third is the teachers' resources server, where the faculty would store their personal resources, and the fourth is the students' resources server, where the students would store their personal resources. To provide uninterrupted access to the servers even in situations where any one of the paths goes down, a redundant path has been provided which has been automatically blocked by STP (Spanning Tree Protocol), to avoid loop formation.

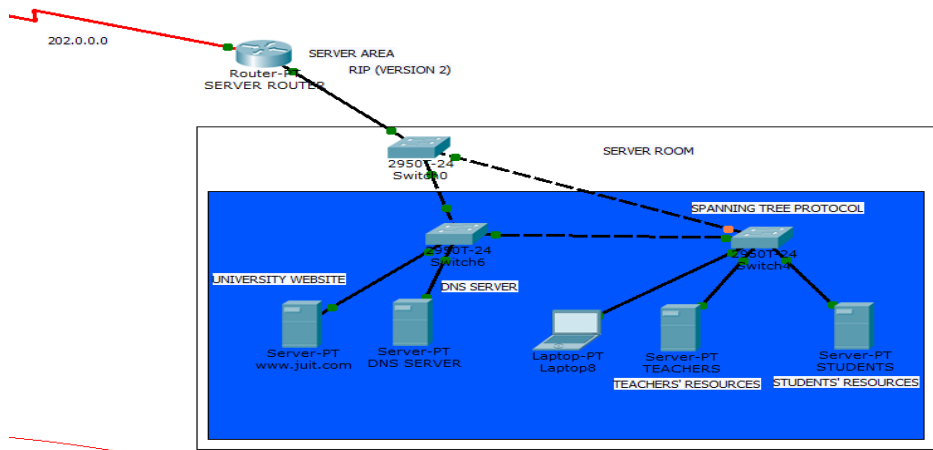


Figure 3.17 – Server Room

PROGRAMMING MODULES FOR SERVER ROOM

- **Configuration of HTTP Server (University's Website):**

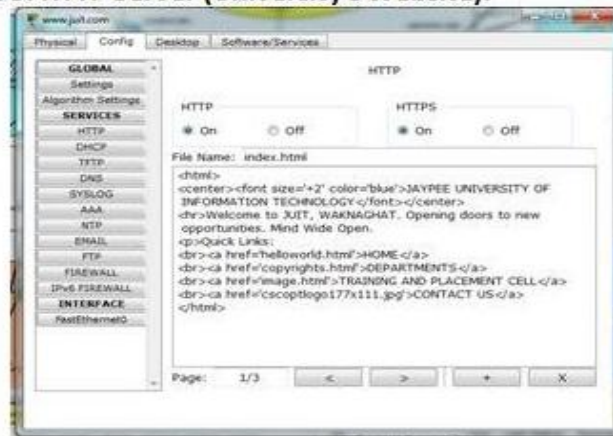


Figure 3.18 – Configuration for HTTP server

- **Configuration of FTP Server (Students' Resources):**

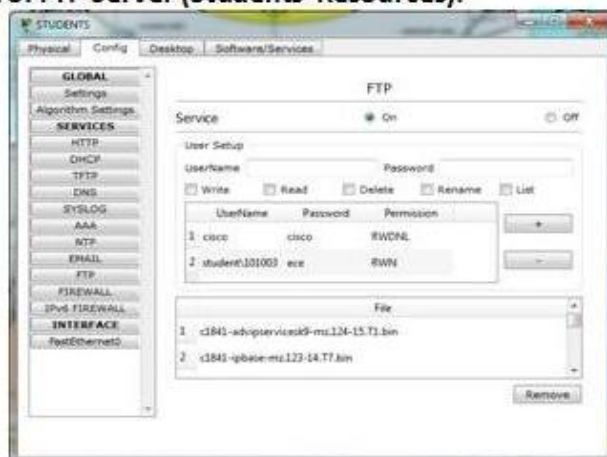


Figure 3.19 – Configuration for FTP server

- **Configuration of DNS Server:**

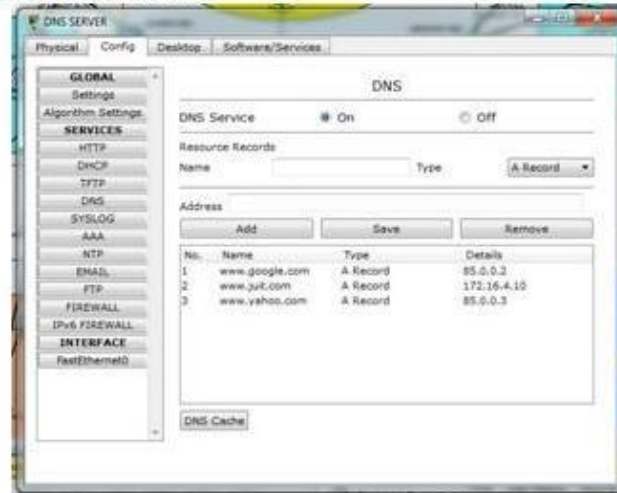


Figure 3.20 – Configuration for DNS server

- **Routing – RIP version2:**

```

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.16.4.0
Router(config-router)#exit
  
```

Figure 3.21 – Configuration for RIPv2 on Server Router

- **REDISTRIBUTION ON CENTRAL ROUTER**

As the design is based on a multiple protocol environment, redistribution is a necessity, and has been implemented on the edge router, to make communication between the three different protocols, i.e. OSPF, EIGRP and RIPv2 possible.

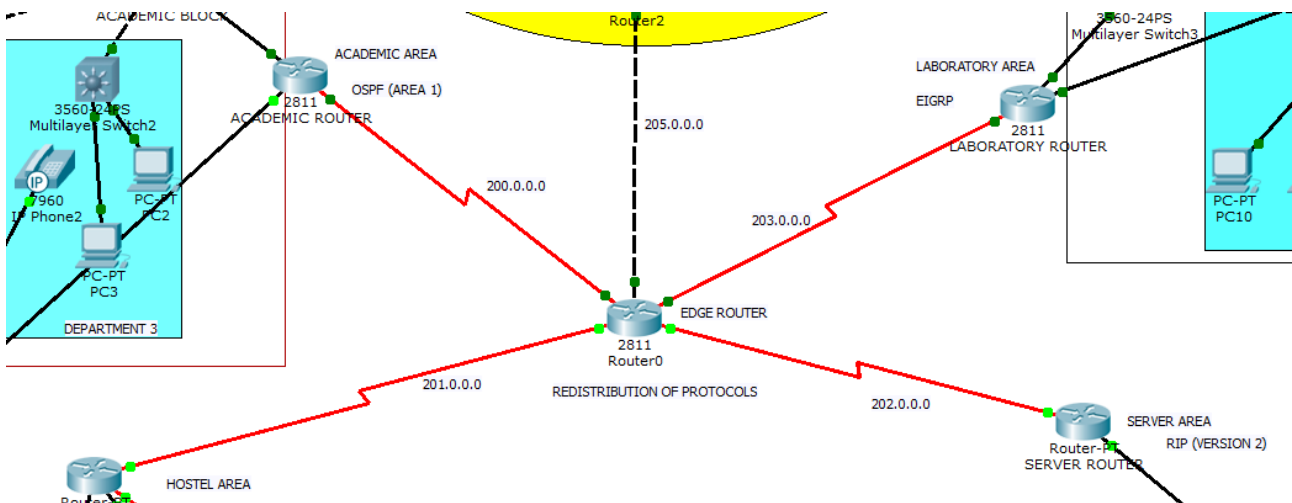


Figure 3.22- Edge Router and its connections to different areas

PROGRAMMING MODULES FOR EDGE ROUTER

```

• Adding the networks leading to various areas to their respective routing:
Router(config)#router ospf 1
Router(config-router)#network 200.0.0.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#router ospf 2
Router(config-router)#network 201.0.0.0 0.0.0.255 area 1
Router(config-router)#exit

• Redistribution of Routing Protocols:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#redistribute ospf 3 metric 2
Router(config-router)#redistribute eigrp 2 metric 2
Router(config-router)#exit
  
```

Figure 3.23 – Configuration for redistribution on central router

• PAT (PORT ADDRESS TRANSLATION)

To tackle a catastrophic situation in which the connection to the primary ISP breaks down, a stand-by private network with an exclusive connection to a redundant ISP has been set-up. This private network will be used for internet access in emergency situations. The private network can communicate with the rest of the campus' network, but the redundant ISP is accessible only through the private network. PAT has been implemented here, i.e. the private IP network 172.16.4.128/25 has been translated to the public IP network 204.0.0.0/24.

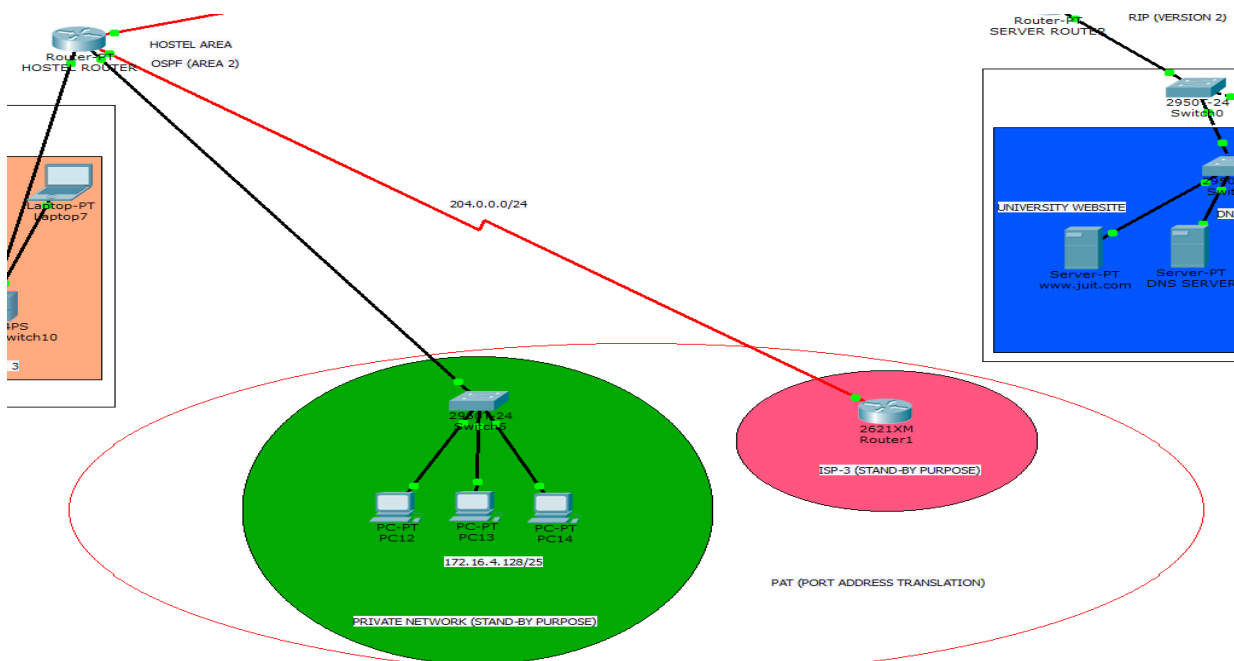


Figure 3.24 – Redundant ISP Block

- **Assigning IP address to the interface connecting the network:**

```
Router#conf t
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 172.16.4.129 255.255.255.128
Router(config-if)#no shut
```
- **Creating DHCP pool for the network:**

```
Router(config)#ip dhcp pool stand-by
Router(dhcp-config)#network 172.16.4.128 255.255.255.128
Router(dhcp-config)#default-router 172.16.4.129
Router(dhcp-config)#exit
```
- **Defining NAT pool and access restriction for the Redundant ISP:**

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat pool stand_by 204.0.0.1 204.0.0.1 netmask 255.255.255.252
Router(config)#access-list 50 permit 172.16.4.128 0.0.0.128
Router(config)#ip nat inside source list 50 pool stand_by overload
Router(config)#interface f1/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface s3/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Figure 3.25 – Configuration for NAT

- **ISP (Internet Service Provider)**

The ISP is shown by a router, switch and two servers of example websites (www.google.com, www.yahoo.com). The edge router is under OSPF area 3.

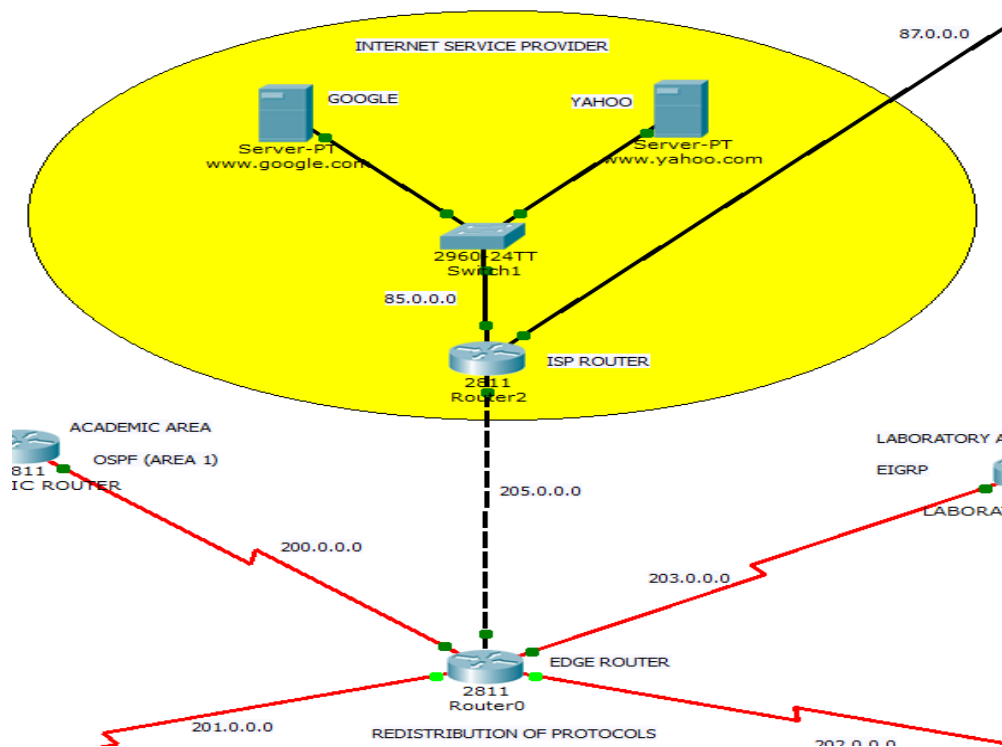
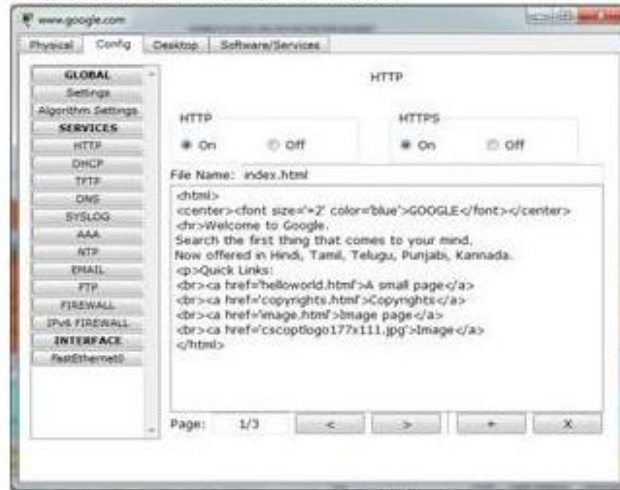


Figure 3.26- Area showing connection of ISP router and Edge router

- **Configuration of one of the website's Server:**



- **Routing – RIP version2:**

```

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 85.0.0.0
Router(config-router)#network 87.0.0.0
Router(config-router)#network 205.0.0.0
Router(config-router)#exit
  
```

Figure 3.27 – Configuration for Google Server and routing

- **Remote Access VPN (Virtual Private Network)**

The cloud is symbolic of a WAN. The private home network can be of any student/faculty of Jaypee University of Information Technology, who wants to access the students' resources/faculty resources server from outside the college's intranet. To make this service possible, Remote access VPN has been implemented.

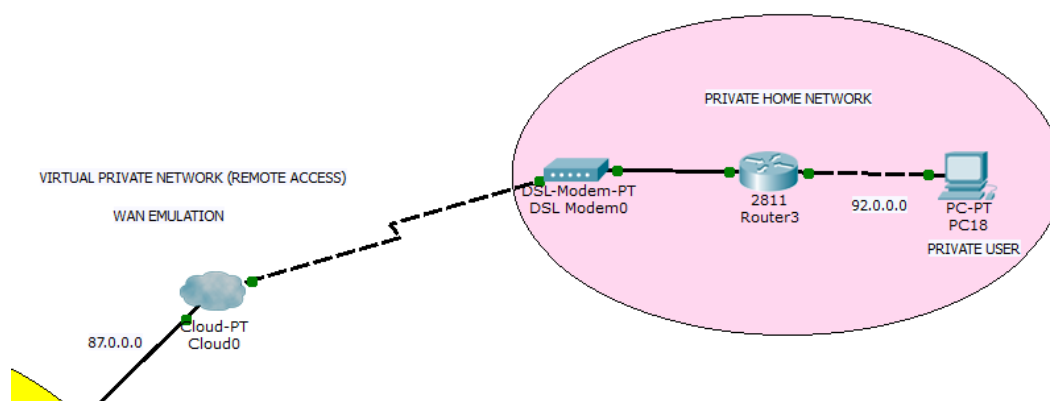


Figure 3.28 – Private Home Network

3.2) DEMONSTRATION OF THE NETWORK

The proposed architecture, when simulated on Cisco packet tracer, produced results which are demonstrated as follows:

(a). When PC2 from the Academic Block sends an ICMP message to PC10 of the Laboratory Block, the packet transfer is demonstrated as follows:

1. From PC2 to the Department 3 switch

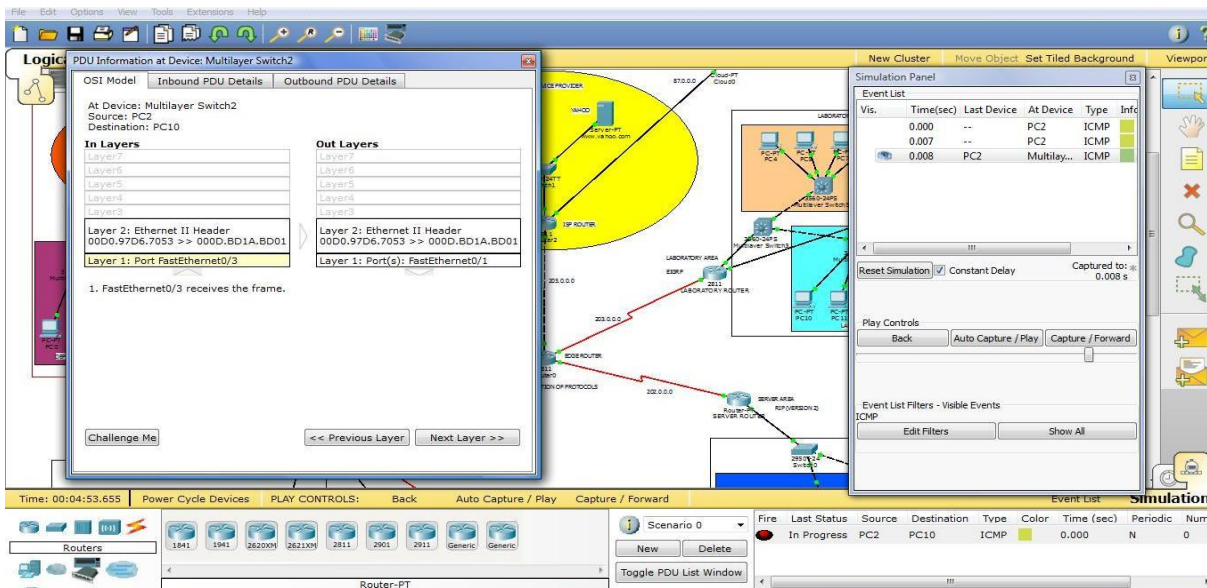


Figure 3.29 – PDU at Multilayer switch2

2. From Department 3 switch to Academic block switch

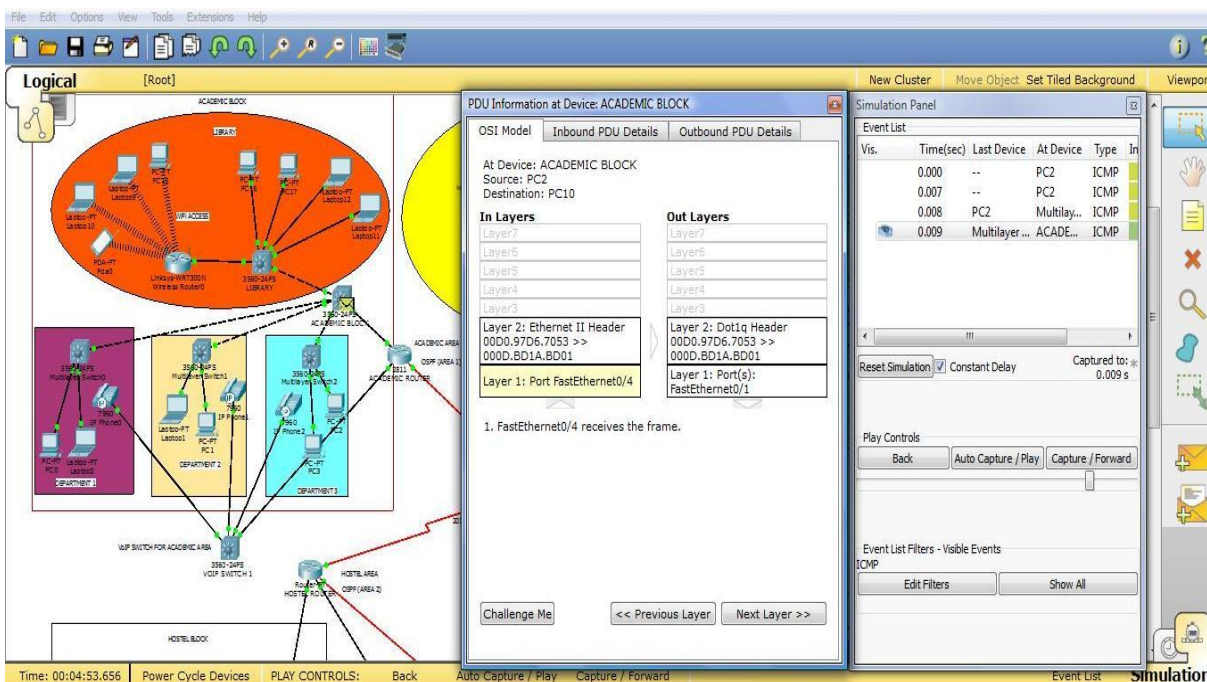


Figure 3.30 – PDU at Academic Block Switch

3. From Academic block switch to Academic router

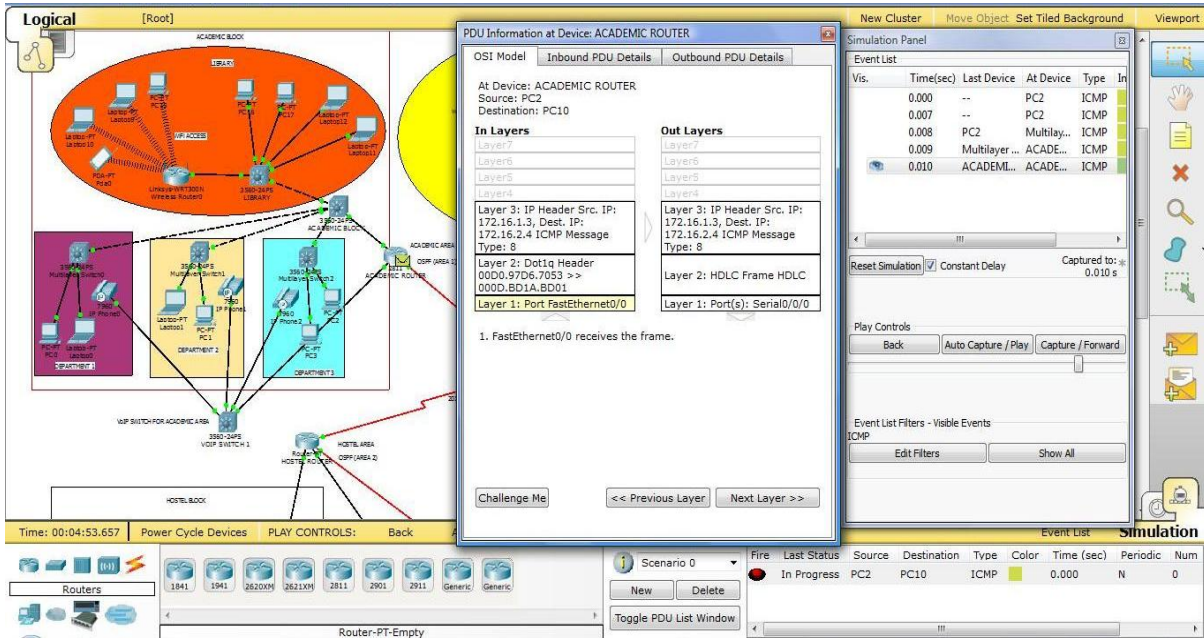


Figure 3.31 – PDU on Academic Router

4. From Academic router to Edge router

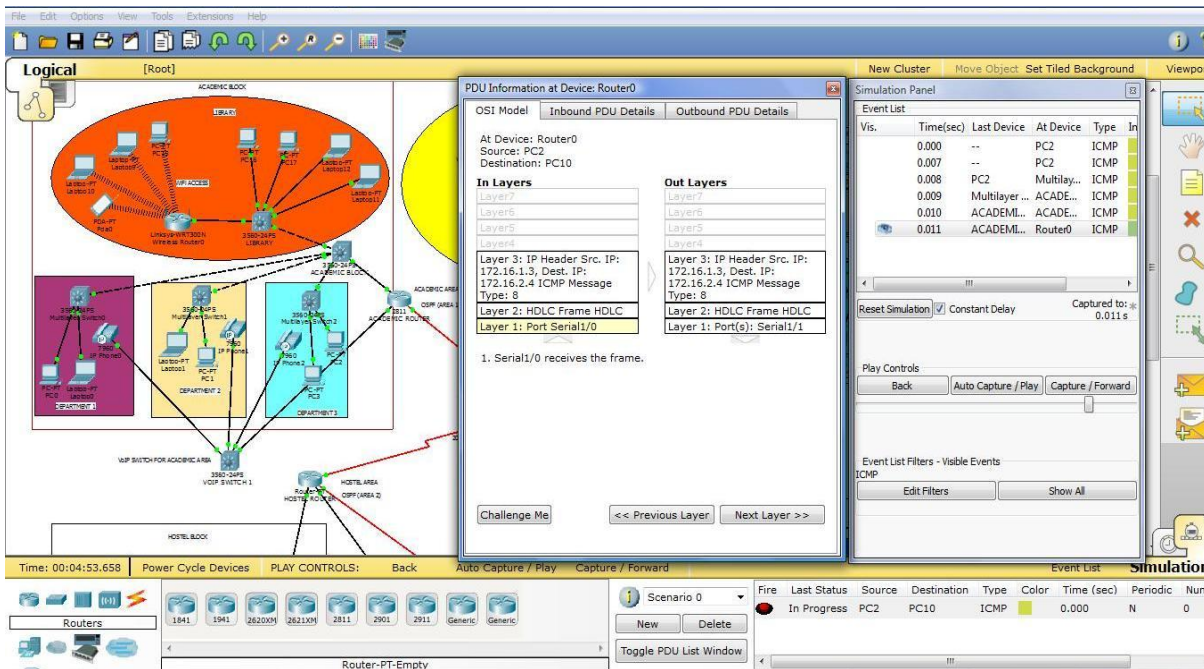


Figure 3.32 – PDU at Edge Router

5. From Edge router to Laboratory router

The screenshot displays the PDU information at the Laboratory Router. The PDU is an ICMP message from PC2 to PC10. The simulation panel shows the event list with the current event at 0.005 seconds.

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: LABORATORY ROUTER	Source: PC2 Destination: PC10	
In Layers		Out Layers
Layer7		Layer7
Layer6		Layer6
Layer5		Layer5
Layer4		Layer4
Layer3: IP Header Src. IP: 172.16.1.3, Dest. IP: 172.16.2.4 ICMP Message Type: 8		Layer3: IP Header Src. IP: 172.16.1.3, Dest. IP: 172.16.2.4 ICMP Message Type: 8
Layer 2: HDLC Frame HDLC		Layer 2: Dot1q Header 000B.BE6C.2601 >> 0001.4244.7915
Layer 1: Port Serial0/0/0		Layer 1: Port(s): FastEthernet0/0

1. Serial0/0/0 receives the frame.

Event List	Vis.	Time(sec)	Last Device	At Device	Type
0.000		--	PC2	ICMP	
0.001			PC2	Multilay...	ICMP
0.002			Multilayer...	ACADEM...	ICMP
0.003			ACADEML...	ACADEM...	ICMP
0.004			ACADEML...	Router0	ICMP
0.005			Router0	LABORA...	ICMP

Figure 3.33 – PDU at Laboratory Router

6. From Laboratory router to Laboratory block switch

The screenshot displays the PDU information at the Multilayer Switch3. The PDU is an ICMP message from PC2 to PC10. The simulation panel shows the event list with the current event at 0.006 seconds.

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: Multilayer Switch3	Source: PC2 Destination: PC10	
In Layers		Out Layers
Layer7		Layer7
Layer6		Layer6
Layer5		Layer5
Layer4		Layer4
Layer3		Layer3
Layer 2: Dot1q Header 000B.BE6C.2601 >> 0001.4244.7915		Layer 2: Ethernet II Header 000B.BE6C.2601 >> 0001.4244.7915
Layer 1: Port FastEthernet0/1		Layer 1: Port(s): FastEthernet0/3

1. FastEthernet0/1 receives the frame.

Event List	Vis.	Time(sec)	Last Device	At Device	Type
0.000		--	PC2	ICMP	
0.001			PC2	Multilay...	ICMP
0.002			Multilayer...	ACADEM...	ICMP
0.003			ACADEML...	ACADEM...	ICMP
0.004			ACADEML...	Router0	ICMP
0.005			Router0	LABORA...	ICMP
0.006			LABORAT...	Multilay...	ICMP

Figure 3.34 – PDU at Laboratory Switch

7. From Laboratory block switch to Laboratory 2 switch

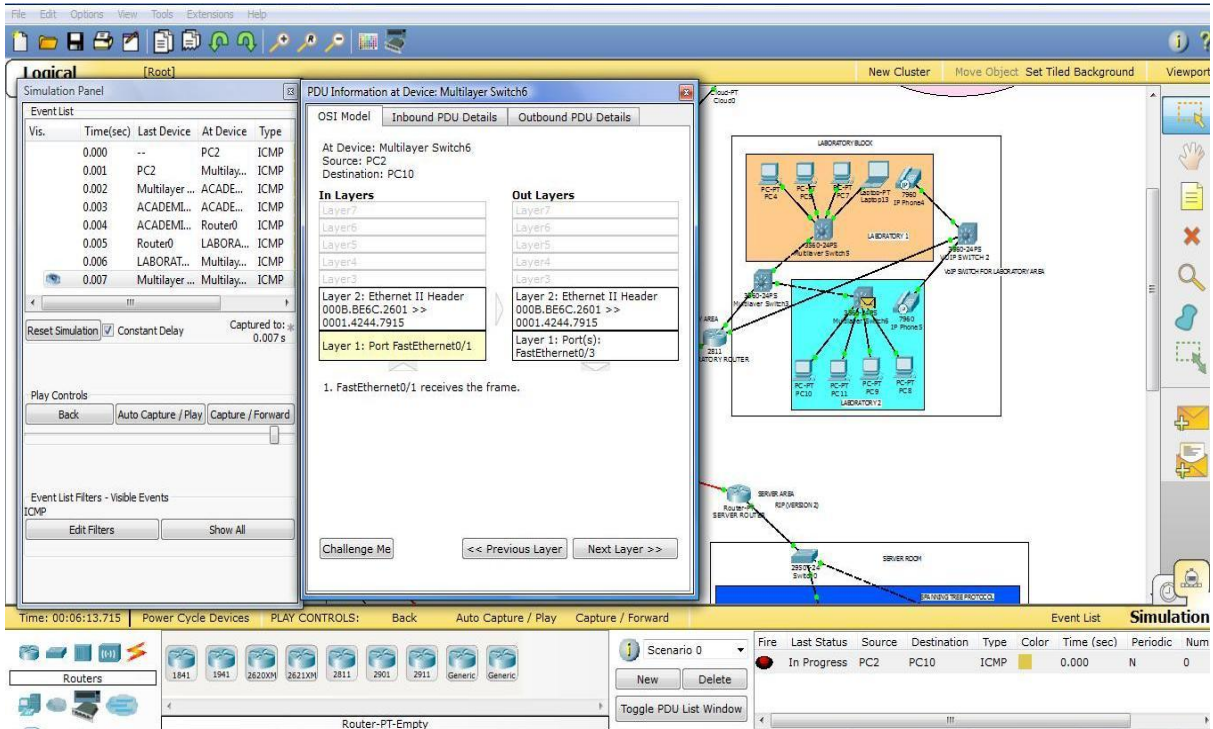


Figure 3.35 – PDU at Laboratory 2 switch

8. From Laboratory 2 switch to PC 10

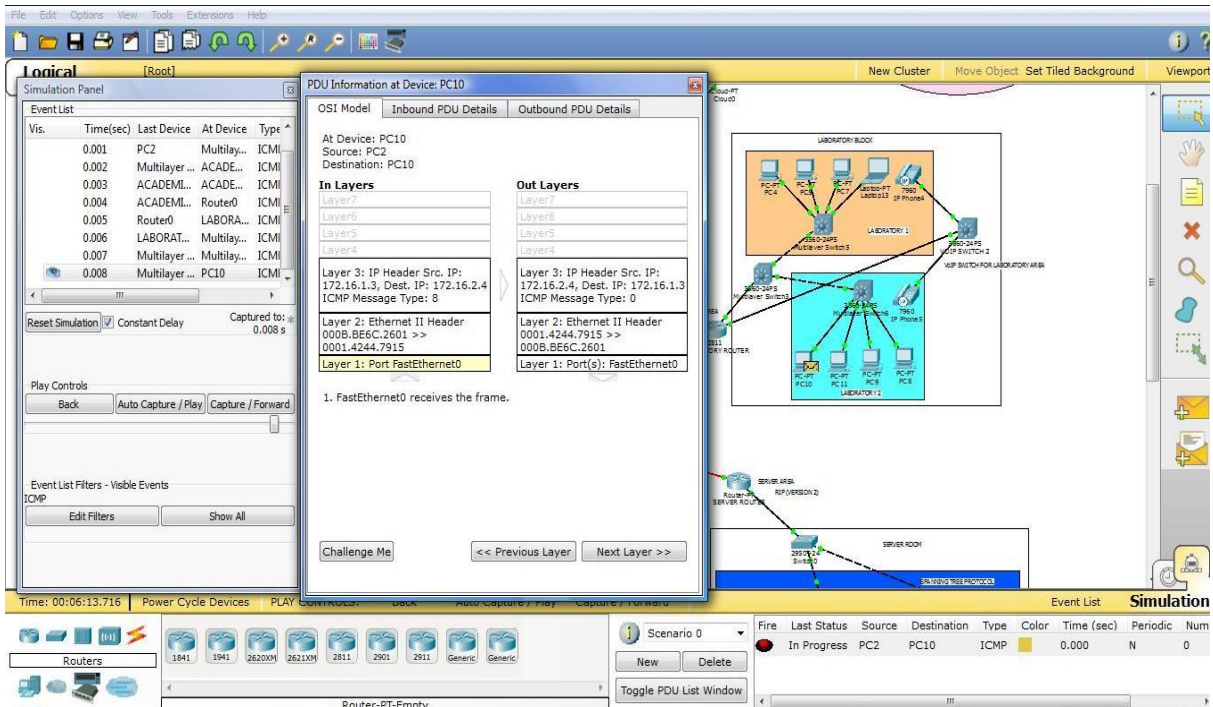


Figure 3.36 – PDU at PC10

(b) The case of a student, with an example username *student\101003* and password *ece*, trying to access the students' resources server in the campus' server room, from his private home network:

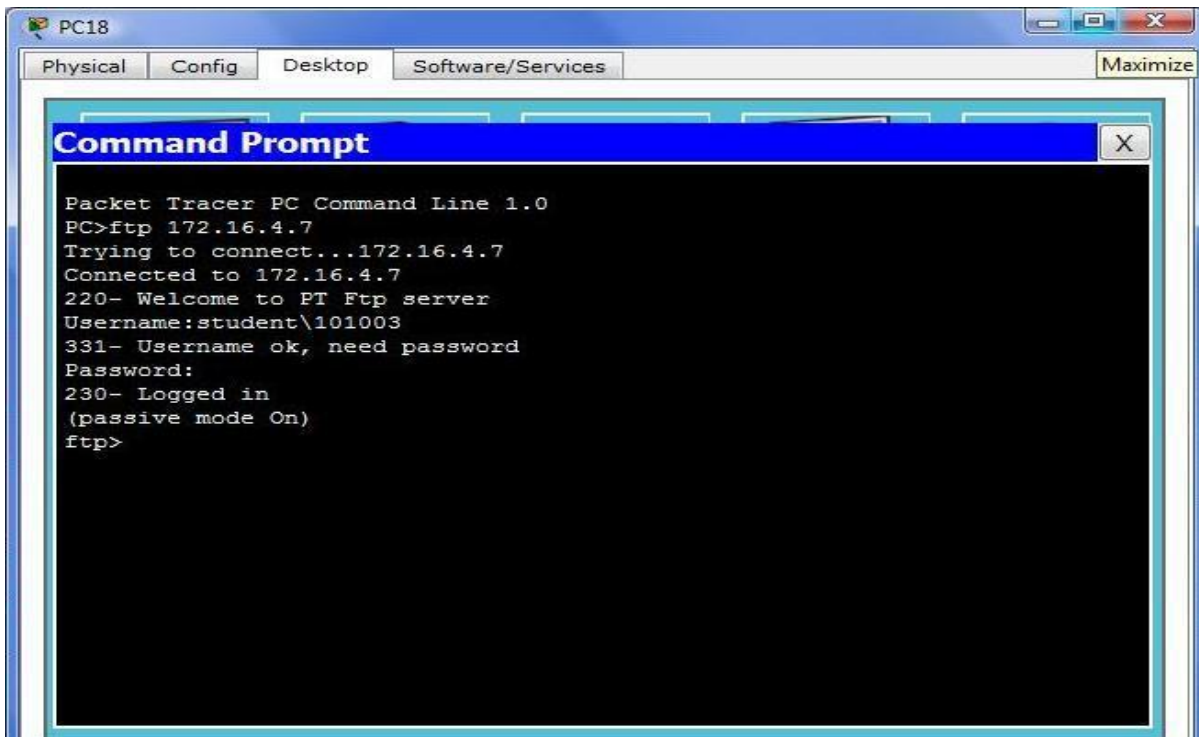


Figure 3.37 – Accessing Students' Resource

(c) The case where an IP phone user with number 1000, from department 3 of the academic block, wishes to call an IP phone user with number 4000, in laboratory 1 of the laboratory block. As redistribution of protocols on the edge router, and appropriate configurations on the academic and laboratory routers have been carried out, IP phones under different protocols and networks can communicate with each other.



Figure 3.38 – Ring going out from the IP Phone with number 1000



Figure 3.39 – IP Phones connected

3.3) CONCLUSION

Thus, concluding the description of the network in a nutshell, the Ether Channels provide link redundancy and an increase in bandwidth, thus making the network faster and more reliable. A VPN enables the students and faculty to remotely access the college's resources. In the event of a catastrophe, where the connection to the primary ISP breaks down, there exists a private connection to a redundant ISP, for access to the internet. Moreover, the feature of VoIP is advantageous as it leads to cost savings and poses no geographical boundaries. The proposed network architecture, though has higher cost of implementation as compared to the existing network of Jaypee University of Information Technology, it presents important enhancements. The design can further be improved by creating a back-up of the campus' server data, using cloud technology. Nowadays, as cloud services are being provided at reasonable prices, the university can have this alternate storage area for the important resources, so that in case of a calamity, the data can be retrieved from the cloud.

CHAPTER – 4

ENTERPRISE NETWORK ARCHITECTURE DESIGN

4.1) PROPOSED NETWORK ARCHITECTURE

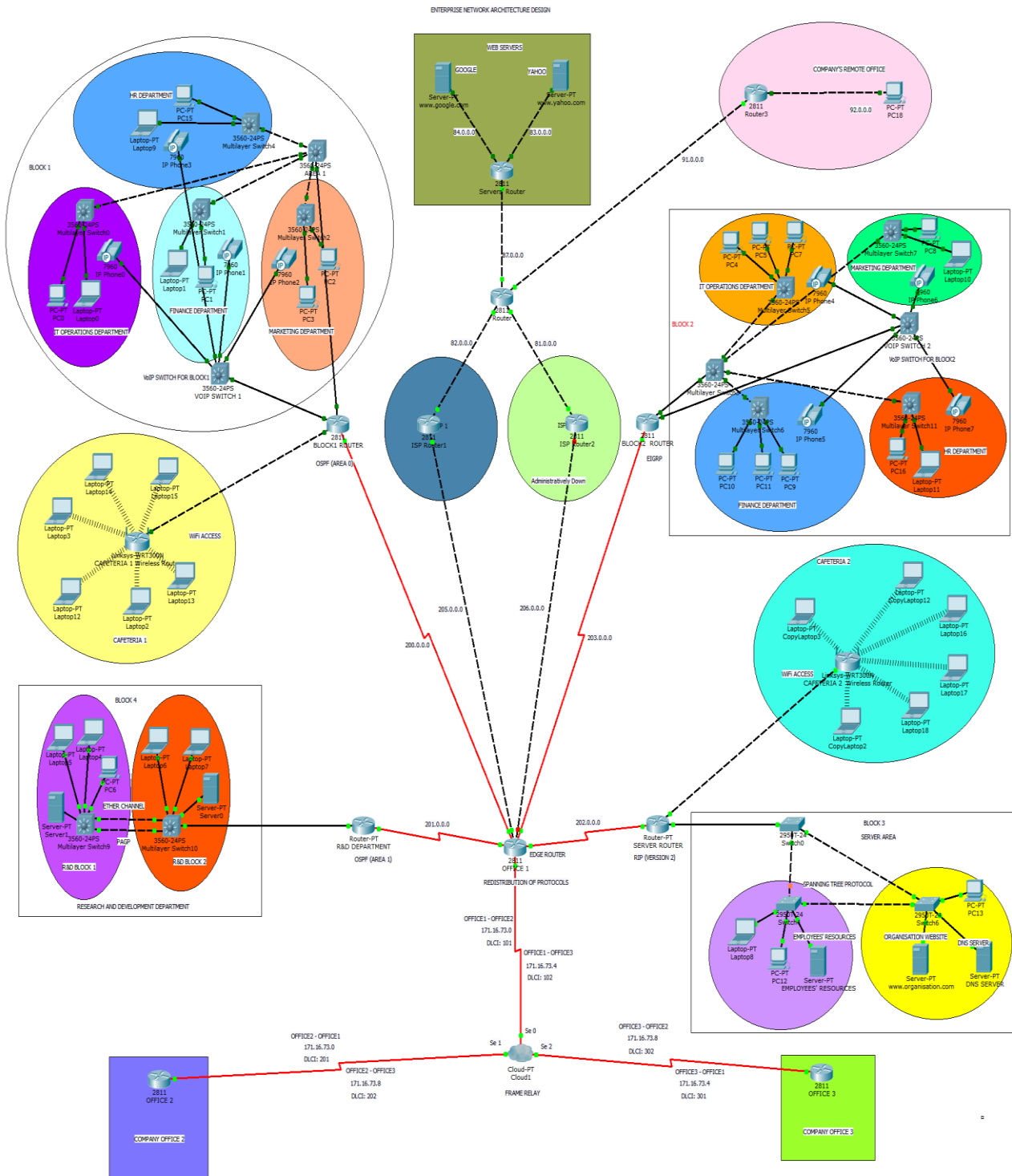


Figure 4.1 – Network design proposed for an enterprise

- **BLOCK 1**

Block 1 is the area where one leg of all the different departments, namely, IT Operations, Marketing, Human Resource, and Finance, are placed. A separate switch for VoIP facility has been used, to which the IP phones for each department are connected. Configuration for VoIP has been depicted. Cafeteria 1 is located next to Block 1, and Wi-Fi access has been provided here for conducting informal meetings and for employee recreation. OSPF (Open Shortest Path First) routing protocol has been implemented in these areas. Block 1 and Cafeteria 1 are under OSPF area 0.

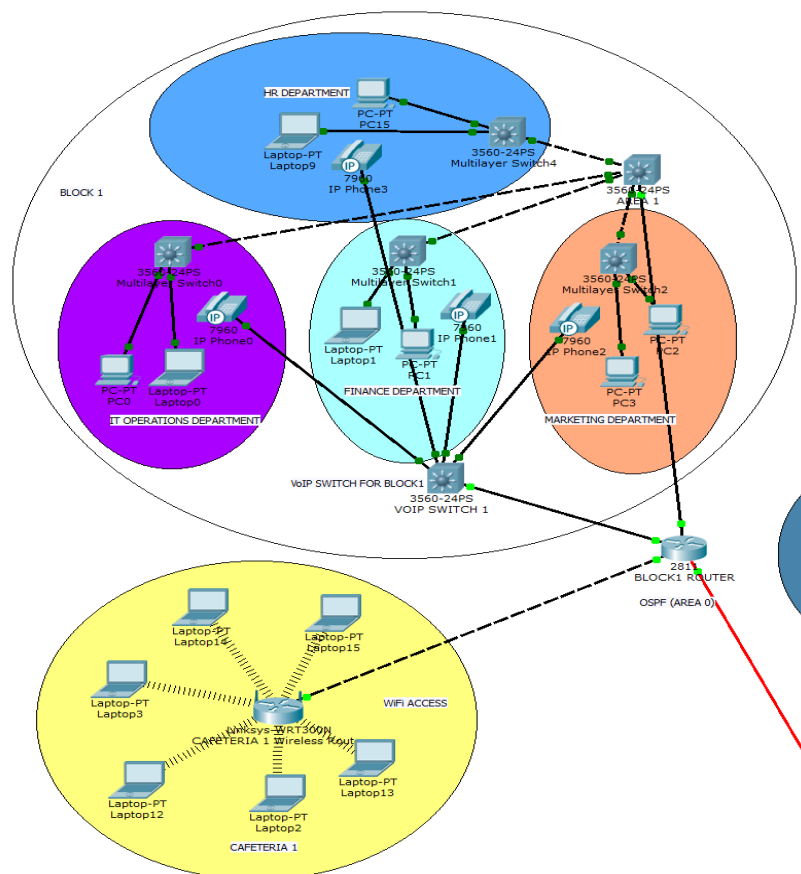


Figure 4.2 – Block 1

- **BLOCK 2**

Block 2 is the area where the second leg of the organisation’s departments, along with VoIP Phones, has been placed. Cafeteria 2 has been designed next to Block 2. EIGRP (Enhanced Interior Gateway Routing Protocol) has been implemented for Block 2 and RIPv2 for Cafeteria 2.

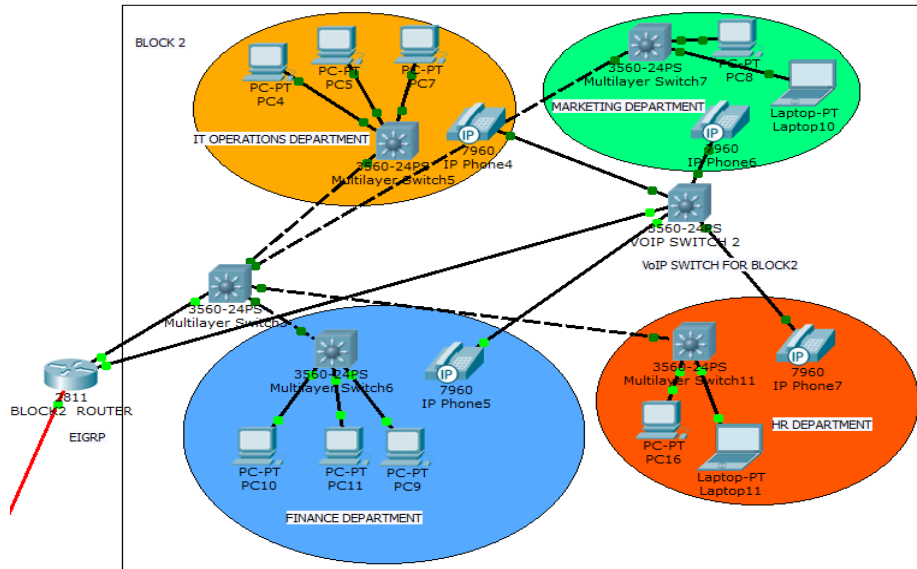


Figure 4.3 – Block 2

• **BLOCK 3**

The servers supporting the organisation’s network are present in Block 3, which is the Server Area, running on RIPv2 (Routing Information Protocol version 2). One server is the Employees’ resources server, second is the DNS server, and third is the organisation’s website server. To provide undeterred access to the servers even in situations where any one of the paths goes down, a redundant path has been provided which has been automatically blocked by STP (Spanning Tree Protocol), to avoid loop formation.

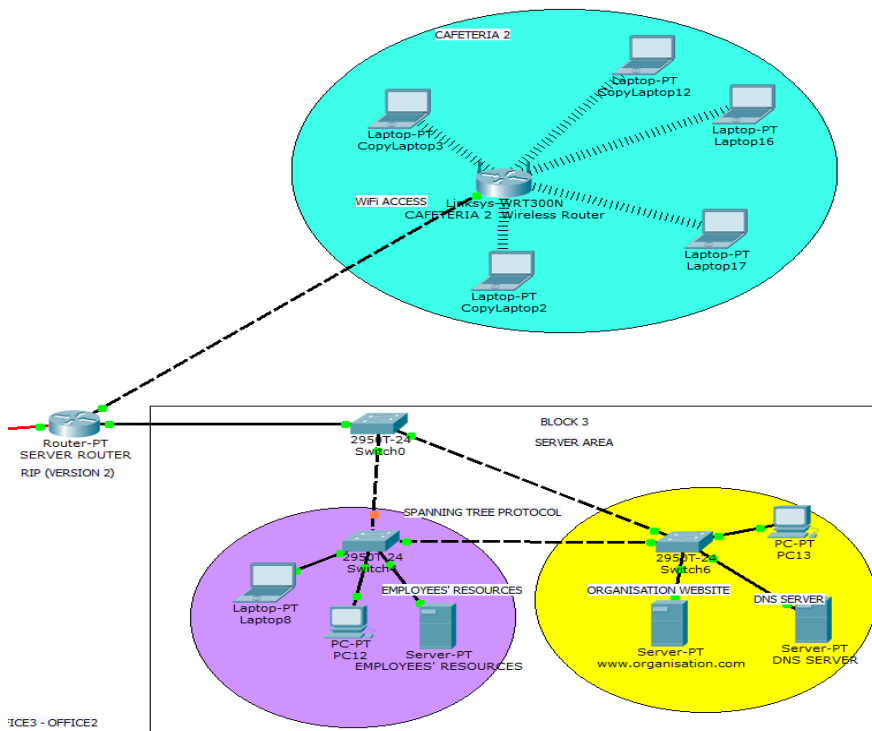


Figure 4.4 – Block 3

• **BLOCK 4**

Block 4 houses the R&D (Research and Development) Department of the organisation. This area has further been divided into R&D Block 1 and R&D Block 2. In order to shield the organisation's R&D activities from leaking out, ACL has been deployed on the R&D department router. Block 4 is thus secured, as neither a user from within the R&D department can reach any other part of the organisation's network or the internet, nor vice versa. Moreover, Port Security has been implemented on the switches in the R&D department. The MAC addresses of the verified users' computers have been configured on the ports of the switches, so that an alien user cannot connect to the switch. Also, Ether Channels have been deployed between the two switches, i.e. two individual Ethernet links have been bundled into a single logical link. If a segment within an Ether Channel fails, traffic previously carried over the failed link switches to the second segment within the Ether Channel. This has been done to guarantee greater bandwidth as well as uninterrupted communication between the members of the two blocks. The Ether Channels have been configured using the *Port Aggregation Control Protocol (PAgP)*. Block 4 is running on OSPF and is a part of Area 1.

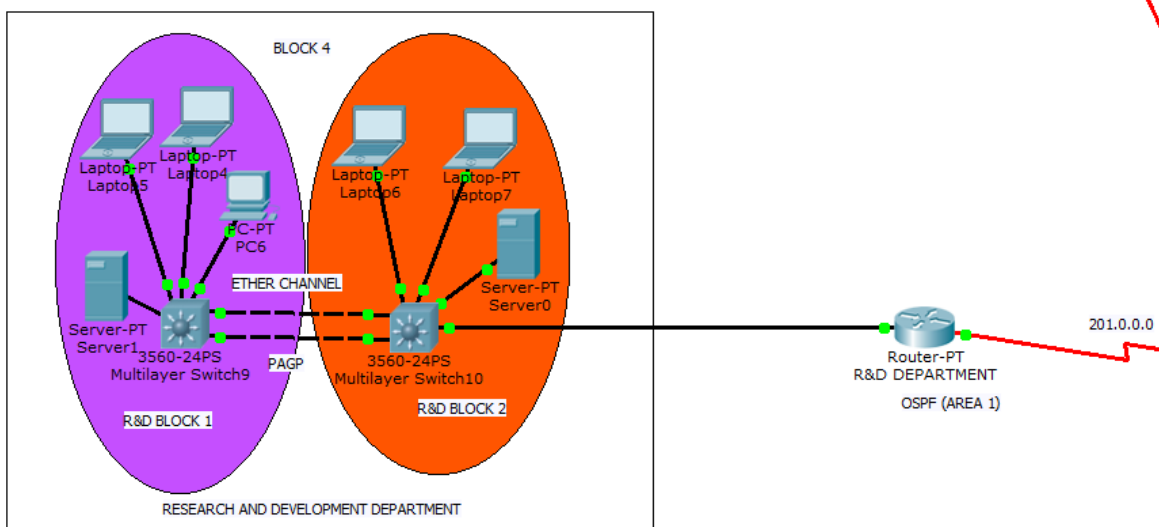


Figure 4.5 – Block 4

PROGRAMMING MODULES FOR BLOCK 4

- **Securing the ports on the switch in R&D department:**

```
Switch#conf t
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
```

Figure 4.6 – Configuration for Port Security in Block 4

- **Defining ACL to isolate the R&D department:**

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 deny any
Router(config)#int f0/0
Router(config-if)#ip access-group 10 out
Router(config-if)#exit
```

Figure 4.7 – Configuration for access control list (ACL) in Block 4

• FRAME RELAY

It has been assumed that offices 1, 2 and 3 of the organization are situated in the city A, with other offices in far-away states and countries. To connect the three offices in the same city, *Frame Relay* has been used, as this would lead to cost savings as well as provide high bandwidth according to the *CIR* (Committed Information Rate). *PVCs* have thus been created between each of the three offices, therefore guaranteeing secure and fast transmission of data between the offices. The cloud represents the Frame Relay network and the organization's offices 2 and 3 have each been depicted by a router, for representational purpose.

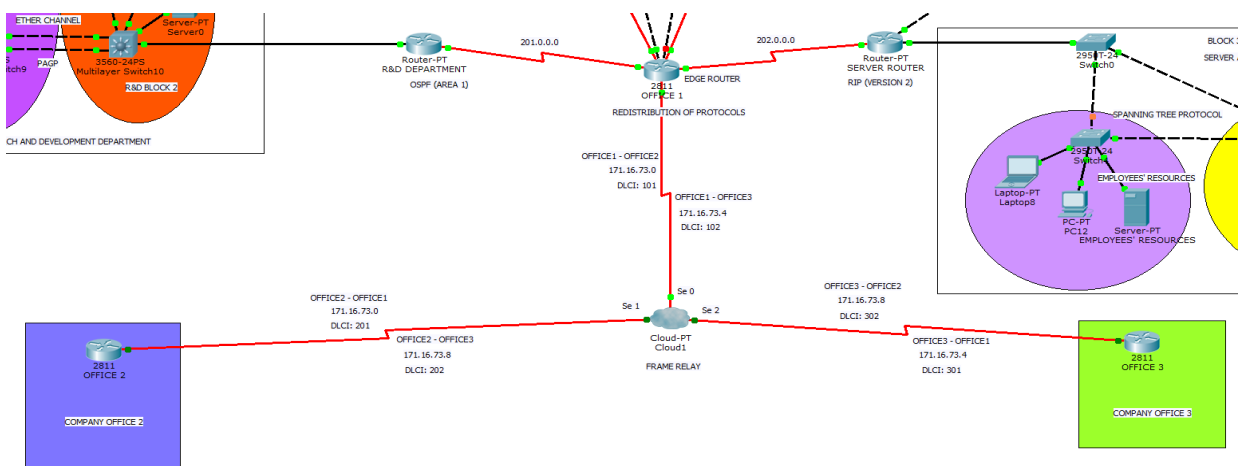


Figure 4.8 – Frame Relay Network

PROGRAMMING MODULES FOR FRAME RELAY

- **Creating sub-interface and assigning DLCI and IP address to them, for each office's router:**

```
Router#conf t
Router(config)#int s1/7
Router(config-if)#no ip address
Router(config-if)#encapsulation frame-relay
Router(config-if)#int s1/7.1 point-to-point
Router(config-subif)#frame-relay interface-dlci 101
Router(config-subif)#ip address 171.16.73.1 255.255.255.252
Router(config-subif)#int s1/7.2 point-to-point
Router(config-subif)#frame-relay interface-dlci 102
Router(config-subif)#ip address 171.16.73.5 255.255.255.252
Router(config-subif)#exit
```

Figure 4.9 – Frame Relay: Configuration for sub-interface

- **Defining DLCI numbers in each serial connection of cloud:**

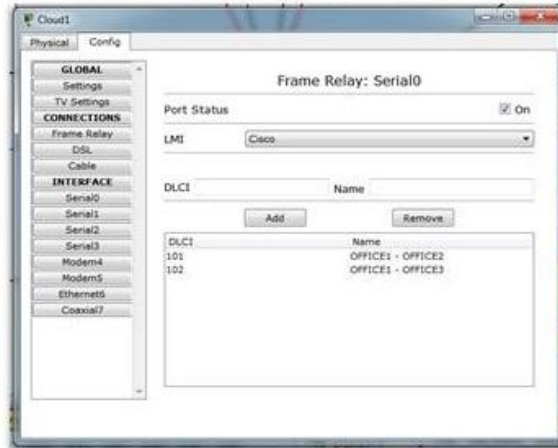


Figure 4.10 – Frame Relay: Configuration for DLCI numbers on serial connection of cloud

- **Creating end-to-end connections, i.e., Permanent Virtual Circuits:**

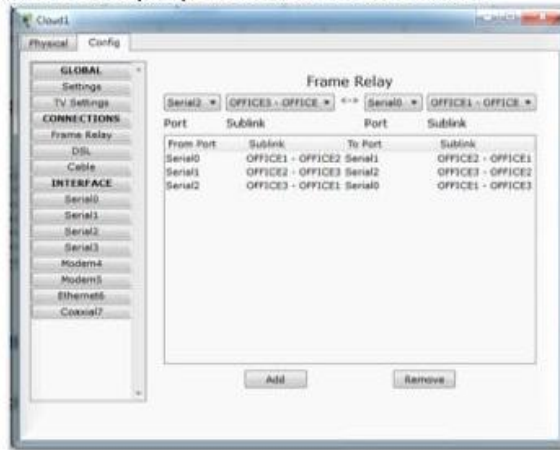


Figure 4.11 – Frame Relay: Configuration for Permanent Virtual Circuit

• **ISP 1 AND ISP 2**

ISP (Internet Service Provider) 1 and ISP 2, represent the internal networks of the two Internet Service Providers for the organization. The link to ISP 2 has been kept in shut-down mode administratively, and would be activated only in case of the link to the primary ISP shutting down. The network incorporates a connection to the (redundant) secondary ISP, to guarantee uninterrupted internet access for the organization.

The Web Servers' Pool represents the servers of two websites, namely, www.xyz.com and www.abc.com. This area is running on RIPv2.

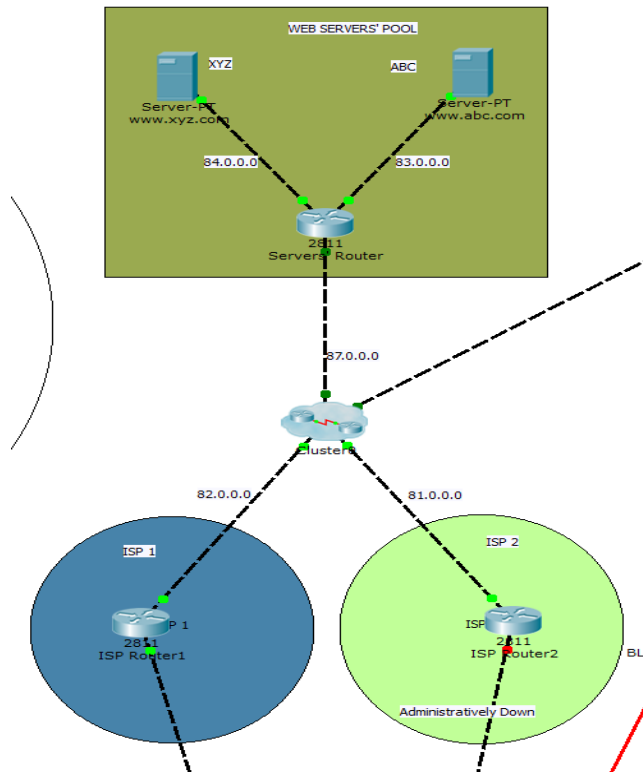


Figure 4.12 – ISPs connecting the network to outside world

- **VIRTUAL PRIVATE NETWORK**

Company's Remote Office represents one of the offices of the organization, in a different region or country. A site-to-site VPN has been established between the remote office and the office under consideration. A secure IPsec tunnel has been set up starting from the remote office's router to the Block 1 router, for representational purposes. Traffic between the two offices is transmitted over the internet at best effort. Therefore, remote offices of the organization are connected to each other as though they are a part of the same network.

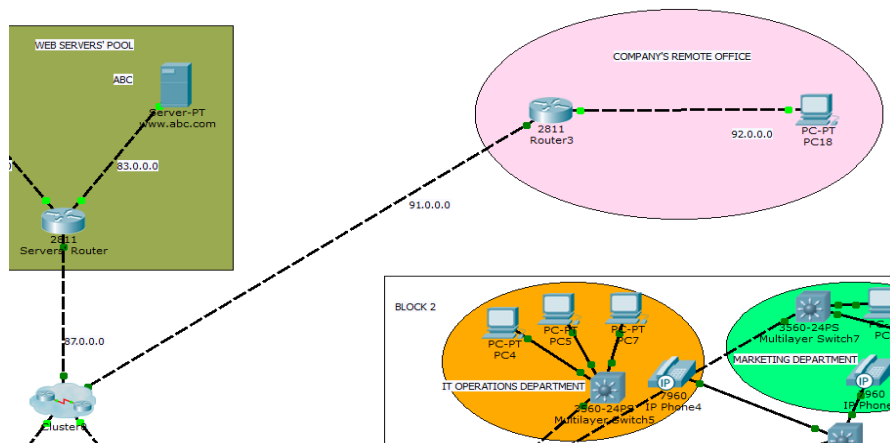


Figure 4.13 – Site-to-site VPN

- Configuring VPN tunnel on the destination router (Block 1 Router)**
 Router>en
 Router#conf t
 Router(config)#crypto isakmp policy 10
 Router(config-isakmp)#authentication pre-share
 Router(config-isakmp)#hash sha
 Router(config-isakmp)#encryption aes 256
 Router(config-isakmp)#group 2
 Router(config-isakmp)#lifetime 86400
 Router(config-isakmp)#exit
 Router(config)#crypto isakmp key toor address 200.0.0.2
 Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
 Router(config)#access-list 101 permit ip 172.16.0.0 0.0.0.127 205.0.0.0 0.0.0.255
 Router(config)#access-list 101 permit ip 172.16.0.128 0.0.0.127 205.0.0.0 0.0.0.255
 Router(config)#access-list 101 permit ip 172.16.1.0 0.0.0.127 205.0.0.0 0.0.0.255
 Router(config)#access-list 101 permit ip 172.16.5.0 0.0.0.127 205.0.0.0 0.0.0.255
 Router(config)#crypto map CMAP 10 ipsec-isakmp
 % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.
 Router(config-crypto-map)#set peer 200.0.0.2
 Router(config-crypto-map)#match address 101
 Router(config-crypto-map)#set transform-set TSET
 Router(config-crypto-map)#EXIT
 Router(config)#int serial 0/0/0
 Router(config-if)#crypto map CMAP
 *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

Figure 4.14 – Configuration for one end of VPN tunnel

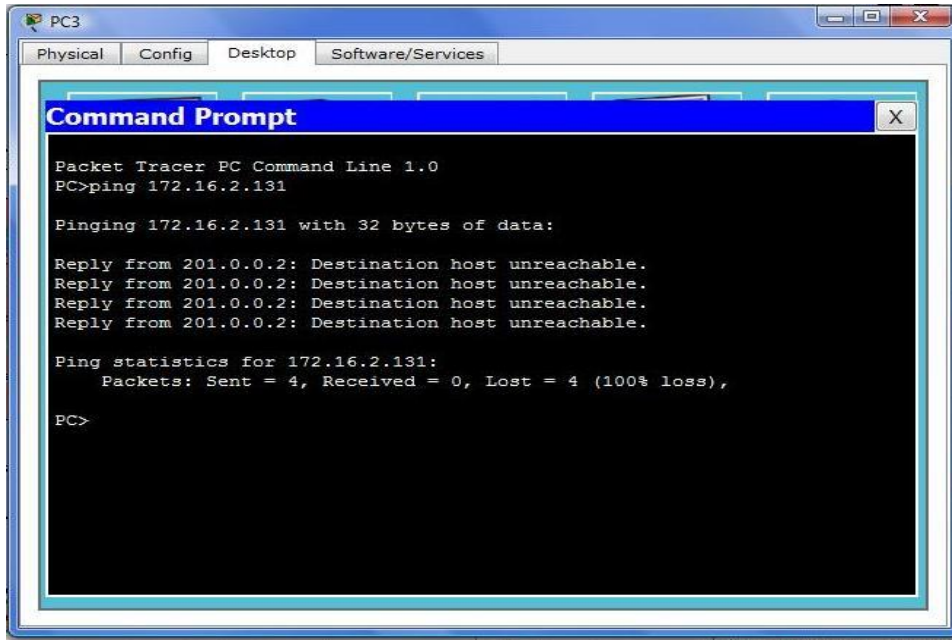
- Configuring VPN tunnel from remote office (Router 3)**
 Router#configure terminal
 Router(config)#interface FastEthernet0/0
 Router(config-if)#ip address 91.0.0.2 255.0.0.0
 Router(config-if)#exit
 Router(config)#router rip
 Router(config-router)#version 2
 Router(config-router)#network 92.0.0.0
 Router(config-router)#network 91.0.0.0
 Router(config-router)#exit
 Router(config)#crypto isakmp policy 10
 Router(config-isakmp)#authentication pre-share
 Router(config-isakmp)#encryption aes 256
 Router(config-isakmp)#group 2
 Router(config-isakmp)#lifetime 86400
 Router(config-isakmp)#exit
 Router(config)#crypto isakmp key toor address 91.0.0.1
 Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
 Router(config)#access-list 101 permit ip 92.0.0.0 0.255.255.255 82.0.0.0 0.255.255.255
 Router(config)#crypto map CMAP 10 ipsec-isakmp
 Router(config-crypto-map)#set peer 91.0.0.1
 Router(config-crypto-map)#match address 101
 Router(config-crypto-map)#set transform-set TSET
 Router(config-crypto-map)#exit
 Router(config)#int f0/0
 Router(config-if)#crypto map CMAP
 *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
//Configuration of VPN tunnel is also carried out on all the intermediate routers.

Figure 4.15 – Configuration for other end of VPN tunnel

4.2) DEMONSTRATION

The network, when simulated on Cisco Packet Tracer, produced the following results:

(a) On trying to ping a member of the R&D Department from another part of the network, the result “Destination Host Unreachable” gets displayed.



```
PC3
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.2.131

Pinging 172.16.2.131 with 32 bytes of data:

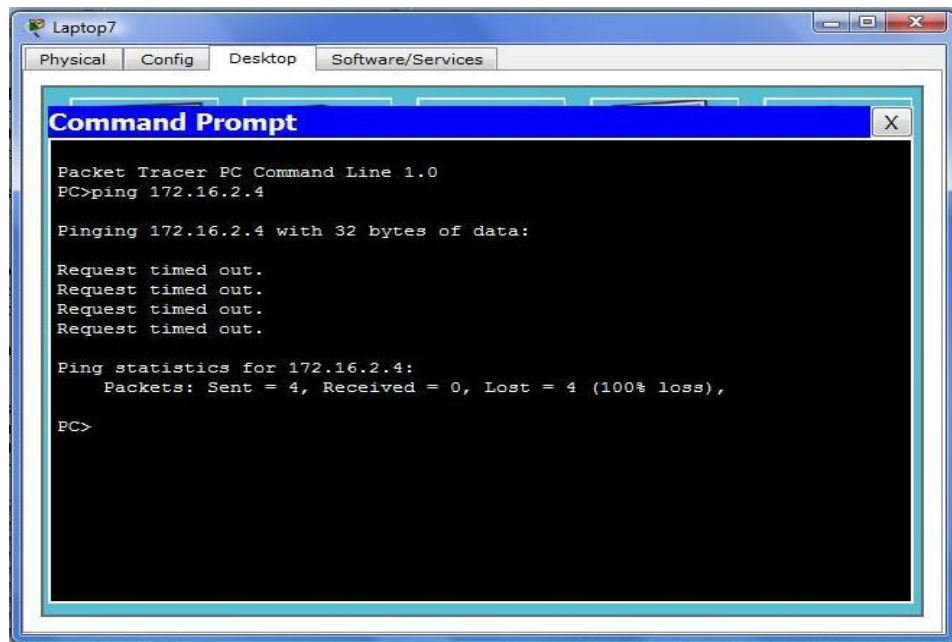
Reply from 201.0.0.2: Destination host unreachable.
Reply from 201.0.0.2: Destination host unreachable.
Reply from 201.0.0.2: Destination host unreachable.
Reply from 201.0.0.2: Destination host unreachable.

Ping statistics for 172.16.2.131:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 4.16 – Unsuccessful Ping originating from outside the R&D Department

(b) When a member of the R&D Department tries to ping a member of say, Block 1, “Request Timed out” gets displayed.



```
Laptop7
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.2.4

Pinging 172.16.2.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 4.17 – Unsuccessful Ping originating from inside the R&D Department

4.3) CONCLUSION

Thus, winding up the description of the network in a nutshell, the fact that nowadays in an organization, peer-to-peer communication is a more important part of Local Area Networks than client-server communication, led to the incorporation of Voice over Internet Protocol in the proposed design. Moreover, VoIP is advantageous as it leads to cost savings and poses no geographical boundaries. In case of the connection to the primary ISP breaking down, a redundant connection to a secondary ISP has been provisioned to guarantee 24*7 internet connectivity. The R&D department in the designed network has been supplied with Ether Channel technology to guarantee the best availability of resources and its functionality under the most severe circumstances. The isolation of R&D department from the other parts of the organization and the exterior world could be possible due to implementation of software firewall in the form of Access Control List. The sensitive company data on the servers of R&D department has been secured by incorporation of Port Security in the area, which will prevent anyone to disconnect the presently connected computers, connect any unauthorized device and hack the data. Also, established as a network of privately owned equipment, Frame Relay is able to connect multiple offices of the organization in the same city. Site to site VPN is able to utilize the flexibility and ubiquity of the Internet in connecting remote offices of the organisation, for the holistic working and growth of the entire enterprise.

PUBLICATION
**DEPLOYING PRAGMATIC TECHNIQUES FOR CAMPUS
NETWORK DESIGN**

¹ADITYA AHUJA, ²NIKITA GUPTA, ³KAMAL DEWAN, ⁴MEENAKSHI SOOD

^{1,2,3}ECE Department Jaypee University of Information Technology , Waknaghat, Solan ⁴Faculty, ECE Department Jaypee University of Information Technology , Waknaghat, Solan E-mail: adityaahuja2005@gmail.com, nikita92gupta@yahoo.com, kdewan9495@gmail.com

Abstract- This paper dwells on the notion that the designing of networks must escalate from applying just a basic set of rules, to utilizing the myriads of technologies now available to us, the plethora of services whose provision to end users is now possible and the nuances that emerge by the combination of the different technologies and services. To adapt to the changes in network designing, we propose an architecture for campus network design using state of the art technologies such as Ether Channels, VoIP (Voice over Internet Protocol), VPN (Virtual Private Network), Wi-Fi, redistribution of protocols, Link Redundancy and ISP Redundancy. The network architecture has been designed on Cisco's network simulation software: Cisco Packet Tracer. The proposed design is an enhancement of the existing network architecture of Jaypee University of Information Technology. The design can be utilized while laying down the LAN architecture of any other campus, be that a University, Corporate office or Hospital.

Index Terms- Ether Channels, VoIP (Voice over IP), VPN (Virtual Private Network), STP (Spanning Tree Protocol)

I. INTRODUCTION

Network architecture and designing, which was considered sheer art few decades ago, today, in the contemporary world, is an amalgamation of knowledge and art. Today, networks are embedded within our workplaces, homes and outside environment, making possible the miraculous aspect of real-time access to information throughout the world. The modern networks are designed to meet security, connectivity, and performance challenges while enabling key IT initiatives. They also must scale, offer operational simplicity, and flexibly accommodate new computing trends without an entire redesign. Networks are broadly classified as LAN (Local Area Network), and WAN (Wide Area Network). LANs, which persist over a relatively shorter distance are designed to allow personal computers to share resources, which can include hardware (e.g., a printer), software (e.g., an application program), or data. A WAN, which is a geographically dispersed collection of LANs, provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world [3]. In networking's early days, networks were not considered a critical resource as they did not directly support revenue generation. Now, the picture has changed radically. As our ability to gather, process, and distribute information grows, the demand for ever more sophisticated information processing grows even faster. The issue here is resource sharing, and the goal is to make all programs, equipments, and especially data available to anyone on the network without regard to the physical location of the resource and the user [4]. The roots of this paper lie in the corporate LAN, which has matured from an inert business element to a very active and visible asset that

today's organizations rely on to support their day-to-day functions, critical to their market success. Another major evolution witnessed is the shift from traditional client/server data flow support to peer to peer flow support.

This paper focuses on enhancing the existing LAN architecture Of Jaypee University of Information Technology (JUIT), by the incorporation of new and advanced technologies such as VoIP, VPN, Ether Channels, STP, ISP redundancy. The proposed architecture has been implemented and tested on Cisco's Network Simulation Program: "Cisco Packet Tracer". In addition to being an upgrade for the existing LAN of JUIT, the proposed architecture is generic and can be utilized for any campus, be that of a university, a corporate office, a hospital or myriads of other organizations.

The rest of the paper is organized as follows: section 2 presents a brief description about techniques employed in the proposed architecture. Section 3 demonstrates the proposed network architecture, as designed in Cisco Packet Tracer. Section 4 presents the results and discussions along with demonstration of some of the results.

II. TECHNIQUES EMPLOYED

A. LAN ARCHITECTURE DESIGN

To devise the architecture of a LAN, hierarchical model is employed, as depicted in Fig. 1. This model uses layers, which simplifies the task required for internetworking along with ease of understanding and fault isolation [5]. The Layered Approach stretches up to three layers: the access layer, the aggregation layer, and the core layer. The access layer marks the access boundary of the network and ensures connectivity to

end users in the network. The aggregation layer fuses connections and traffic flows from multiple access layer switches which is further delivered to the switches in core layer. The core layer provides secure link between aggregation layer switches and the routers connecting to the WAN and the Internet to empower business-to-business association. This layer also provides a link for high-speed packet switching between multiple aggregation devices in the network [1].

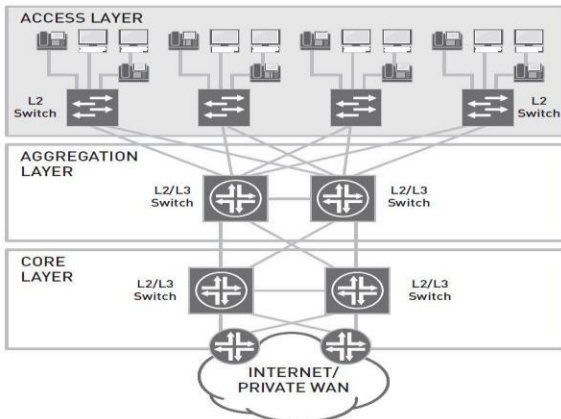


Fig. 1 Hierarchical Model of LAN design [1]

Earlier, local area networks used to be simple, as they were not required to do hefty jobs. But as the organizations started growing in almost every dimension, the LANs were required to be capable of providing high speed connections and integrate data and voice services. Some of the technical features fulfilling such requirements, which authors have also incorporated in their proposed design, are discussed below.

VoIP is a rapidly emerging technology that converges the voice and data networks for voice communication, using the omnipresent IP-based networks to deploy VoIP client devices such as IP phones, mobile VoIP-enabled handheld devices, and VoIP gateways. With the replacement of conventional telecommunications systems – even Private Branch Exchanges (PBX) – by IP-based systems (IP PBX), Voice over IP can also be used in the local network (LAN) of a company [6].

Ether Channel allows multiple physical Fast Ethernet links to combine into one logical channel. This allows load sharing of traffic among the links in the channel as well as redundancy in the event that one or more links in the channel fail. Fast Ether Channel can be used to interconnect LAN switches, routers, servers, and clients via unshielded twisted pair (UTP) wiring or single-mode and multimode fibre [7].

VPN (Virtual Private Network) is an overlay network that is built over a public network infrastructure, providing the VPN user with a private network using

tunneling, encryption and authentication mechanisms [8]. There exist two types of VPNs, Site to Site VPN and Remote Access VPN. Site to site VPN can be used when several different companies need to work in a shared environment. Remote Access VPN is mainly used in scenarios where access to data on company's private network is required by a member sitting at a distant location. The authors have incorporated remote access VPN in their proposed architecture.

B. PROTOCOLS EMPLOYED

A device, connected to a network, is capable of sending or receiving information. However, two devices cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications [4].

RIP (Routing Information Protocol) is a distance-vector routing protocol which sends the complete routing table out to all active interfaces every 30 seconds. It only uses hop count to determine the best way to a remote network with a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it is inefficient on large networks with slow WAN links or on networks with a large number of routers installed [2].

RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask. In the network designed, authors are using version 2 which utilizes classless routing. OSPF (Open Shortest Path First) is a link state routing protocol that has been implemented by a wide variety of network vendors, including Cisco. OSPF is based on Shortest Path First routing algorithm. Each router computes the shortest path tree with itself as the root and then the routing table is populated with the resulting best paths [9]. It supports both IPv4 and IPv6 routed protocols. EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance-vector routing protocol that is used on a computer network to help automate routing decisions and configuration. It is a classless protocol because it includes the subnet mask in its route updates.

It synchronizes routing tables between neighbors initially and then sends specific updates only when topology changes occur, thus making it suitable for very large networks, having a maximum hop count of 255. STP (Spanning Tree Protocol) is a data link layer protocol which is implemented on bridges and switches. STP vigilantly monitors the network to find all links, making sure that no loops occur by shutting down any redundant links.

STP uses the spanning-tree algorithm (STA) to first create a topology database and then search out and disable redundant links.

III. PROPOSED ARCHITECTURE

The proposed network architecture has been depicted in Fig. 2. The academic block is the area where all the different departments and the library are located. Each of the departments and the Library are under different VLANs. Each department has been provided an IP phone. The laboratory block is the area where the campus' laboratories are located. Here too, IP phones have been provided. The campus' server room is the area where all the servers supporting the campus' network have been placed. Separate servers have been provided for the university's website, data storage and

for DNS service. The hostel block is the area where all the hostels are located. To increase bandwidth and provide link redundancy, ether channels have been implemented in this area. To tackle a situation where the link to the primary ISP breaks down, the network incorporates a private network which has an internet connection via a redundant ISP. To enable communication between the different protocols, redistribution has been implemented on the edge router. Another feature of the network is the remote access VPN, which allows students and faculty to access their resources on the university's servers, from outside the university intranet.

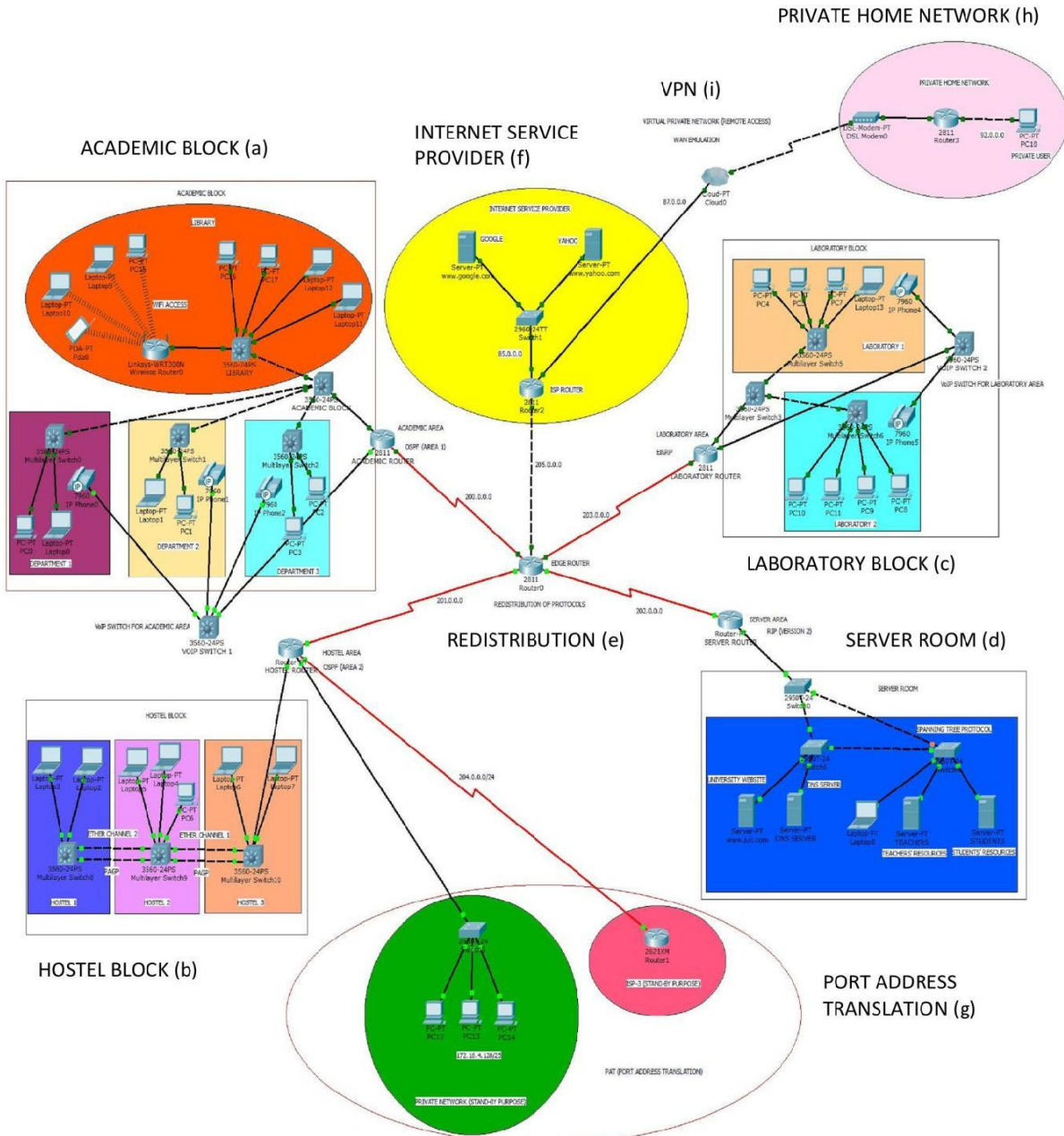


Fig. 2 Proposed Network architecture

IV. RESULTS AND DISCUSSIONS

The programming modules for each department are developed independently, given in Fig 3-5. The complete network is DHCP (Dynamic Host Configuration Protocol) enabled and each of the Departments and the Library are under different VLANs, as shown in Fig. 3(a). The routing protocol used in the academic block and hostel block is OSPF. The Academic Block, as shown in Fig. 2(a), is under OSPF area 1 and the Hostel Block, as shown in Fig. 2(b) is under OSPF area 2. The edge router is under OSPF area 3.

The routing protocol used in the Laboratory Block, as depicted in Fig. 2(c), is EIGRP. The Library has wired as well as Wi-Fi access. Configuration for Wi-Fi has been depicted in Fig. 3(c). Separate switches for VoIP facility have been used, to which the IP phones for each department and each laboratory are connected, the configuration for which is shown in Fig. 3(b). In the hostel block, Ether Channels have been deployed, i.e. bundling of two individual Ethernet links into a single logical link. If a segment within an Ether Channel fails, traffic carried over the failed link, switches to the second segment within the Ether Channel. The Ether Channels have been configured using the Port Aggregation Control Protocol (PAgP), as shown in Fig. 3(d).

```
Switch(config)#vlan 2 //VLAN configuration on Academic Switch
Switch(config-vlan)#name DEPARTMENT_1
Switch(config-vlan)#exit
Switch(config)#interface range f0/2, f0/24
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit.
Router#conf t
Router(config)#int f0/0 //Creating sub-interfaces for multiple VLANs
Router(config-if)#no ip address
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int f0/0.1
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 172.16.0.1 255.255.255.128
Router(config-subif)#exit.
Router(config)#ip dhcp pool dep1 //DHCP Pool for department 1
Router(dhcp-config)#network 172.16.0.0 255.255.255.128
Router(dhcp-config)#default-router 172.16.0.1
```

Fig. 3(a) Configuration of VLAN on academic switch and DHCP on academic router

```
Router>en
Router#conf t
Router(config)#telephony-service //Activating telephony services On IP Phone
Router(config-telephony)#no auto-reg-ephone
Router(config-telephony)#ip source-address 10.0.0.1 port 2000
Router(config-telephony)#max-ephones 10
Router(config-telephony)#max-dn 100
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 1000 //Assigning a phone number to the IP Phone
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#exit
Router(config)#ephone 1
Router(config-ephone)#mac-address 0009.7C08.C930
Router(config-ephone)#exit
Router#conf t //enabling inter-network IP phone calls
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern ....
Router(config-dial-peer)#session target ipv4:200.0.0.1
Router(config-dial-peer)#exit
Router(config)#router ospf 1 //adding the sub-networks to OSPF
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router(config-router)#network 20.0.0.0 0.0.0.255 area 0
Router(config-router)#network 30.0.0.0 0.0.0.255 area 0
Router(config-router)#exit
```

Fig. 3(b) Configuration for VoIP on academic router

Fig. 4 Configuration of DNS server

Proceedings of SARC-IRF International Conference, 12th April-2014, New Delhi, India, ISBN: 978-93-84209-03-2

```
//Configuration on the Library switch
Switch#conf t
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#exit
Router#conf t
Router(config)#router ospf 1 //wireless network is added to OSPF
Router(config-router)#network 172.16.5.0 0.0.0.127 area 0
Router(config-router)#exit
```

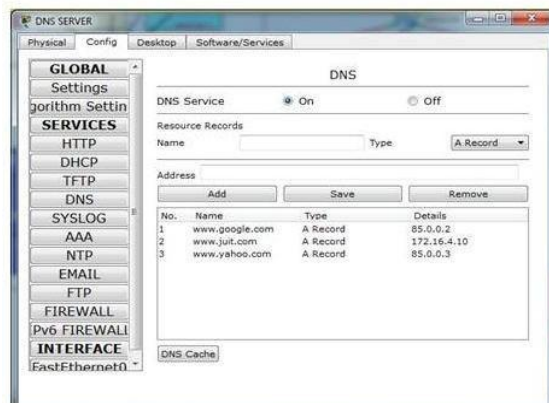
Fig. 3(c) Configuration of Wi-Fi in Library

```
Switch(config)#interface port-channel 3 //configuring the Ether Channels
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface range f0/3-4
Switch(config-if-range)#channel-protocol pagp
Switch(config-if-range)#channel-group 3 mode desirable
Switch(config-if-range)#exit
//The corresponding channel is completed by configuring the same on the opposite switch
```

Fig. 3(d) Configuration for Ether Channels in hostel block

We propose the Server Room, as depicted by Fig. 2(d), which runs on RIPv2 (Routing Information Protocol version 2). One server is exclusively for the university's website (www.juit.com), second as the DNS (Domain Name System) server, third acts as teachers' resources server, and the fourth is the students' resources server. The configuration for the DNS server is as shown in Fig. 4. To provide uninterrupted access to the servers even in situations where any one of the links fails, a redundant path has been provided which has been automatically blocked by STP, to avoid loop formation.

//configuring the DNS server



As the design is based on a multiple protocol environment, redistribution is a necessity, and has been implemented on the edge router, to enable

communication between the three different protocols, i.e. OSPF, EIGRP and RIPv2, as depicted in Fig. 2(e). The corresponding configuration has been shown in Fig. 5.

```

Router(config)#router rip //redistribution of RIP with EIGRP and OSPF
Router(config-router)#version 2
Router(config-router)#redistribute ospf 3 metric 2
Router(config-router)#redistribute eigrp 2 metric 2
Router(config-router)#exit
Router(config)#exit
//Redistribution of OSPF with RIP and EIGRP, and of EIGRP with OSPF and RIP is also carried out
    
```

Fig. 5 Redistribution of the different protocols on edge router

The ISP is shown in Fig. 2(f), with two servers of example websites (www.google.com, www.yahoo.com). The network connecting the servers to the ISP, i.e. 85.0.0.0 has been added to RIPv2. To tackle a catastrophic situation in which the connection to the primary ISP breaks down, a stand-by private network with an exclusive connection to a redundant ISP has been set-up, as depicted in Fig. 2(g). This private network will be used for internet access in emergency situations. The private network can communicate with the rest of the campus' network, but the redundant ISP is accessible only through the private network. PAT has been implemented here, i.e. the private IP network 172.16.4.128/25 has been translated to the public IP network 204.0.0.0/24, as shown in Fig. 6.

```

Router#conf t // configuring PAT (Port Address Translation)
Router(config)#ip nat pool stand_by 204.0.0.1 204.0.0.1 netmask 255.255.255.252
Router(config)#access-list 50 permit 172.16.4.128 0.0.0.128
Router(config)#ip nat inside source list 50 pool stand_by overload
Router(config)#interface f1/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface s3/0
Router(config-if)#ip nat outside
Router(config-if)#exit
    
```

Fig. 6 PAT for redundant ISP

The cloud is symbolic of a WAN. The private home network, as depicted by Fig. 2(h), can belong to any student/faculty of Jaypee University of Information Technology, who wants to access the students' resources or faculty resources server from outside the college's intranet. To make this service possible, remote access VPN has been implemented, in which the concerned person would log onto the ftp server using his unique username and password. Fig. 2(i) represents the layout of VPN designed for the institute.

A. DEMONSTRATION

The proposed architecture, when simulated on Cisco packet tracer, produced results which are demonstrated as follows:

(a). The case of a student, with an example username student\101003 and password ece, trying to access the students' resources server in the campus' server room, from his private home network, is demonstrated by Fig. 7.

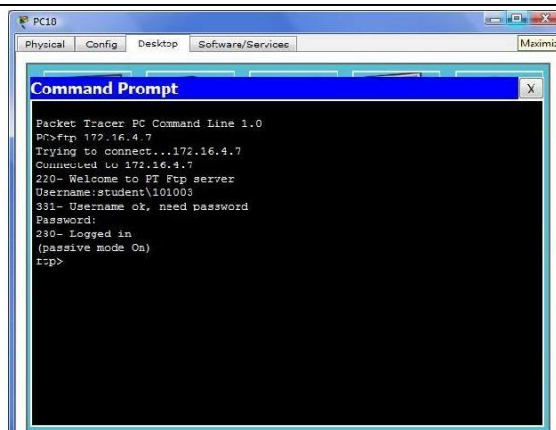


Fig. 7 accessing the students' resources server from outside the campus' intranet, using remote access VPN

(b). The case where an IP phone user with number 1000, from department 3 of the academic block, wishes to call an IP phone user with number 4000, in laboratory 1 of the laboratory block, is demonstrated in Fig. 8(a) and (b). As redistribution of protocols on the edge router, and appropriate configurations on the academic and laboratory routers have been carried out, IP phones under different protocols and networks can communicate with each other.



Fig. 8(a) User with number 1000 calling user with number 4000.

Ring Out message gets displayed on the screen.



Fig. 8(b) User with number 4000 receives the call from user with number 1000. Connected message gets displayed on the screen.

Thus, concluding in a nutshell, the Ether Channels provide link redundancy and an increase in bandwidth, thus making the network faster and more reliable. A VPN enables the students and faculty to remotely access the college's resources. In the event of

catastrophe, where the connection to the primary ISP breaks down, there exists a private connection to a redundant ISP, for access to the internet. Moreover, the feature of VoIP is advantageous as it leads to cost savings and poses no geographical boundaries. The proposed network architecture, though has higher cost of implementation as compared to the existing network of Jaypee University of Information Technology, it presents important enhancements. The design can further be improved by creating a back-up of the campus' server data, using cloud technology. Nowadays, as cloud services are being provided at reasonable prices, the university can have this alternate storage area for the important resources, so that in case of a calamity, the data can be retrieved from the cloud.

REFERENCES

- [1] Campus LAN Design Guide: Design Considerations for the High-Performance LAN, Juniper Networks, Inc., 2009
- [2] Todd Lammle, CCNA: Cisco Certified Network Associate Study Guide, John Wiley & Sons, 2009
- [3] Andrew S. Tanenbaum, 2003, Computer Networks, Prentice Hall PTR
- [4] Behrouz A. Forouzan, Catherine Ann Coombs, Sophia Chung Fegan, 2001, Data Communications and Networking, McGraw-Hill Higher Education
- [5] Network Topologies and LAN Design, Cisco Systems, 2000.
- [6] T-Systems, White paper- "Voice over Internet Protocol (VoIP)"
- [7] Y. Qin, K. Sivalingam and Bo Li, "Architecture and Analysis for providing Virtual Private Networks(VPN) with QoS over Optical WDM Networks", in SPIE Optical Networks Magazine, Vol. 2, No. 2, pp. 59–67, Mar/Apr. 2001.
- [8] Cisco Systems, "Understanding Ether Channel Load Balancing and Redundancy On catalyst Switches," 2011-2012.
- [9] Aman Shaikh, Albert Greenberg, AT&T Labs – Research, "OSPF Monitoring: Architecture, Design and Deployment Experience", in NSDI'04 Proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation - Volume 1

REFERENCES

- [1] Saadat Malik, Network Security Principles and Practices: Expert solutions for securing network infrastructures and VPNs, Cisco Press, 2003
- [2] Andrew S. Tanenbaum, 2003, Computer Networks, Prentice Hall PTR
- [3] Qutaiba Ali, Salah Alabady, and Yehya Qasim, “Applying reliability solutions to a cooperative network,” International Arab Journal of e-Technology, Vol. 1, No. 2, pp. 9-17, June 2009
- [4] V. Fuller, T. Li, J. Yu, K. Vardhan, “Classless Inter-Domain Routing(CIDR): An Address Assignment Strategy”, Daebgnata, Sep 1993
- [5] Robert Shimonski, Naomi Alpern, Michael Cross, Dustin L. Fritz, Mohan Krishnamurthy, Scott Sweitzer, 2009, CompTIA Network+ Certification Study Guide, Syngress
- [6] Sushruta Misra, Lamboder Jena, Aarti Pradhan, “Networking Devices and Topologies: A Succint Study”, Volume 2, Issue 11, November 2012
- [7] ISRD, 2006, Data Communication and Computer Networks, McGraw Hill Education
- [8] Cisco Systems, “Configuring Network Address Translation”
- [9] Paul F. Tsuchiya, “The IP Network Address Translator (Nat):Preliminary Design”, Bell Communications Research
- [10] R. Das, 2006, Enabling IP Routing with CISCO Routers, Laxmi Publications
- [11] Cisco IOS IP Configuration Guide,” Configuring Routing Information Protocol”
- [12] Cisco IOS IP Configuration Guide, “Enhanced Interior Gateway Routing Protocol”
- [13] Cisco IOS IP Configuration Guide, “Open shortest Path First”
- [14] Cisco Systems Solutions – Unified Communications
- [15] Germaine Bacon, Lizzi Beduya, Jun Mitsuoka, Betty Huang, Juliet Polintan, “Virtual private network,” unpublished
- [16] Aaron Balchunas, “Frame relay,” unpublished