Protocols for VLAN based Infrastructure: Design and Layout

Project report submitted in partial fulfillment of the requirement for the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted By

SANDHYA BHADOURIA	**(141043)**
ANUBHAV JAIN	**(141048)**
SUSHILA KUMARI MEHTA	**(141096)**

UNDER THE GUIDANCE OF

MR. MOHIT GARG

JAYPEE UNIVERSITYOF INFORMATION TECHNOLOGY, WAKNAGHAT

MAY-2018

TABLE OF CONTENTS

DECLARATION BY THE SCHOLAR

We hereby declare that the work reported in the B-Tech thesis entitled **“Protocols for VLAN based Infrastructure: Design and Layout”** submitted at **Jaypee University of Information Technology, Waknaghat India,** is an authentic record of my work carried out under the supervision of **Mr. Mohit Garg, Assistant Professor**. We have not submitted this work elsewhere for any other degree or diploma.

Sandhya Bhadouria (141043)

Anubhav Jain (141048)

Sushila Kumari Mehta (141096)

Department of Electronics & Communication Engineering

Jaypee University of Information Technology, Waknaghat, India

CERTIFICATE

This is to certify that the work reported in the B.Tech project report entitled **"Protocols for VLAN based Infrastructure: Design and Layout "**which is being submitted by **Sandhya Bhadouria (141043), Anubhav Jain (141048) and Sushila Kumari Mehta (141096)** in fulfillment for the award of Bachelor of Technology in Electronics and Communication Engineering by the Jaypee University of Information Technology, is the record of candidate's own work carried out by him/her under my supervision. This work is original and has not been submitted partially or fully anywhere else for any other degree or diploma.

Mr. Mohit Garg

Assistant Professor

Department of Electronics & Communication Engineering

Jaypee University of Information Technology, Waknaghat,

ACKNOWLEDGEMENT

In performing our project, we had to take help and guidelines from some respected persons who deserves our greatest gratitude. We would like to show our gratitude to **Mr. Mohit Garg, Assistant Professor** for giving us the guidelines for project throughout numerous consultations. We would also like to extend our deepest gratitude to all those who have directly and indirectly guided us in completing the project and this report.

We also thank **Prof. Dr. Samir Dev Gupta, Head of Department, Electronics and Communication Engineering**, Jaypee University of Information Technology, Waknaghat for consent to include copyrighted pictures as a part of our report. We also thank **…** Technical and Laboratory, Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Waknaghat for providing us with all facilities, necessary components required to complete the project.

Sandhya Bhadouria (141043)
Anubhav Jain (141048)
Sushila Kumari Mehta (141096)

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

ABBREVIATIONS	**FULLFORM**
VLAN	Virtual Local Area Network
IP	Internet Protocol
MAC	Media Access Control
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ASCII	American Standard Code for Information Interchange
DNS	Domain Name Service
NTP	Network Time Protocol
OSI	Open Systems Interconnection

ABSTRACT

VLANs are broadly utilized as a part of the present endeavor systems to enhance Ethernet adaptability and encouraging network policies. In any case, manuals and reading material offer next to no data about how VLANs are really utilized as a part of training. Through dialogs with network administrators and examination of design information, we depict how college grounds utilize VLANs to accomplish an assortment of objectives. We contend that VLANs are ill-suited to a portion of these objectives (e.g., VLANs are frequently used to acknowledge get to control arrangements, however oblige the sorts of strategies that can be communicated). Moreover, the utilization of VLANs prompts critical multifaceted nature in the configuration of network device.

Every organization is using computer network to share their information and resources. They are connecting their network to the public network (for example internet). The organization is subdivided into different departments (administrative block, internet block, server block, hostel block) by implementing VLANs. Through Internet VLAN routing these departments can communicate with each other. The size of the network is increasing day by day. Membership in a VLAN can be based on port members, MAC addresses, IP addresses or combination of these features. VLANs are time effective, cost effective, can reduce traffic and provide an extra measure of security.

CHAPTER 1
INTRODUCTION

1.1 VLAN

Virtual LAN is a logical grouping of networking components. In Virtual LAN, multiple networks on the same physical network switch. Traffic from one virtual LAN is logically separated from other virtual LAN.

1.1.1 ADVANTAGES

Advantages of VLAN are :

- Solving broadcast issue
- Reducing the extent of broadcast domain
- Allowing us to include extra layer of security
- Allow us to actualize the logical grouping of device by work

Solving broadcast issue

When the switch ports is interfaced into the device, switch makes single broadcast domain for all ports and isolate impact space for each port.. Switch advances a broadcast outline from every conceivable port. In large area network having many PCs, it could make execution issue. we could make use of switches to be careful of broadcast problem, however this would be costly arrangement since each broadcast domain requires its own particular port on switch. Switch is only the solution for broadcast problem known as Virtual LAN. In most of the condition we use Virtual LAN rather than router to understand communicate problem.

Allowing us to include extra layer of security

In case of VLAN the no of devices sharing same VLAN can only get the data send on that particular VLAN. Other devices of different VLAN can’t access the data. So it helps in exchanging files without any fear of data being leak to unwanted devices. So it also help in case of broadcasting data. VLANs promote the security of network. If we have 100 devices, out of which 50 connected to VLAN1 and 50 connected to different VLAN2 then data send to VLAN1 cant not be access by other 50 devices connected to VLAN2. So designed VLAN provide us a control over each devices and port. We can also control the devices from unwanted access over files. It is providing security because no two devices connected to different VLAN can share any kind of data.

Reducing the extent of broadcast domain

VLAN is more interesting because it reduces the use of routers and also the size .If we have a network of 90 devices then we need only one VLAN but if we want to send different information to 30 devices then we have to create 2 VLAN one for those 30 devices and other for remaining 60 devices .We don’t need to allot routers to every domain .So in the same way if we use more VLAN then we can get more domains with less devices.

Allowing us to actualize the logical grouping of device by work

VLANs also help us to logically or simplified grouping or making different sections of devices. Every devices owner can able to watch just what they required to see in any case about their physical infrastructure or area.

1.1.2 EXAMPLES

Let's take an example to understand VLAN more clearly.

In this figure 1.1.2 there is one router connected, trunking is done .two computers are connected with the help of switch containing different network. In this figure we have 2 VLAN i.e. VLAN1 and VLAN2 which are manually configured on switch .if we send packet from a PC of VLAN2 to PC of VLAN1. Then the packet from PC will first send to switch then switch will send it to router will check the address information which include IP address and then further send it to the respective PC of respective VLAN1. Then the source PC will get the acknowledgement that the packet has received successfully by the

destination PC.

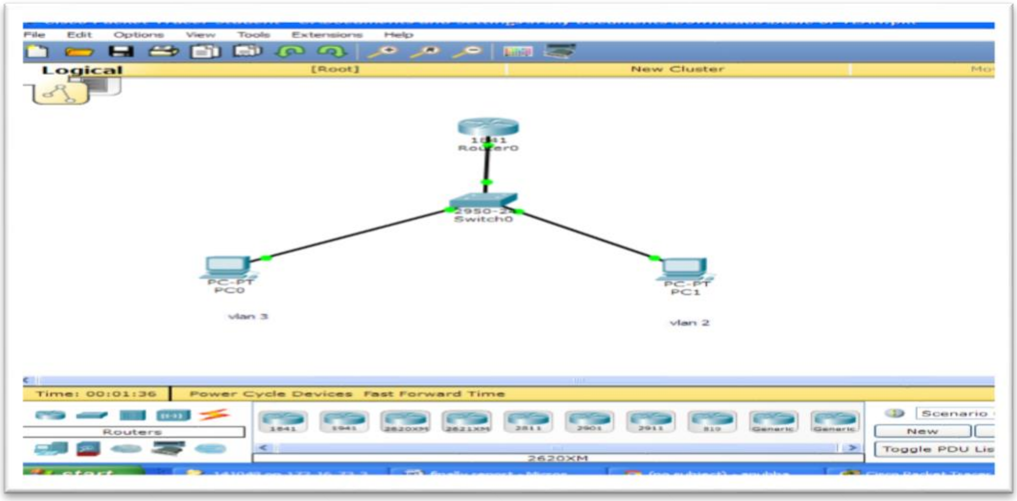


Figure 1.1.2: Basic VLAN Configuration

1.1.3 MEMBERSHIP

VLAN membership can be assigned by one of two strategies

- Static
- Dynamic

Static

Allotting VLANs statically is the most widely recognized and secure strategy. It is really simple to set up and manage. In this technique we physically allocate VLAN to switch port. VLANs designed along these lines are typically known as port-based VLANs.

Static strategy is the most secure technique too. As any switch port that we have doled out a VLAN will keep this affiliation constantly unless we physically transform it. It works extremely well in a systems networking condition where any client development inside the network should be controlled.

Dynamic

In dynamic method, VLANs are doled out to port naturally contingent upon the associated device. In this strategy we have configure one switch from arrange as a server. Server contains device particular data like MAC address, IP address and so forth. This data is mapped with VLAN. Switch going about as server is known as VMPS (VLAN Membership Policy Server). Just top of the line switch can configure as VMPS. Low end switch works as client and recover VLAN data from VMPS. Dynamic VLANs bolsters fitting and play mobility. For instance in the event that we move a PC starting with one port then onto the next port, new switch port will naturally be configured to the VLAN which the user has a place. In static method we need to do this procedure physically.

1.1.4 CONNECTIONS

We have to realize what sort of connection it has.

The two types of VLAN connection supported by Switch are:

- Access link
- Trunk link

Access link

In Access link connection is assigned to a single VLAN. Example, In my campus infrastructure, Administrative Block and Hostel Block has its own VLAN. In Administrative Block, different floors are assigned different VLAN. Each floor can easily send and receive data packets among themselves easily by the help of access link.

Trunk link

In Trunk link connection, VLAN is not specified. Example, In my campus infrastructure different floor can share their information easily by the help of trunk link. Trunk link connection is done between 2 switches and between switch and router. Trunk link connection connects multiple VLANs.

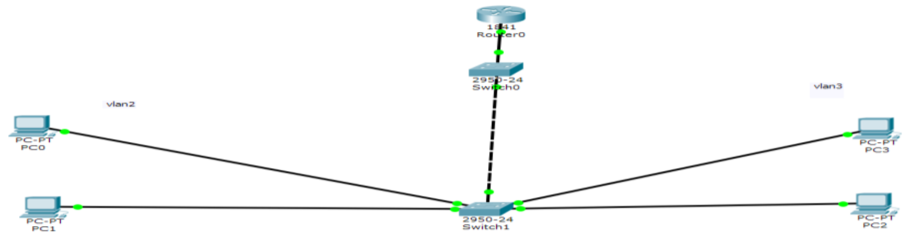


Figure 1.1.4: VLAN Connections

In the above figure, left side PC's share their information and right side PC's share their information among themselves respectively by the help of access link but cannot send or receive data packets from left side to right side and vice-versa. It can be done by the help of trunk link, it enables both side PCs to send or receive packets.

1.2 ROLE OF OSI MODEL

The OSI model consists of 7 layers. A protocol is the standard that allows the data communication.

1.2.1 PURPOSE

To make a typical stage for programming engineers and equipment makes that support the formation of systems networking items that can speak with each other over the network. To help network administrators by separating huge information trade process in littler sections. Littler sections are less demanding to comprehend, oversee and troubleshoot. With layer approach they just need to troubleshoot the devices, which are working in flawed layer.

1.2.2 LAYERS

Physical Layer

The physical layer is also known as layer 1, the functions are as follows:

- It is responsible for electrical sign.
- Repeaters, Hub are the devices works on this layer.
- ATM, FDDI are the protocols present on this layer.
- It is also known as hardware layer.

Data Link layer

The physical layer is also known as layer 1, the functions are as follows:

- It is responsible for the interpreting of the electrical sign and encode it into bits
- This layer converts electrical sign into frames.
- It manages the information provided by physical layer.
- Media Access Control (MAC) layer, Logical Link Control (LLC) layer are the two sub-layers of Data link layer
- The MAC sub layer controls how a PC on the system accesses the information and consent to send it.
- Switch like devices works on this layer.

Network Layer

The physical layer is also known as layer 1, the functions are as follows:

- The technique of routing and switching works on this layer.
- It routes the data information or packets to destination
- Router is also known has interworking device and contains IP Address.

- TCP/IP like protocols works on this layer.

Transport layer

The transport layer is also known as layer 4. These are features of transport layer mentioned below:

- It manages the flow control and also end-to-end mistake recuperation.
- Between end frameworks it manages the straightforward exchange of information.
- This layer consists of protocols like TCP and UDP work here
- Also manages or responsible for finish information exchange.

Session layer

The session layer is also known as layer 5. These are some of the features mentioned below:

- It exchanger between the application at each end and also set up , sort out and trades happened in this layer.
- It is also responsible for administration, foundation and termination of connection between applications.
- This layer consists of protocols like NFS, SQL and RPC, which has played an important role in this layer.

- It manages association coordination and sessions.

Presentation layer

Presentation layer is also known as layer 6. These are some of the features, which help us in transferring data from source to destination:

- It provides encryption and decoding of the information.
- It is responsible for the information portrayal on the screen.
- It helps us in data semantics and syntax.
- To secure our data it illustrations incorporate encryption, ASCII and so on.

Application layer

Application layer is also known as layer 7. These are some of the features:

- It provides quality of service.
- It underpins application and end client form.
- This also provides us in exchanging of records, email, and other system programming administration.
- Some of the protocols works in this layer are FTP, HTTP, DNS, NTP.

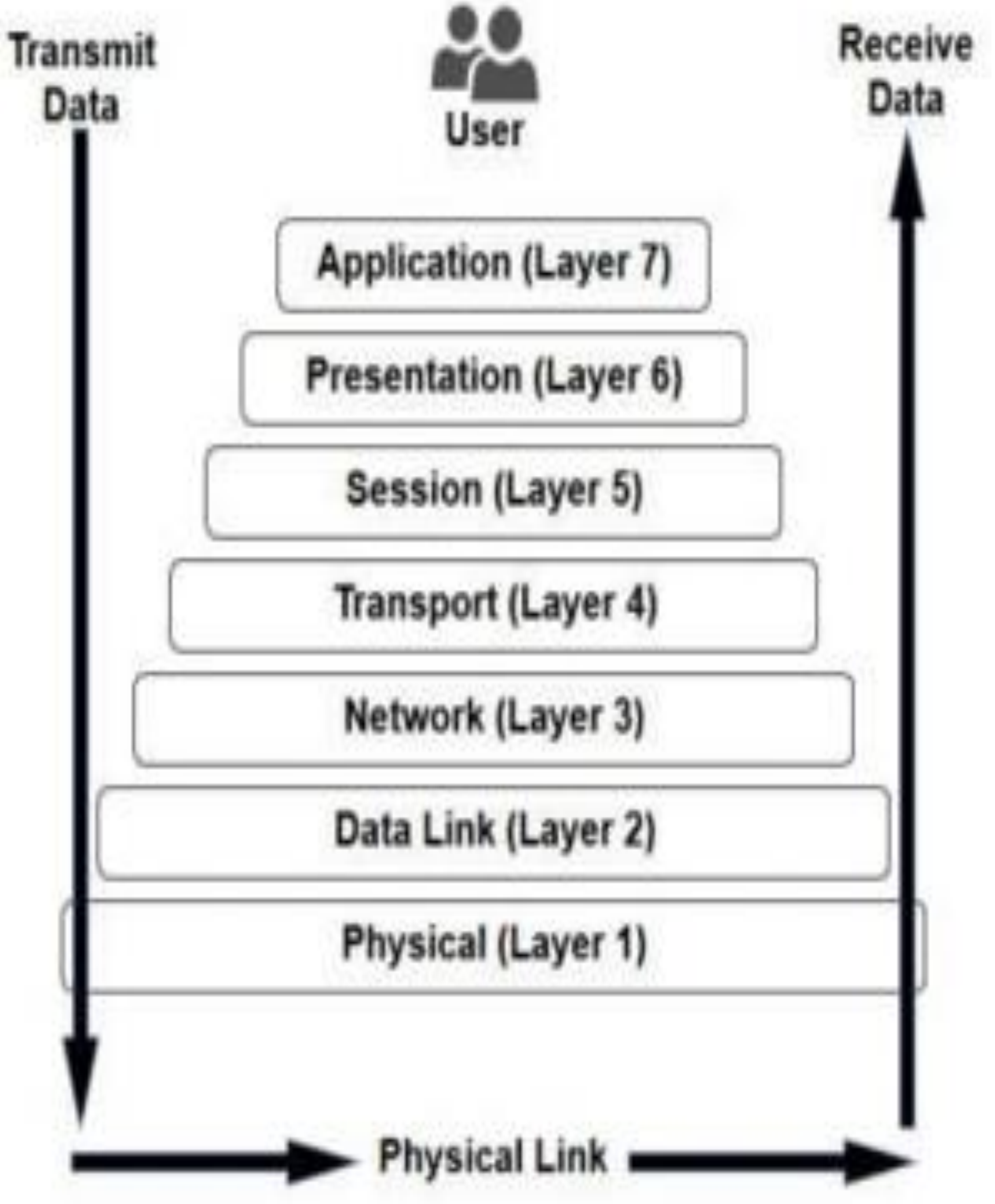


Figure 1.2.2: Layers of OSI Model

CHAPTER 2

LITERATURE SURVEY

1. Minlan Yu and Jennifer Rexford., Xin Sun .,Sanjay Rao., Nick Feamster., "A Survey of Virtual LAN Usage in Campus Networks", IEEE Communications Magazine • July 2011.

- In this paper they surveyed in the four campuses to better understand how VLANs are used in practice.
- The use of VLANs leads to significant complexity in the configuration of the network devices.
- VLANs are used for many objectives that they were not originally intended for and often are ill suited for the tasks, the use of the VLANs complicate network management.
- For the better understanding of VLAN, we have how three-university campus and one academic department are connected and having communication with each other.

2. Hasan, MD.Kamrul, Ahammed, Shamim, "Design and implementation a corporate network using inter –VLAN routing protocol" EWU institutional repository • November 2015.

- In this paper they used the OSPF routing protocol in company network topology, which is useful for real time communication.
- The OSPF protocol provides a high functionality open protocol that allows multiple vendor networks to communicate using the TCP/IP protocol family.
- This paper presents the PRAN RFL GROUP Company having 7 branches and 7 sub branches, every main branches have admin VLAN these VLANs communicating with each other using OSPF Routing protocol.

3. S.Somasundaram, M.Chandran, “A simulation based study on inter –VLAN routing” IJCSE all rights reserved • 2016.

- In this VLAN author have analyzed the importance of inter VLAN routing.
- VLAN is unique broadcast domain so that packets can only delivered between ports with same VLAN group member.
- Inter-VLAN routing is used to permit different VLANs to communicate. Different router interface configurations facilitate inter-VLAN routing.

CHAPTER 3
ROUTING AND ITS PROTOCOLS

3.I NTRODUCTION

In internetworking, the way toward moving a packet of information from source to goal. Device used here is router, which normally performs routing. Router is a device by which routing is done. Router is designed to perform a specific task known as routing. It works on layer 3. Best path is taken while transferring a packet from source to destination. Routing is not possible without layer 3. Routing is used in between two LANs and wide area network. By the help of routing, data of one network reaches to other network. For the delivery of data, unique table is used, that table is known as routing table. By routing table, routers identify which best path is to be taken in sending the data packet from source to destination.

3.2 TYPES OF ROUTING

There are two types of routing that are:

- Static Routing
- Dynamic Routing

3.2.1 STATIC ROUTING

Manual Configuration is done in Static Routing and also known as default routing.
Static routing can be used in following steps:

Static routing may have the accompanying employments:

- Static routing can be utilized to characterize a end point from router when no different routes are important.
- Static routing can be utilized for little networks that require just a single or many routes.
- Static routing is regularly utilized as a part of correlative with dynamic routing to give safeguard reinforcement if a dynamic route is inaccessible.

3.2.2 DYNAMIC ROUTING

Dynamic is related to automatic routing. To find the route, routers does automatically, also known as routing to routing protocol. Routing protocols are configured by administrators on routers. These routing protocols shares the information of routing table in order to send data packets to destination. Examples are RIP, OSPF, and EIGRP etc.

3.3 ROUTING PROTOCOL

A routing protocol determines routes between any two nodes on a PC organize. Routing protocol is divided into two categories that are:

- Interior gateway protocol
- Exterior gateway protocol

3.3.1 INTERIOR GATEWAY PROTOCOL

It is designed for the use inside a single autonomous system. It is categories as

- Distance Vector Routing Protocol – Examples are RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol).
- Link Sate Routing Protocol – Example is OSPF (Open shortest path first)
- Hybrid routing protocol – EIGRP

Routing Information Protocol

Distance specifies how much is the distance covered to send packet from one network to another. Vector specifies in which direction, packet is to be forwarded, covering the distance to reach the destination. In case of routers, vector and directions are indicated as interfaces of routers, which interface is to be used while forwarding the packet. Distance vector routing protocol calculates the distance and the vector to take best path from source to destination. In order to reach the destination it takes route metrics, use hop count as a metrics.

Interior Gateway Routing Protocol

It uses delay and bandwidth as a metrics to forward the packet from source to destination.

Link Sate Routing Protocol

It access router's interface and link state in order to perform routing process, tracks the status of each link and type of connection whether Ethernet, fast Ethernet etc. keep the knowledge of bandwidth on the basis of these factors it calculated metric is produced to perform routing tasks. Some of the factors are set by network administrator. It knows whether the link is in up state or in down state.it decide the path by calculating cost and which link is fast. It does not use hop metrics instead of it, it uses bandwidth develops the calculated metric and routing decision is taken. It uses shortest path first algorithm to formulate the best path taken to destination. Example is OSPF (Open shortest path first)

Enhanced Interior Gateway Routing Protocol

It is the improvement of interior gateway routing protocol and it takes best path or route in order to transfer the data packet from source to destination like other any routing protocol. It is a cisco proprietary protocol, which works only on cisco routers. If we do not have cisco router in our network layout, we can’t use enhanced interior gateway routing protocol, one of the disadvantage of it. It is made up of best feature used in distance vector and link state like simplicity and fast convergence respectively that’s why it is known as mix or hybrid routing protocol. Delay and bandwidth are the factors used as metrics. We apply formula upon them that is diffusing-update algorithm to determine the least cost, more efficient path or route to destination, it uses reliable routing protocol in delivery of packet and uses 88(IP protocol number). It supports classless routing that have any network or host id. In our infrastructure layout we have used enhanced interior gateway routing protocol.

3.3.2 EXTERIOR GATEWAY PROTOCOL

Exterior gateway protocol is designed for the use between the multiple autonomous systems. Example is BGP (Border Gateway Protocol) use it in decision-making.

CHAPTER 4

DESIGN & METHODOLOGIES

SOFTWARE USED: Cisco Packet Tracer 6.2

DESIGN: VLAN based infrastructure

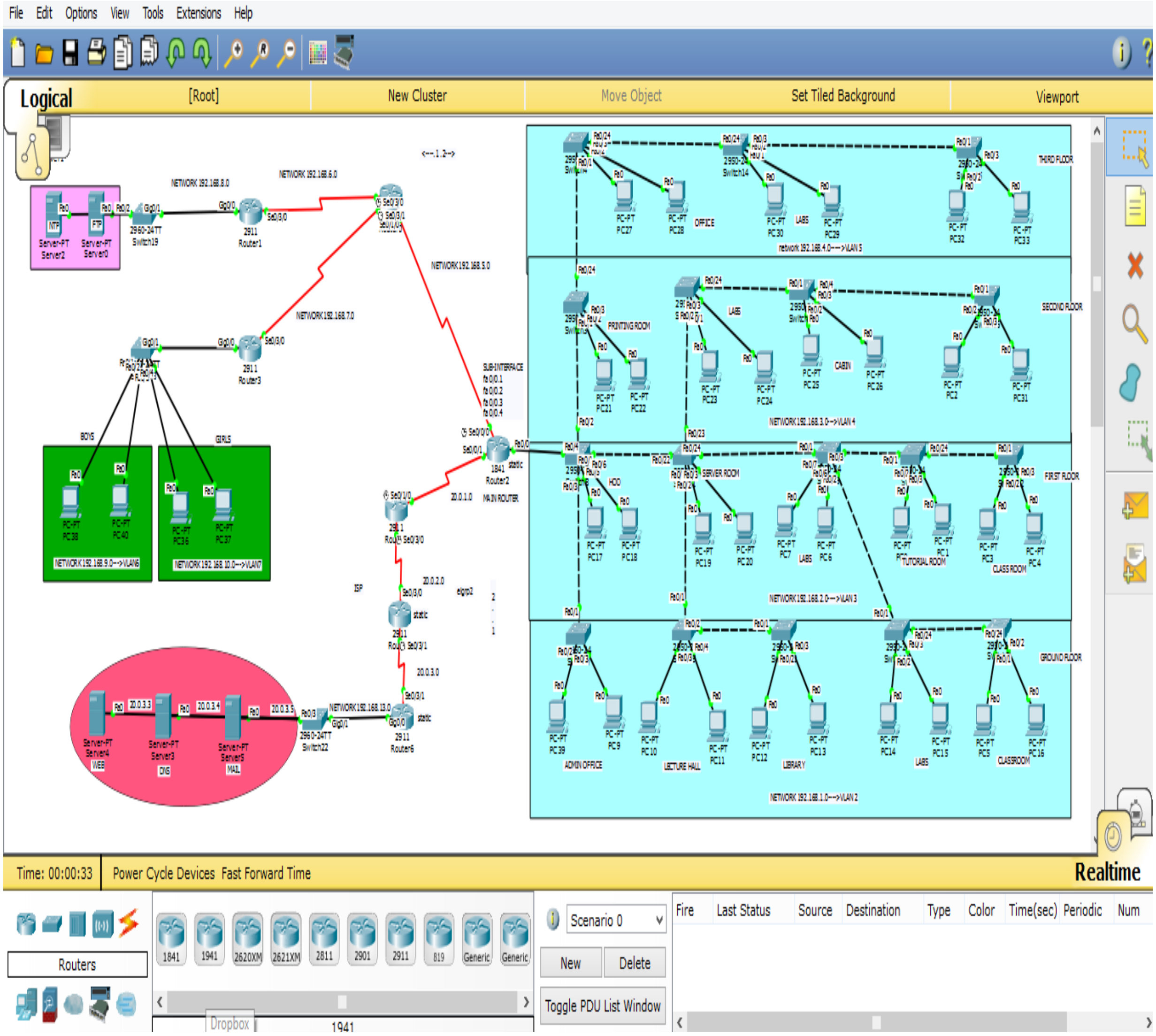


Figure 4.1: Layout

In this campus infrastructure there are four blocks

- Server
- Hostel
- Internet
- Administrative

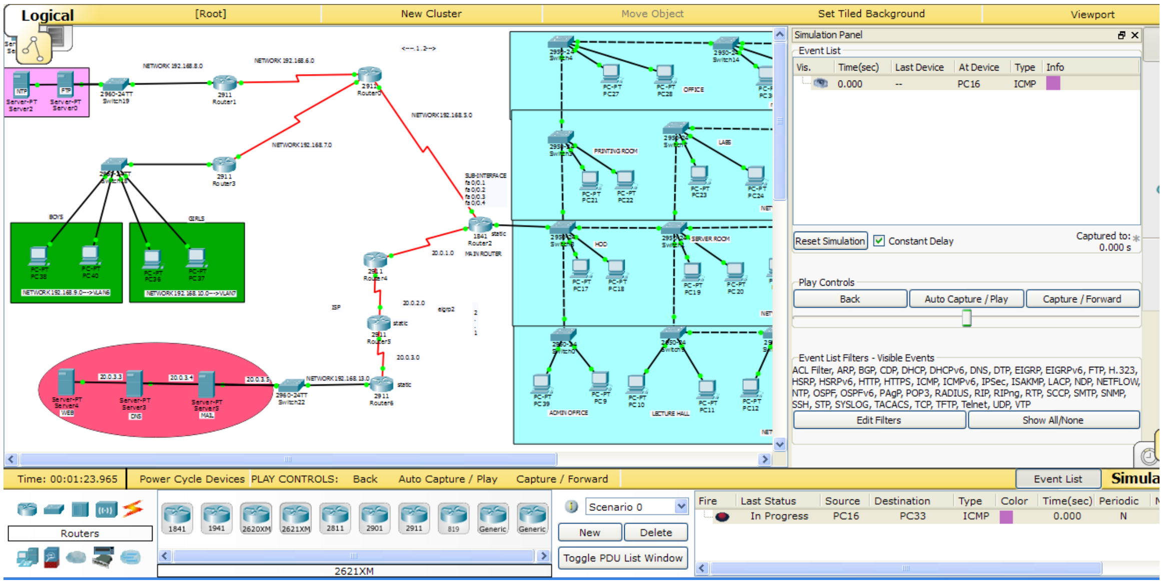
And these blocks are connected to main router.

Administrative Block

- Administrators utilize VLANs to build arrange sections that carry on legitimately like a regular LAN however are autonomous of the physical areas of the hosts.

- Once the VLANs and IP tending to construction has been set, the following key plan choice is the manner by which to convey VLANs into the system foundation.

- VLANs are physically arranged on the switches.

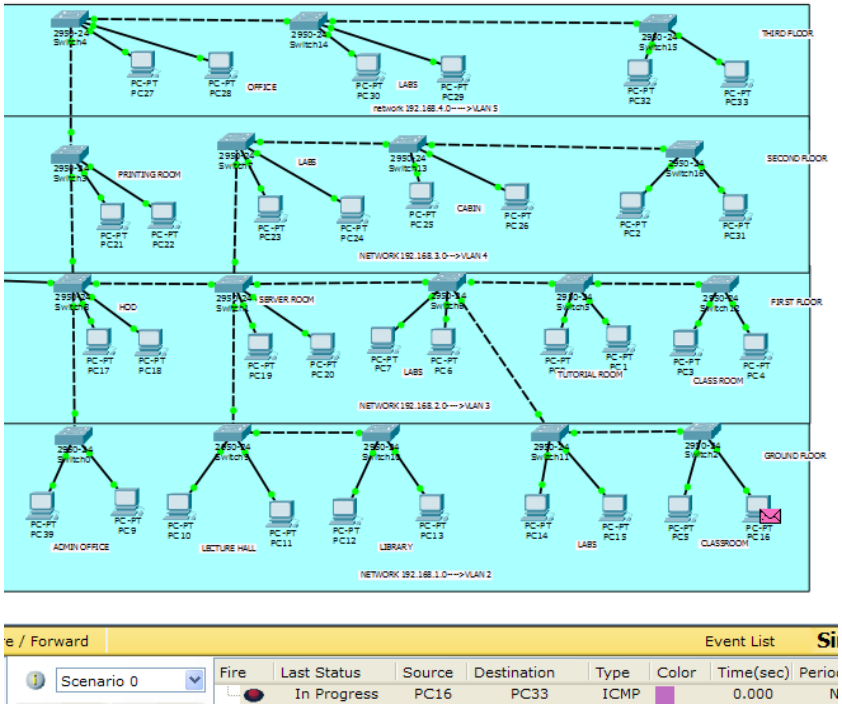


Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC16	ICMP	🟪

ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

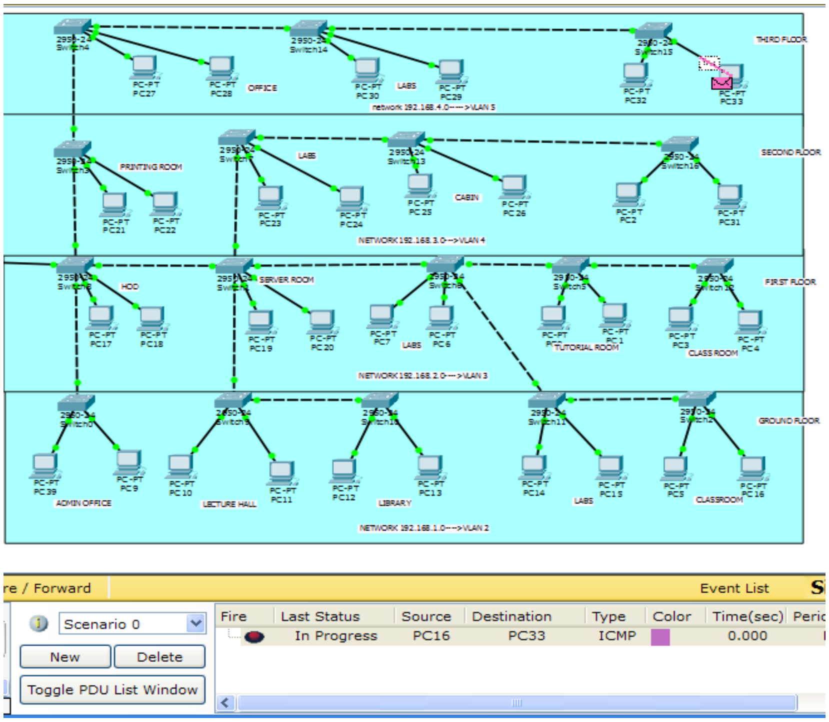
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
●	In Progress	PC16	PC33	ICMP	🟪	0.000	N

Figure 4.2: Simulation Panel



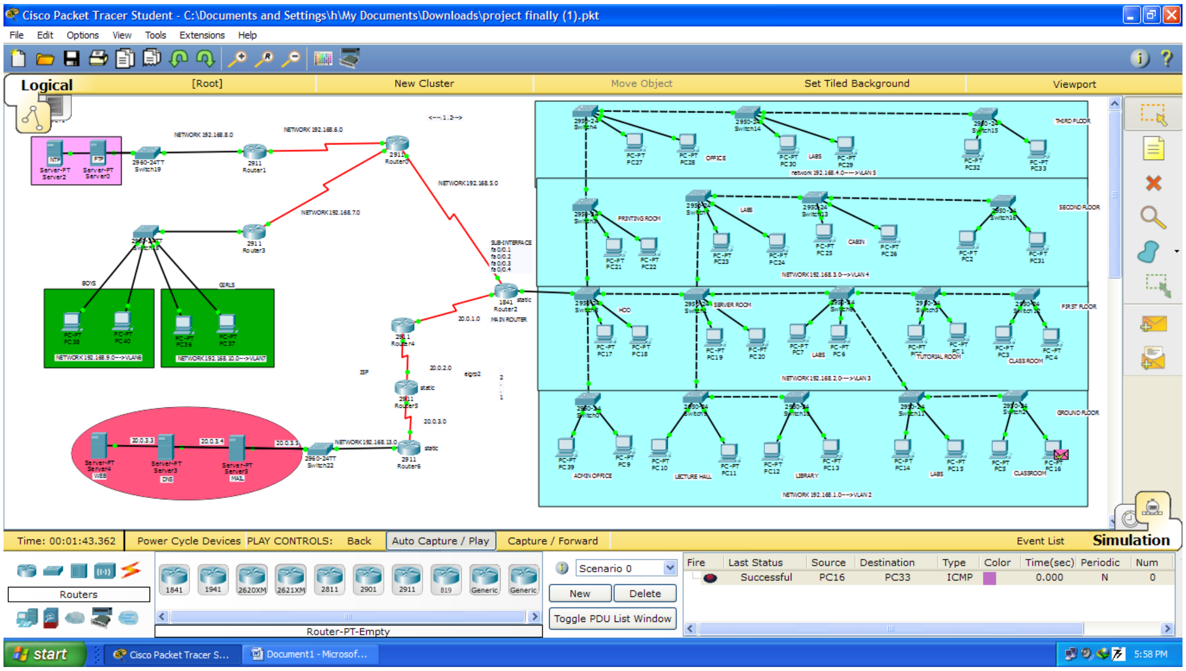
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Perio
●	In Progress	PC16	PC33	ICMP	🟪	0.000	N

Figure 4.3: Data packet is sent from source PC



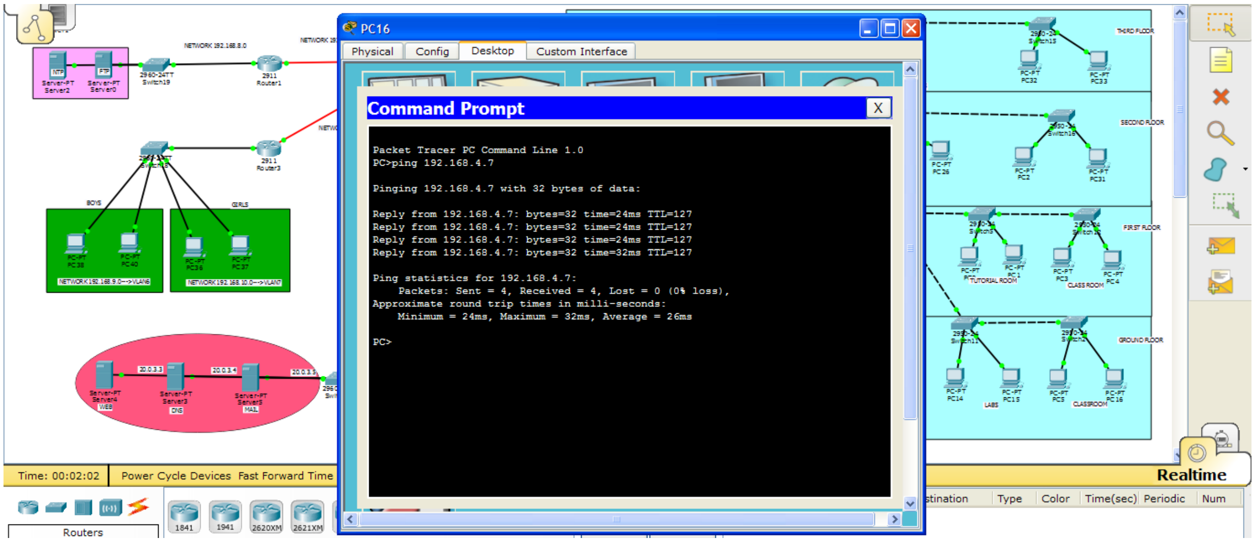
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Peri
●	In Progress	PC16	PC33	ICMP	🟪	0.000	I

Figure 4.4: Data packet is received by destination PC



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	PC16	PC33	ICMP	🟪	0.000	N	0

Figure 4.5: Data packet is acknowledged by source PC



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.4.7

Pinging 192.168.4.7 with 32 bytes of data:

Reply from 192.168.4.7: bytes=32 time=24ms TTL=127
Reply from 192.168.4.7: bytes=32 time=24ms TTL=127
Reply from 192.168.4.7: bytes=32 time=24ms TTL=127
Reply from 192.168.4.7: bytes=32 time=32ms TTL=127

Ping statistics for 192.168.4.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 32ms, Average = 26ms

PC>
```

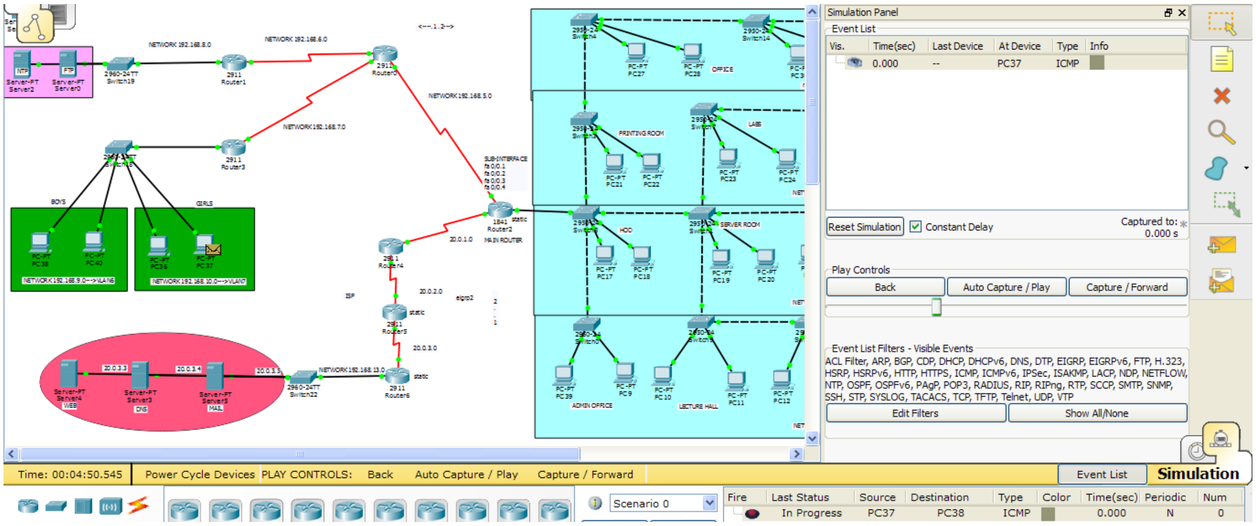
Figure 4.6: Command prompt table

Above figures describe how the data packet is sent from source to destination; sub-interfacing is done on main router to divides the network uniformly on each floor. Figure

3.1, 3.2, 3.3, shows the simulation about how the packet follows the path to reach the destination. Figure 3.4, source gets the acknowledgement of the delivery of data packet, successful in sending the packet from source to destination.

In Figure 3.5, ping command is used to prove the user that the specific IP address exists. In this command prompt packet sent are 4 with no loss.

Hostel Block



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC37	ICMP	

Reset Simulation ☑ Constant Delay

Captured to: 0.000 s

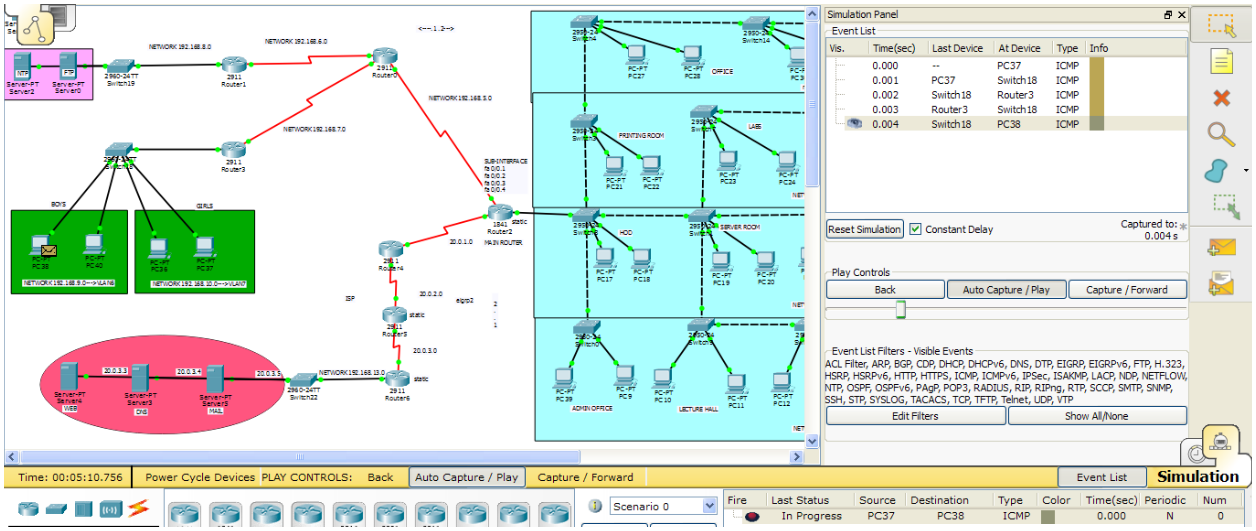
Event List Filters - Visible Events

ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Time: 00:04:50.545

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	In Progress	PC37	PC38	ICMP		0.000	N	0

Figure 4.7: Data packet is sent from source PC



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC37	ICMP	
	0.001	PC37	Switch18	ICMP	
	0.002	Switch18	Router3	ICMP	
	0.003	Router3	Switch18	ICMP	
	0.004	Switch18	PC38	ICMP	

Reset Simulation ☑ Constant Delay

Captured to: 0.004 s

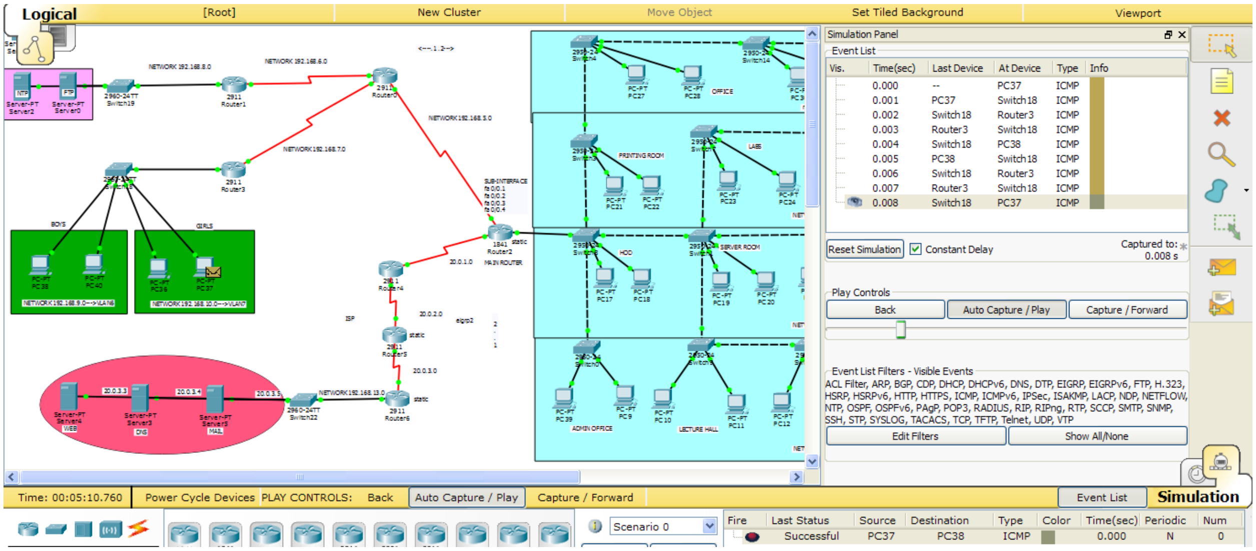
Event List Filters - Visible Events

ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Time: 00:05:10.756

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	In Progress	PC37	PC38	ICMP		0.000	N	0

Figure 4.8: Data packet is received by destination PC



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC37	ICMP	
	0.001	PC37	Switch18	ICMP	
	0.002	Switch18	Router3	ICMP	
	0.003	Router3	Switch18	ICMP	
	0.004	Switch18	PC38	ICMP	
	0.005	PC38	Switch18	ICMP	
	0.006	Switch18	Router3	ICMP	
	0.007	Router3	Switch18	ICMP	
	0.008	Switch18	PC37	ICMP	

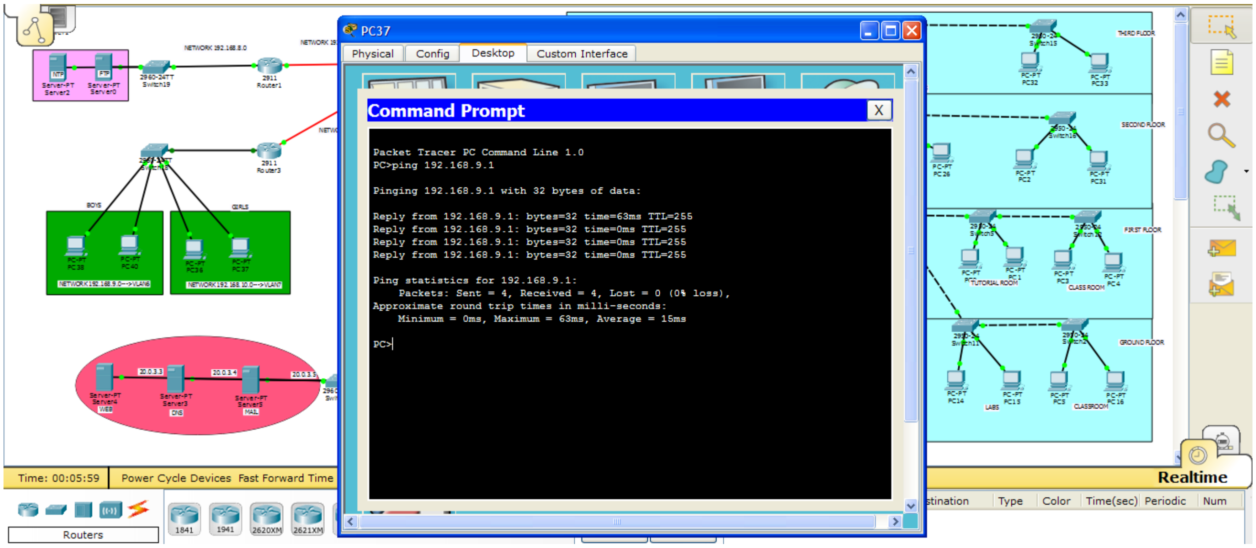
☑ Constant Delay

Captured to: 0.008 s

ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	PC37	PC38	ICMP	■	0.000	N	0

Figure 4.9: Data packet is acknowledged by source PC



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.9.1

Pinging 192.168.9.1 with 32 bytes of data:

Reply from 192.168.9.1: bytes=32 time=63ms TTL=255
Reply from 192.168.9.1: bytes=32 time=0ms TTL=255
Reply from 192.168.9.1: bytes=32 time=0ms TTL=255
Reply from 192.168.9.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.9.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 63ms, Average = 15ms

PC>
```

Figure 4.10: Command prompt table

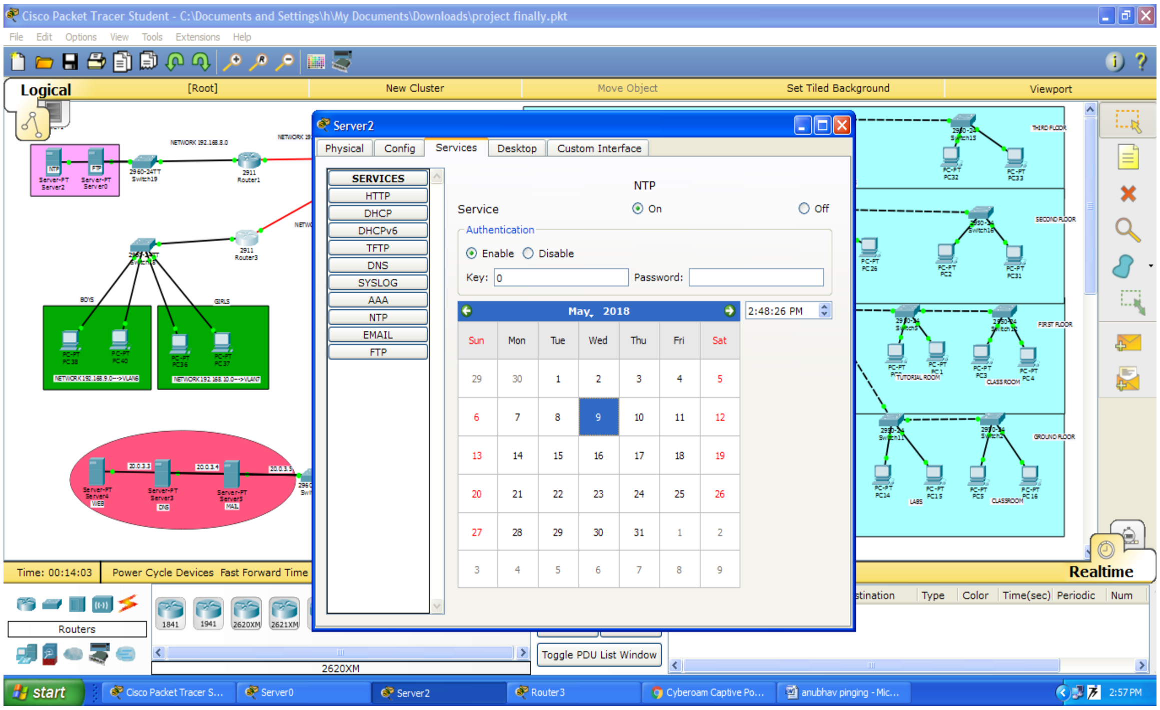
Above Figure 3.6 shows how the data packet is sent from source to destination; sub-interfacing is done on router to divides the network uniformly on each block. Source of data packet is girls block and destination is boys block as shown in Figure 3.7. In Figure 3.8, source gets the acknowledgement of the delivery of data packet.

In Figure 3.9, ping command is used to prove the user that the specific IP address exists. In this command prompt packet sent are 4 with no loss.

Server Block

Sorts of Servers utilized:

- Network Time Protocol (NTP) is a frameworks organization tradition for clock synchronization between PC structures over bundle traded, variable-latency data frameworks.
- File Transfer Protocol (FTP) is used for transferring a document between a client and server. These servers are configured on any routers in my campus infrastructure. We have used these two servers to get a general idea how it works on the respective routers.



NTP

Service ● On ○ Off

Authentication

● Enable ○ Disable

Key: 0 Password:

May, 2018 — 2:48:26 PM

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Figure 4.11: NTP Server

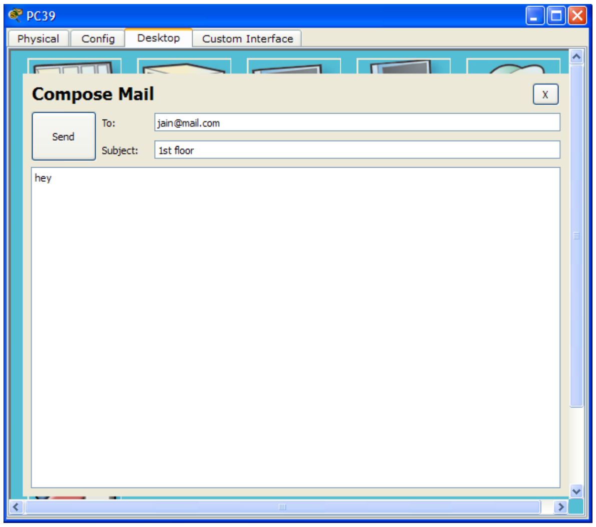
Internet Block

Servers utilized under TCP/UDP Protocol:

- Email Server
- Web Server
- DNS Server

Email Server

Email Clients, for example, Microsoft Outlook, Netscape, and numerous others, associate with TCP port 110 of a remote e-mail server, at that point utilize the pop3 protocol to recover their e-mail. They initially recognize and confirm themselves by signing on to the remote e-mail server utilizing their e-mail account data.

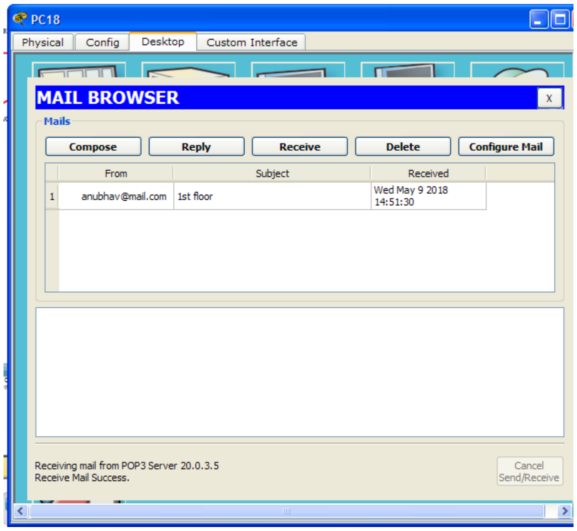


To: jain@mail.com

Subject: 1st floor

hey

Figure 4.12: Sending email



	From	Subject	Received
1	anubhav@mail.com	1st floor	Wed May 9 2018 14:51:30

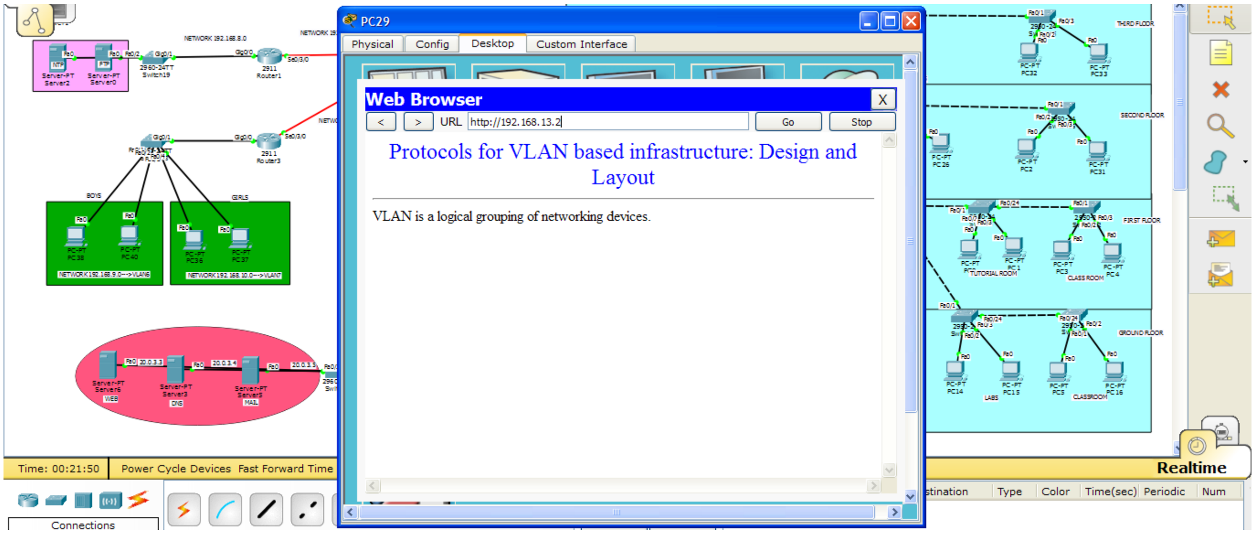
Receiving mail from POP3 Server 20.0.3.5
Receive Mail Success.

Figure 4.13: Receiving email

In the above Figure 3.11 showing that the email is sent from PC39 of ground floor and is received by PC18 of first floor.

Web Server

Tune in on TCP port 80 to serves the content to World Wide Web.



http://192.168.13.2

Protocols for VLAN based infrastructure: Design and Layout

VLAN is a logical grouping of networking devices.

Figure 4.14: Web browser

In the above Figure 3.11, A Web server that make use of Hypertext Transfer Protocol to serve the records that frame Web pages to clients, which are sent by their PCs' HTTP clients.

DNS Server

DNS servers tune in on UDP port 53 for inquiries from DNS client.

CHAPTER 5

RESULTS

5.1 OUTPUT

In Figure 3.6, ping statistics for 192.168.4.7 with 32 bytes of data are:
(ADMINISTRATIVE BLOCK)

Packets: Sent = 4, Received = 4, LOST = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 24ms, Maximum = 32ms, Average = 26ms

In Figure 3.10, ping statistics for 192.168.9.1 with 32 bytes of data are:
(HOSTEL BLOCK)

Packets: Sent = 4, Received = 4, LOST = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 63ms, Average = 15ms

5.2 SIMULATION RESULT ANALYSIS

In every Inter-VLAN routing configuration is zero percentage loss or error. Communication between two blocks (Administrative Block And Hostel Block) without data frame loss. Every student can communicate with better security.

CHAPTER 6

CONCLUSION

In campus infrastructure, we have used EIGRP routing protocol, as it is more flexible than OSPF, it has fast convergence over RIP and IGRP. Link bandwidth and delay is used in EIGRP.

256*SAME IGRP metric → more granular

As shown in Figure 3.1 displaying the campus infrastructure, there are four blocks

- Server
- Hostel
- Internet
- Administrative

And these blocks are connected to main router.

In Administrative Block, it consists of 4 floors given different network manually and configuration of VLAN is done on each and every switch. Cross cable is used to connect PC's with the switch; trunking is done between two switches and between router and switch. Access link is configured in respective floor (ground floor, first floor, second floor and third floor) given VLAN 2,3,4,5 respectively in each separate floor, packet has been sent from source and received by the destination successfully.

In Hostel Block, it consists of 2 blocks (girls block and boys block) are given different network manually and configuration of VLAN is done on a single switch. The packet has been sent from source and received by the destination successfully from boys hostel to girls hostel and vice versa.

To send the packet from Administrative Block to Hostel Block and vice-versa, Enhanced Interior Gateway Routing Protocol has been used. Packets has been successfully transmitted and received by the different PCs of Administrative Block and Hostel Block.

In server block, consists of two servers FTP and NTP , basic knowledge about how they works.

In Internet Block, consists of 3 servers that are Web Server, DNS Server, Email Server. Each server has its own significance. Router has been placed outside the Internet Block, we use NAT(Network Address Translation) on that particular router, in order to translate private IP’s to public IP’s.To get an access for Internet we need Internet Service Provider (ISP) and public IP address is unique. POP3 protocol is used in sending and receiving mail. Therefore how the email is sent from one computer to another computer same as Microsoft outlook, how to get an access of Internet to nearby PC’s. DNS server plays an important role in among all the servers as Internet domain name has been translated into IP address successfully.

REFERENCES

[1] Minlan Yu and Jennifer Rexford., Xin Sun .,Sanjay Rao., Nick Feamster., “A Survey of Virtual LAN Usage in Campus Networks”, IEEE Communications Magazine • July 2011.

[2] Sun litan., “The Application on VLAN in College Library Network”,IEEE xplore • August 2010.

[3] V.Rajaravivarma, “ Virtual local Area Network Technology and Applications” IEEE xplore • August 2002.

[4] Xiaoying Wang, “Research and implementation of VLAN based on service “ IEEE xplore • 2004.

[5] Hasan, MD.Kamrul,Ahammed, Shamim, “Design and implementation a corporate network using inter –VLAN routing protocol” EWU Institutional Repository • November 2015.

[6] Zeng xjyang, “Research on VLAN technology in l3 switch” IEEE xplore • December 2009.

[7] S.Somasundaram, M.Chandran, “A Simulation based study on Inter –VLAN Routing” IJCSE all rights reserved • 2016.

[8] Minli Zhu, Mart Molle, “Design and implementation of application-based secure VLAN “, Proceedings of the 29th Annual IEEE International Conference on Local Computer • November 2004.

[9] Xiaoying Wang, Hai Zhao Mo Guan, Chengguang Guo, jiyong Wang,” Research And Implementation of VLAN based on service”, Proceeding of the Global Telecommunications Conference • December 2003.

[10] Xin Sun, Yu-Wei Sung, Krothapalli, S.D., Rao, S.G., “A Systematic Approach for Evolving VLAN Designs”, Proceedings of the IEEE INFOCOM 2010 • March 2010.

[11] Jiajia liu, “Security Analysis of VLAN-Based Virtual Desktop Infrastructure “, IEEE xplore • July 2010.