CHAPTER 1

Introduction

1.1 Introduction

A Virtual LAN is a logical switched LAN formed by segmenting physical Local Area Networks. Virtual LANs offer a method of dividing one physical network into multiple broadcast domains. However, VLAN-enabled switches cannot, by themselves, forward traffic across VLAN boundaries' a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but will allow broadcasts and multicasts (to a pre- specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network.

In order to create a virtual LAN, the network equipment, such as routers and switches must support VLAN configuration. The hardware is typically configured using a software admin tool that allows the network administrator to customize the virtual network. The admin software can be used to assign individual ports or groups of ports on a switch to a specific VLAN. For example, ports 1-12 on switch #1 and ports 13-24 on switch #2 could be assigned to the same VLAN.

1.2 Objectives

1.Performance, VLAN's can reduce the need to send such traffic to unnecessary destination. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic

2.Formation of Virtual workgroups, it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building.

3.Reduced Cost, VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

4.Security, VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion

5.Network management, VLAN Easley manage developed network from main center .

1.3 Justification of study

After successful experiments with voice over Ethernet from 1981 to 1984, Dr. W. David Sincoskie joined Bellcore and began addressing the problem of scaling up Ethernet networks. At 10 Mbit/s, Ethernet was faster than most alternatives at the time. However, Ethernet was a broadcast network and there was no good way of connecting multiple Ethernet networks together. This limited the total bandwidth of an Ethernet network to 10 Mbit/s and the maximum distance between nodes to a few hundred feet.By contrast, although the existing telephone network's speed for individual connections was limited to 56 kbit/s (less than one hundredth of Ethernet's speed), the total bandwidth of that network was estimated at 1 Twit/s [citation needed] (100,000 times greater than Ethernet). Although it was possible to use IP routing to connect multiple Ethernet networks together, it was expensive and relatively slow. Sincoskie started looking for alternatives that required less processing per packet. In the process he independently reinvented transparent bridging, the technique used in modern Ethernet switches. [6] However, using switches to connect multiple Ethernet networks in a fault-tolerant fashion requires redundant paths through that network, which in turn requires a spanning tree configuration. This ensures that there is only one active path from any source node to any destination on the network. This causes centrally located switches to become bottlenecks, limiting scalability as more networks are interconnected.

To help alleviate this problem, Sincoskie invented VLANs by adding a tag to each Ethernet frame. These tags could be thought of as colors, say red, green, or blue. In this scheme, each switch could be assigned to handle frames of a single color, and ignore the rest. The networks could be interconnected with three spanning trees, one for each color. By sending a mix of different frame colors, the aggregate bandwidth could be improved. Sincoskie referred to this as a multitree bridge. He and Chase Cotton created and refined the algorithms necessary to make the system feasible. [7] This color is what is now known in the Ethernet frame as the IEEE 802.1Q header, or the VLAN tag. While VLANs are commonly used in modern Ethernet networks, they are not used in the manner first envisioned here in 2003, Ethernet VLANs were described in the first edition of the IEEE 802.1Q standard. [8] This was extended with IEEE 802.1ad to allow nested VLAN tags in service of provider bridging. This mechanism was improved with IEEE 802.1ah-2008.

A Local Area Network (LAN) was originally defined as a network of computers located within the same area. Today, Local Area Networks are defined as a single broadcast domain. This means that if a user broadcasts information on his/her LAN, the broadcast will be received by every other user on the LAN. Broadcasts are prevented from leaving a LAN by using a router. The disadvantage of this method is routers usually take more time to process incoming data compared to a bridge or a switch. More importantly, the formation of broadcast domains depends on the physical connection of the devices in the network. Virtual Local Area Networks (VLAN's) were developed as an alternative solution to using routers to contain broadcast traffic.

1.4 Scope of study

1) VLAN usage in campus networks
2) Scoping broadcast traffic
3) Limiting the broadcast/flooding overhead
4) Protecting security and privacy
5) Simplifying access control policies
6) Imposing access control policies
7) Concise access control lists
8) Preventing source IP address spoofing
9) Preventing source IP address spoofing
10) Decentralizing network management
11) Decentralizing network management
12) Easier troubleshooting
13) Enabling host mobility
14) Performance, VLAN's can reduce the need to send such traffic to unnecessary destination. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic.
15) Formation of Virtual workgroups, it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building.
16) Reduced Cost, VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.
17) Security, VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion
18) Network management, VLAN Easley manage developed network from main center.

A network has been designed that represents a real time environment of an organization. The organization has been subdivided into different departments by implementing VLANs for proper management. Also, these different departments can communicate with each other using Inter VLAN Routing for controlled flow of information. VLANs divide broadcast domains in a LAN environment. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as inter-VLAN routing. Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data.

CHAPTER 2

Literature review

2.1 Introduction

Since VLAN technology is relatively new, and is different from vendor to vendor, it is not surprising that there is sparse mention of the technology in the literature. However, there is more extensive literature available on networking in general, the problems that VLANs are intended to solve, the networking issues, such as network security, that they are intended to address, and the network applications that VLANs can enhance. The different vendors of VLAN systems have also published information, in the form of white papers and other material regarding VLAN technology in general and their solutions in particular. Additional literature includes background information on computing and networking at UNC-Chapel Hill. The UNC-CH literature will provide a comparison between both the old and new networking technology as well as between old and new roles and policies for the ATN department at UNC.

2.2 Theoretical Under-pinning of the Study

A complete discussion of networking is beyond the scope of this paper. However, Derfler and Freed (1996) usefully define many of the terms used in discussing networks. A local area network (LAN) is "a group of computers typically connected by no more than 1,000 feet of cable, which interoperate and allow people to share resources." A network interface card (or LAN adapter) is the device which packages data for transmission and acts as "a gatekeeper to control access to the shared network cable." Network interface cards break data streams into packets, which are reassembled at the destination. Bridges segment LANs or join LANs together; they act to control traffic by learning the "station address" of each machine on the networks in question, and only send a packet across the bridge if the destination of the packet is a station on the other side. Routers function similarly to bridges but look at the network address of packets and use routing algorithms to send the packet to its destination efficiently. Henry and De Libero (1996) describe the use of switching to divide the network into smaller segments. Switching helps to reduce then number of nodes trying to use the same network segment, resulting in lower congestion on each segment. In switched hubs or bridges, each node can have its own network segment, and therefore have access to all of the network bandwidth of the segment. Switching bridges can look deep into a packet and use protocol information and the like to provide a level of filtering and prioritization (Henry and De Libero, 1996).

2.3 Networking problems and issues

Virtual local area networks address and attempt to solve many of the issues and problems facing network administrators, particularly on large, enterprise-wide networks. Some common issues include network utilization, particularly collisions and broadcasts, and network security. In addition, administrators want to reduce the amount of time and resources required to perform "moves, adds, and changes" to the workstations on a network; such activities often take up a disproportionate amount of an administrator's time and resources.

2.4 Network utilization

Of particular interest to network administrators is the area of network utilization. Network utilization describes the percentage of available network resources that are being used by end stations on the network. Martin, Chapman, and Leben (1994) and Tittel and Robbins (1994) provide a great deal of information on general networking theory, including the issue of network utilization. The most common type of network, Ethernet, allows any station to transmit information on the network as long as no other station is currently transmitting. However, it is possible for two or more stations to simultaneously "sense" that the network is clear and transmit at the same time, causing a collision. While Ethernet and other network protocols include methods for dealing with collisions, the larger the network (i.e. the more users it supports), the higher the frequency of collisions (Martin et al., 1994). As network activity increases, the frequency of collisions can severely degrade network speeds, to the point that the network may seem to have stopped working. Comer (1995) and Chappell and Hakes (1994) describe a feature of local area networks that is related to the problem of collision frequency and its impact on network utilization: the propagation of "useless" network traffic. All signals from a station on a given network are sent to all other stations on the network, regardless of whether they are intended for a station or whether that station can even interpret those signals (Comer, 1995). The designers of Ethernet had the foresight to place the destination address at the beginning of each Ethernet packet (Comer, 1995), and thus the network interface on a particular workstation can rapidly determine whether or not a packet is addressed to it. Packets addressed to other stations can be examined and discarded with minimal use of system resources. However, the Ethernet protocol itself (Comer, 1995) and several higher-level protocols, such as NetWare's IPX/SPX (Chappell & Hakes, 1994) utilize packets that are designed to be received and processed by all interfaces on a network. These packets have a special "broadcast address" instead of the destination address of a single station. When a workstation's network interface receives such a packet, it does not discard the packet based on its destination address; it examines it further to determine what action should be taken. If the interface "speaks" the protocol for which the packet is used, it takes action on the packet's contents; otherwise, the packet is discarded. Determining whether or not a broadcast packet should be discarded requires that the receiver look many bytes deeper into the packet, with a correspondingly greater use of CPU cycles. Roese (1998) discusses the particular problems associated with a "flat," switched

network. Unlike large-scale networks consisting of subnetworks connected through a series of routers, a flat network is essentially one large broadcast domain. While this does have some advantages over traditional, routed networks, namely higher-speed connections between segments, lower cost of networking equipment, and lower administrative overhead, flat networks do have disadvantages as compared to routed networks. According to Roese, connecting switches as routers are connected, with multiple possible paths from one point to another, can lead to "loops" in the network, wherein broadcast packets propagate infinitely, creating "broadcast storms" that can severely degrade network performance.

2.5 Network security

Baker (1995) discusses a broad range of topics related to network security. He provides a good summary of the network security problem. “Good” networks should operate smoothly with other networks, be transparently to users, provide remote access, and maintain peak performance. On the other hand, “secure” networks protect confidential information, keep network performance reliable, and emphasize data integrity. The two dimensions are often at odds (Baker, 1995). Most of what Baker terms “network security” would be more precisely called “server security.” He is more concerned with securing machines on a network than the network itself. Such a focus is appropriate, since common sense tells us that the targets of most malicious attacks are end stations and the data that reside in them, rather than the network itself. However, network abuses (and misuses) do occur, and in any event the means of accessing a server for purposes of breaching security is often a network (Baker, 1995). Network hardware, such as switches and routers, can implement some kinds of security, such as routing traffic in such a way that it travels by the most direct path, thereby minimizing the chance of interception. They can also implement security-oriented functions such as authentication and encryption (Baker, 1995).

2.6 Capabilities

Most literature on VLANs available today comes from vendors who are supplying VLAN technologies. As mentioned earlier, no fully qualified standards exist for defining VLAN implementation; thus definitions are often different from vendor to vendor. One third-party source for VLAN information is the UC-Davis Network 21 initiative (1998). It defines much of the terminology involved in discussing VLANs, and includes a discussion of the uses of VLANs, especially with regard to an academic network. The only VLAN-related standard currently under development comes from the Institute of Electrical and Electronics Engineers (IEEE). Their standard, "IEEE P8021.Q, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Networks" (Institute of Electrical and Electronics Engineers, 1998), describes enhancements to the 802.x LAN/MAN standards for packet structure. The standard (from here on abbreviated to "802.1Q") complements the 802.1p standard for inter-bridge/switch communication, which includes the "Spanning Tree" algorithm used to eliminate network loops

and broadcast storms. The packet structure of the major IEEE-defined network architectures (Ethernet, Token Ring, etc.) are redefined by 802.1Q to include "tags" that further describe the contents of the packet (IEEE, 1998.) The 802.1Q standard dos not, however, define the actual content of these tags under the current draft; rather, it simply "makes room" for the tags in the existing packet structure. A relatively unbiased overview of VLAN technology comes from Passmore and Freeman (1998), writing a white paper for 3Com, Inc. VLANs, they say, “represent an alternative solution to routers for broadcast containment, since VLANs allow switches to also contain broadcast traffic (p. 2)." While many enterprises have used switches to segment their networks, standard switches do not stop broadcast traffic. VLAN technology allows broadcast containment without the high cost and speed penalty of routers. Passmore and White also discuss the typical reasons enterprises do not readily adopt VLAN technology:

- ✓ They are proprietary solutions, which are “anathema” (p. 2) to the networking market, which emphasizes open systems and interconnectivity.

- ✓ VLANs add additional cost, both visible and hidden, to the administration of a network
- ✓ VLANs can impede full-speed access to centralized servers.

Passmore and White divide VLANs into four categories, based on the means by which they assign stations to a given VLAN: port grouping, MAC-layer grouping, network-layer grouping, and multicast grouping. Cisco Systems (Virtual LAN communications, 1996) views VLAN technology (at least, their version of it) as providing flexibility in organization and greater segmentation of an enterprise’s network. Cisco concentrates on port grouping, in which the port to which a user connects her or his workstation is grouped together with the ports of other users in her or his workgroup. Thus, members of the same workgroup (the example in the text is the Accounting department) can work in different locations throughout the organizations, be it different floors, offices, buildings, or even campuses, and still connect to each other as if on the same physical network. Finally, Cabletron Systems (1998), in a series of white papers and technical documentation, and Roese and Knapp (1997) describe Cabletron's proprietary VLAN system, SecureFast Virtual Networking. SecureFast implements a tagging system similar to that proposed by the IEEE's 802.1Q standard, but with some enhancements, such as utilizing both the source and the destination address in determining packet routing (Roese & Knapp, 1997).

CHAPTER 3

Methodology

3.1 Methodology

Methodology is the systematic, theoretical analysis of the methods applied to a field of study. It comprises the theoretical analysis of the body of methods and principles associated with a branch of knowledge. Typically, it encompasses concepts such as paradigm, theoretical model, phases and quantitative or qualitative techniques.

A methodology does not set out to provide solutions - it is, therefore, not the same as a method. Instead, a methodology offers the theoretical underpinning for understanding which method, set of methods, or so-called “best practices” can be applied to specific case, for example, to calculate a specific result.

3.2 Justification of Methodology

1.The network designer and implementer can obtain feedback from the users early in the project

3.It also allows the network engineer some insight into the accuracy of initial project estimates and whether the deadlines and milestones proposed can be successfully met.

3.3 Description of methodology

The Prototyping Model is a systems development method (SDM) in which a prototype (an early approximation of a final system or product) is built, tested, and then reworked as necessary until an acceptable prototype is finally achieved from which the complete system or product can now be developed.

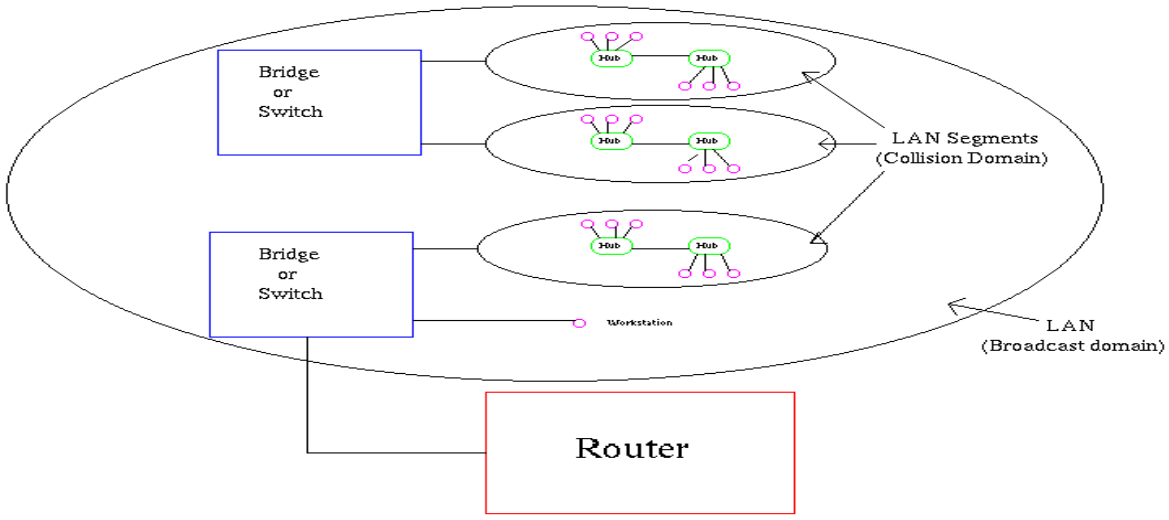

Figure: 3.3 Prototype Model

3.4 Advantages and Disadvantages of methodology

Advantages:

1. Users are actively involved in the development.
2. Since in this methodology a working model of the system is provided, the users get a better understanding of the system being developed.
3. Errors can be detected much earlier.
4. Quicker user feedback is available leading to better solutions.
5. Missing functionality can be identified easily.
6. Confusing or difficult functions can be identified.
7. Requirements validation, Quick implementation of, incomplete, but functional, application.
8. Organization will have source code.
9. Only contains those features that are needed
10. Provides exact requirements

Disadvantages:

1. Leads to implementing and then repairing way of building systems.
2. Practically, this methodology may increase the complexity of the system as scope of the system may expand beyond original plans.
3. Incomplete application may cause application not to be used as the full system was designed
4. Incomplete or inadequate problem analysis.
5. May be excessively costly.
6. Untried software may have performance problems.
7. Untried software may have compatibility problems.
8. First generation software is usually immature.
9. Will generally require development of training and help material from scratch.
10. May not meet user requirements because of poor analysis or design specifications.

CHAPTER 4

Analysis Design and Development

4.1 Requirement gathering Techniques

Requirement gathering technique of resource availability that may affect the ability to achieve an acceptable system. This evaluation determines whether the technology needed for the proposed system is available or not.

1.Can the work for the project be done with current equipment existing network technology & available personal?

2.Can the system be upgraded if developed?

3.If new technology is needed then what can be developed?

This is concerned with specifying equipment and software that will successfully satisfy the user requirement. The technical needs of the system may include:

A. Draw network design.
B. Configuration End Device with Router, Switch.

Front end Selection

1.It must have a graphical user interface that assists employees that are not from IT backgrounds.

2.Scalability and extensibility.

3.Flexibility

4.Robustness

5.According to the organization requirement and the culture

6.Must provide excellent reporting features with good printing support

7.Platform independent

8.Easy to maintain

9.Easy to network design

10.Front end must support some popular back end like Packet Tracer. According to the above features we selected Cisco Packet Tracer as the front end for developing my project.

Back end selection

1.Multiple user support

2.Efficient data handling

3.Provide inherent features for security

4.Efficient data retrieval and maintenance

5.Stored procedure

6.Popularity

7.Operating system compatible

8.Easy to install

9.Easy to implement with the front end

10.According to above stated features we selected Packet Tracer as the backend.

The technical feasibility is frequently the most difficult area encountered at this stage. It is essential that the process of analysis and definition be conducted in parallel with an assessment to technical feasibility. It centers on the existing computer system (hardware, software etc.) and to what extent it can support the proposed system.

4.2 Analysis of Requirements

Hardware requirements:

Processor: Core i3 or Above

Operating System: Windows XP/7/8/10

RAM: Minimum 4GB or Above

Hard Disk: 500 GB or Above

Software requirements:

Front End: cisco Packet Tracer Software.

Back End: Cisco Packet Tracer Software.

4.3 Entity Relationship Diagram (ERD)

An entity-relationship diagram (ERD) is a data modeling technique that graphically illustrates an information system's entities and the relationships between those entities. An ERD is a conceptual and representational model of data used to represent the entity framework infrastructure.

The elements of an ERD are: Entities, Relationships, Attributes.

Steps involved in creating an ERD include:

1.Identifying and defining the entities

2.Determining all interactions between the entities

3.Analyzing the nature of interactions/determining the cardinality of the relationships

4.Creating the ERD

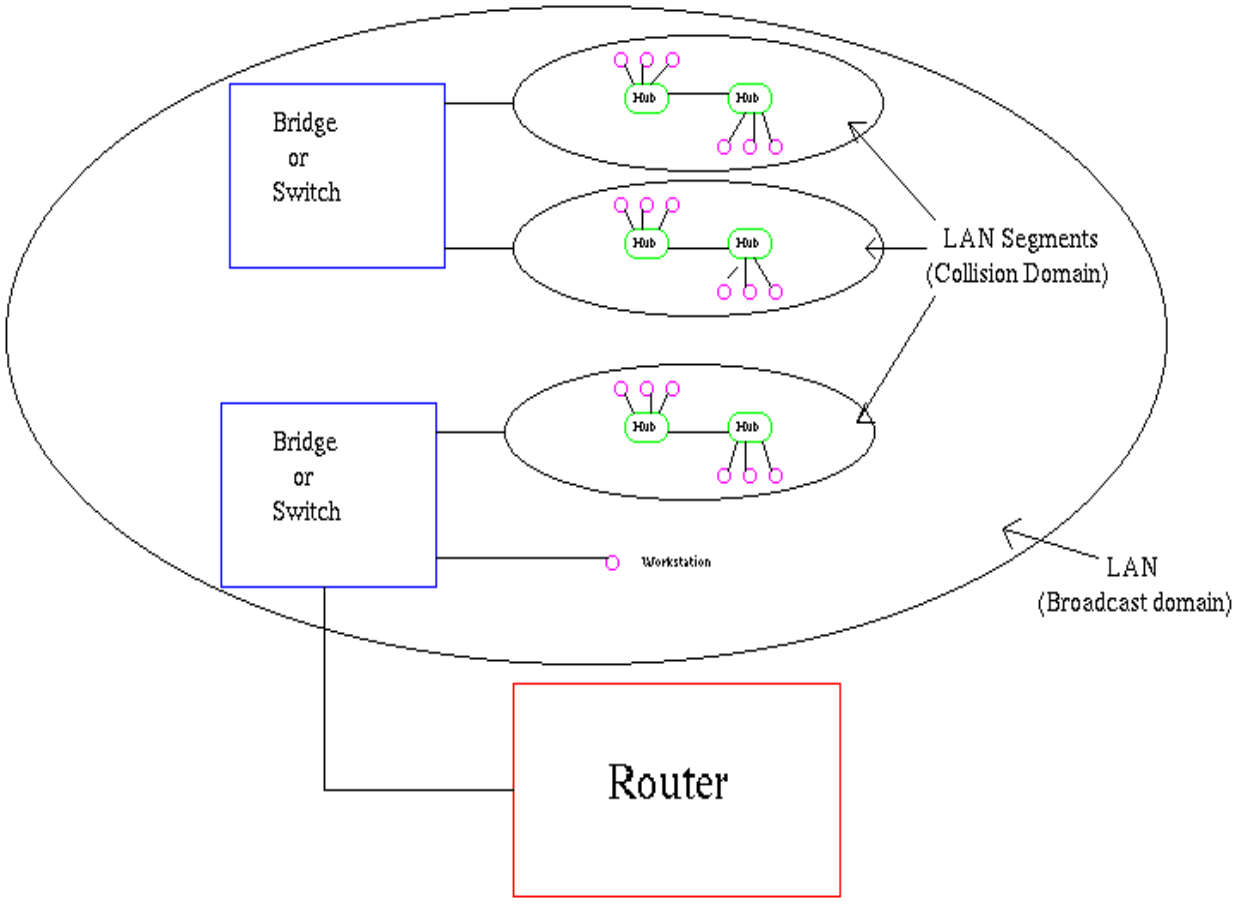

Figure: 4.3 Entity Relationship Diagram (ERD)

4.4 Data Flow Diagram (DFD)

The data flow diagram is a graphical representation of the flow of data through an information system. It enables you to represent the process in your information system from the viewpoint of data.

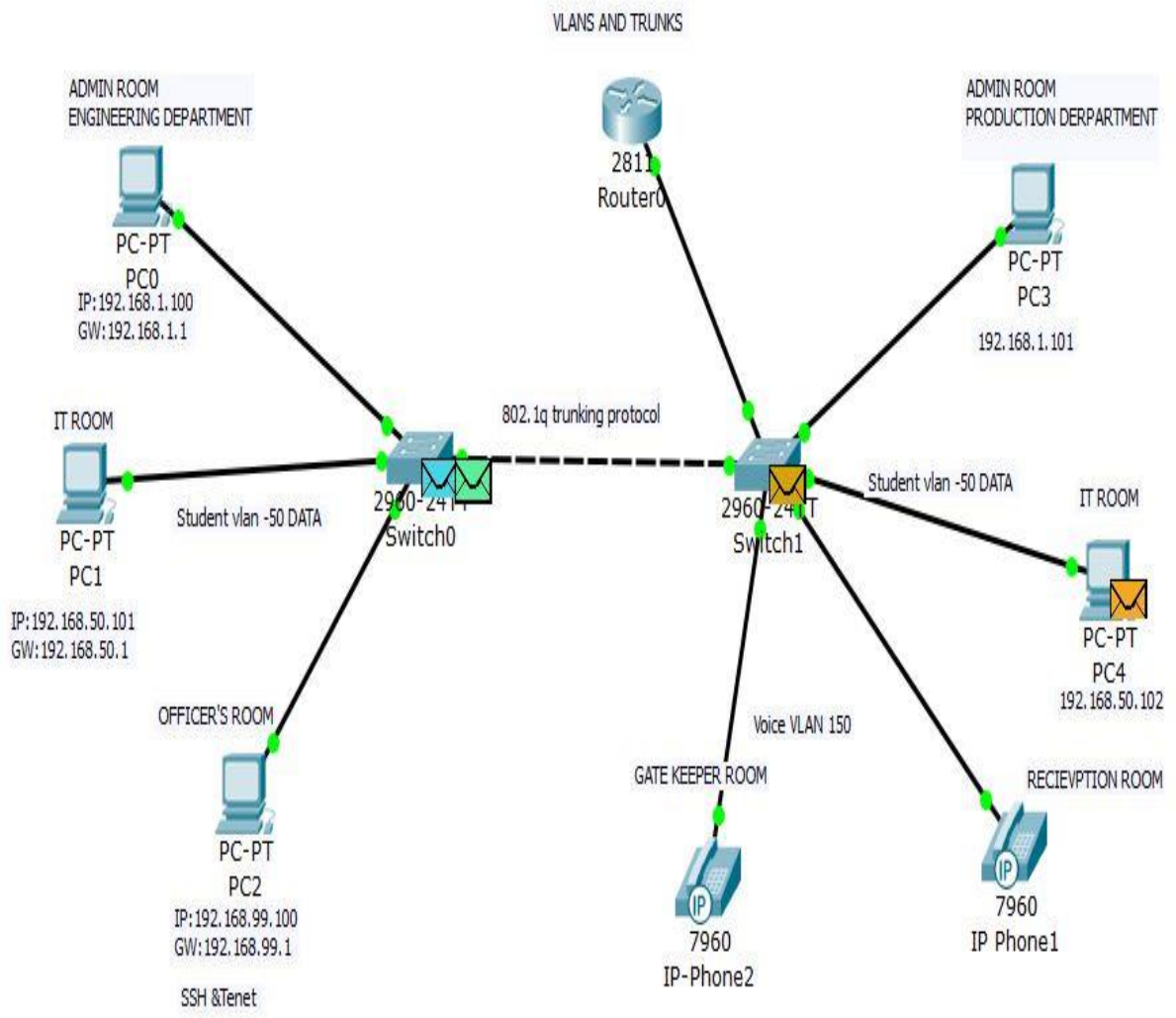

Figure: 4.4 Data Flow Diagram (DFD)

4.5 IP Plan for this Project VLANS

An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network. The IP address is the core component on which the networking architecture is built; no network exists without it. An IP address is a logical address that is used to uniquely identify every node in the network.

Branch Name	IP Address	Gateway
IT ROOM	192.168.50.101	192.168.50.1
IT ROOM	192.168.50.102	192.168.50.1
OFFICER ROOM	192.168.99.100	192.168.99.1
ADMIN ROOM	192.168.1.100	192.168.1.1
ADMIN ROOM	192.168.1.101	192.168.1.1
GATE KEEPER	192.168.150.3	192.168.150.1
RECIEPTION ROOM	192.168.150.1	192.168.150.1

Table 1: IP Planning for this Project

4.6 Use Case Diagram and Narratives

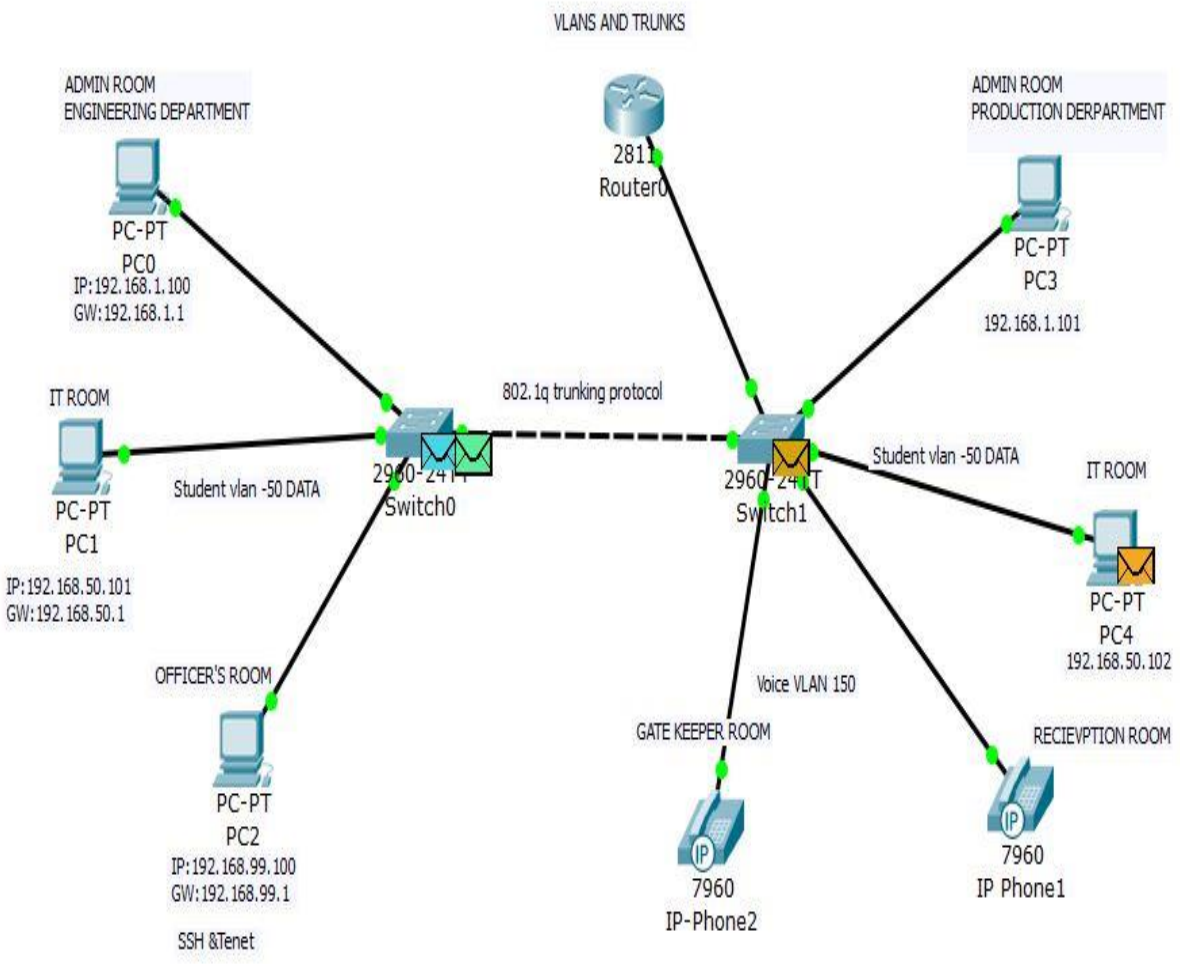

Figure :4.6 Use Case Diagram and Narratives

4.7 Underlying Network Design

The SAFE security best practices, designs, and configurations presented in this document were integrated and validated using the network design for medium enterprises as documented in the Medium Enterprise Design Profile. The Medium Enterprise Design Profile is a network architecture that enables medium enterprises to deliver all the services required for an enhanced business environment. The Medium Enterprise Design Profile includes a routing and switching LAN foundation and integrates services such as WAN connectivity, security, unified communications, and mobility. The Medium Enterprise Design Profile is based on a validated network architecture designed around both business operations and technical considerations. Because cost is a common limiting factor to medium enterprise network designs, the architecture topologies and platforms were carefully selected to increase productivity while reducing overall costs. The Medium Enterprise Design Profile accommodates a main site and one or more remote sites of various sizes, interconnected over a metro Ethernet or managed WAN service. Each of these sites may contain one or more buildings of varying sizes.

4.8 Enterprise Network Security Design

The architecture is designed with built-in security to protect the infrastructure and to provide a secure online environment for businesses. A series of network security technologies and products are strategically deployed throughout the network to protect employees and company assets, to guarantee confidentiality of sensitive data, and to ensure the availability and integrity of systems and data. Safeguards were carefully chosen to mitigate well-known attacks as well as emerging threats. Understanding the diverse nature of threats and how they may evolve over time is the first step towards a successful enterprise security strategy.

The following are some of the common threats to enterprise environments:

Service disruption—Disruption to the infrastructure, applications, and other business resources caused by botnets, worms, malware, adware, spyware, viruses, denial-of-service (DoS) attacks, and Layer 2 attacks

Network abuse—Use of non-approved applications by employees, peer-to-peer file sharing and instant messaging abuse, and access to non-business-related content

Unauthorized access—Intrusions, unauthorized users, escalation of privileges, IP spoofing, and unauthorized access to restricted resources

Data loss—Loss or leakage of private data from servers and endpoints while in transit or as a result of spyware, malware, key-loggers, viruses, and so on

Identity theft and fraud—Theft of personal identity or fraud on servers and end users through phishing and E-mail spam

4.9 Network Foundation Protection

Medium enterprise networks are built with routers, switches, and other infrastructure network devices that keep the applications and services running. These infrastructure devices must be properly hardened and secured to maintain continued operation and access to these services.

To ensure the availability of the medium enterprise network infrastructure, the security design leverages the Network Foundation Protection best practices for the following areas Secure management servers and endpoints with endpoint protection software and operating system (OS) hardening best practices.

4.10 VLAN Communication

Currently, in every department of this company 253 employees can work highest. OSPF has been used to work in this big network. OSPF can configure in any router easily and in this kind of big network, OSPF is a proven system to work fast. After all, company configure separate VLAN for every department so that the important files and information for a selected department can't deliver to another department. After establishing this VLAN, the network security has been increased minimum x3 times better.

In every department, Inter-VLAN routing configure has been completed so that one employee can communicate with another from own department/another department or district in emergency purpose. We can communicate with higher security from one branch to another one which is far from the communicator branch. Moreover, as the number of the domain is decreased, no data loss of any communication or any kind of error don't happen.

We hope that by using this Inter-VLAN routing system, the company can spread its branch and sub branches all over the Bangladesh.

CHAPTER 5

Project Description

5.1 Project Description

Virtual LANs (VLANs) divide one physical network into multiple broadcast domains. But, VLAN-enabled switches cannot, by themselves, forward traffic across VLAN boundaries. So you need to have routing between these VLANs which is called inter-VLAN routing consider, this, as the network administrator, one of your tasks is to create and assign different users to VLANs in your network, you have three main departments which should be logically segmented using

5.2 Screenshot of this project

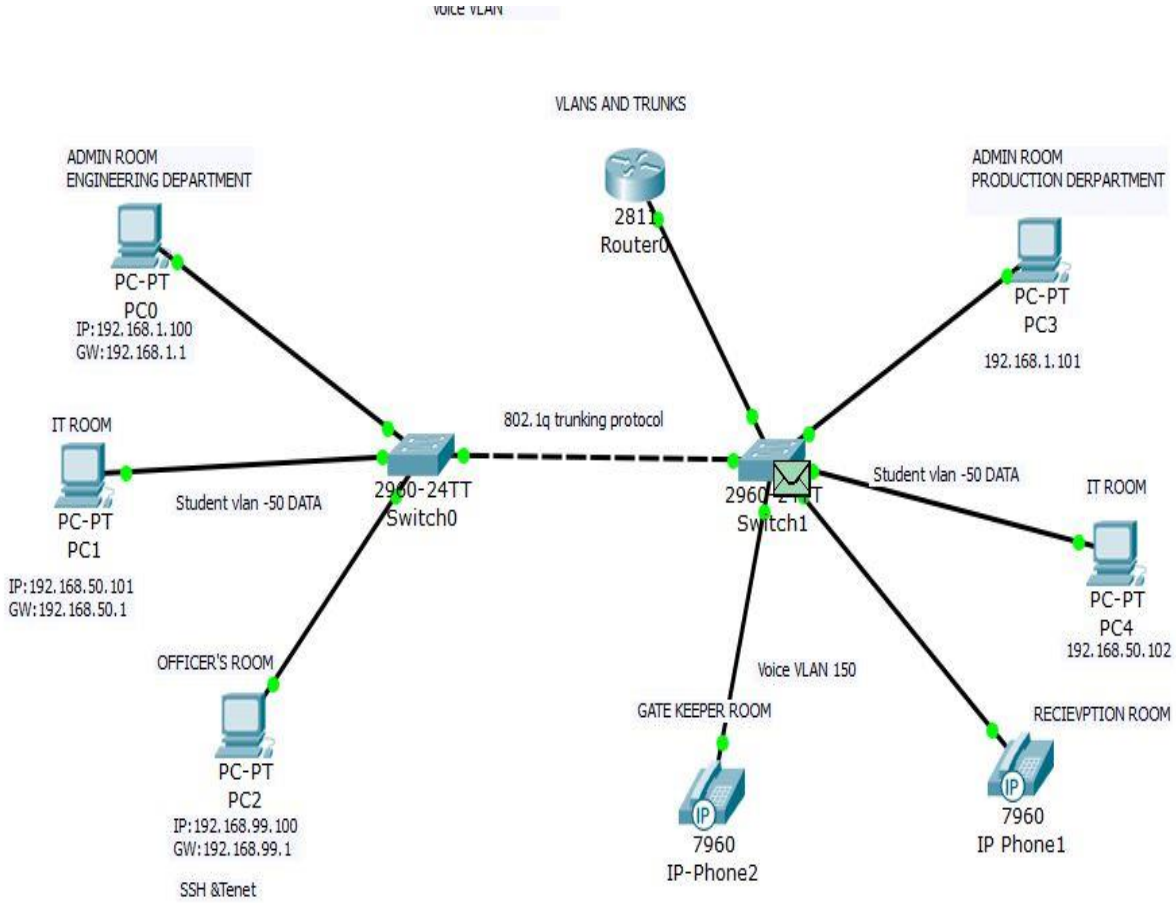

Figure 5:2 Project Data Flow

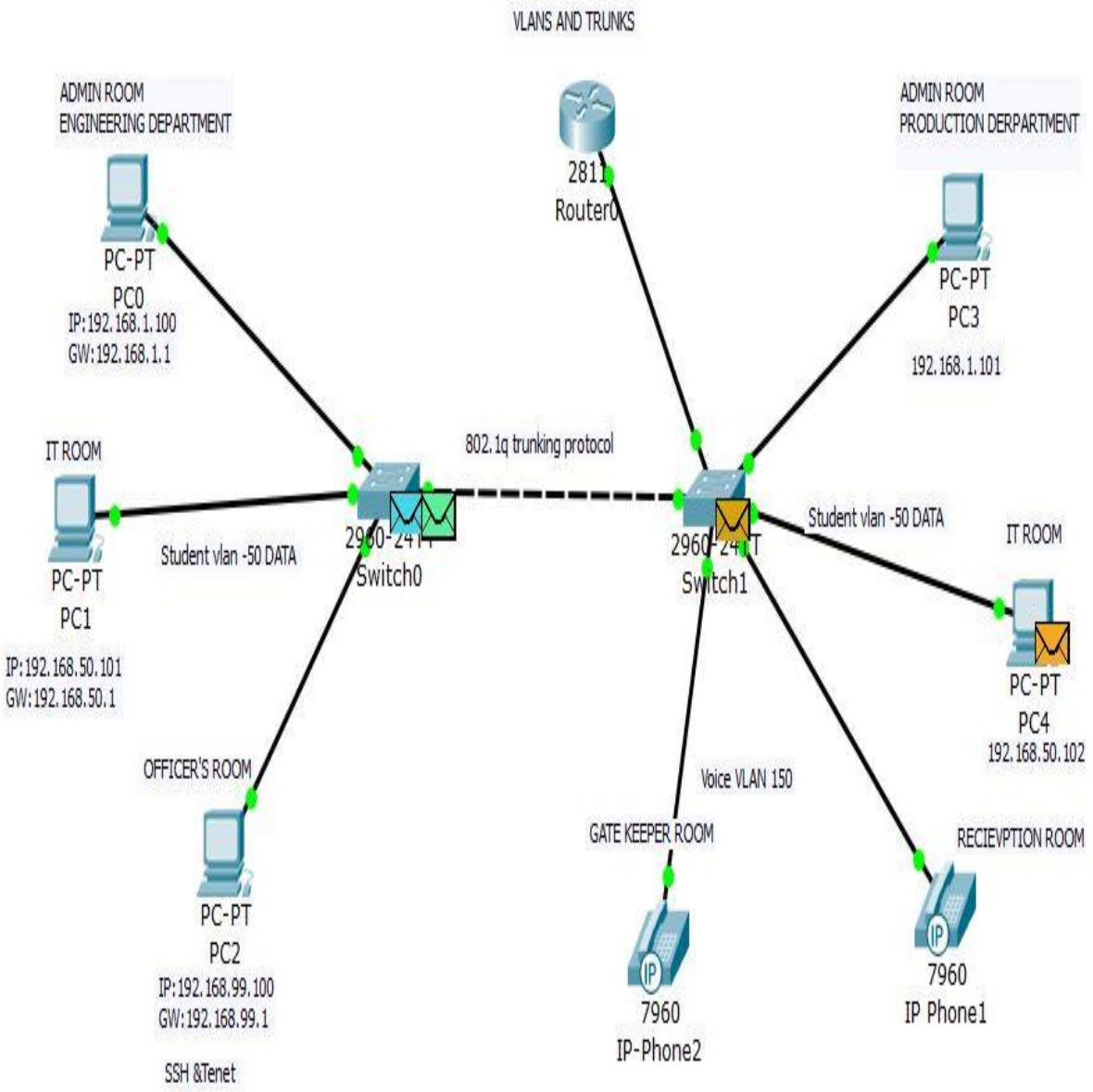

Figure 5:2.1 How to project Data Flow

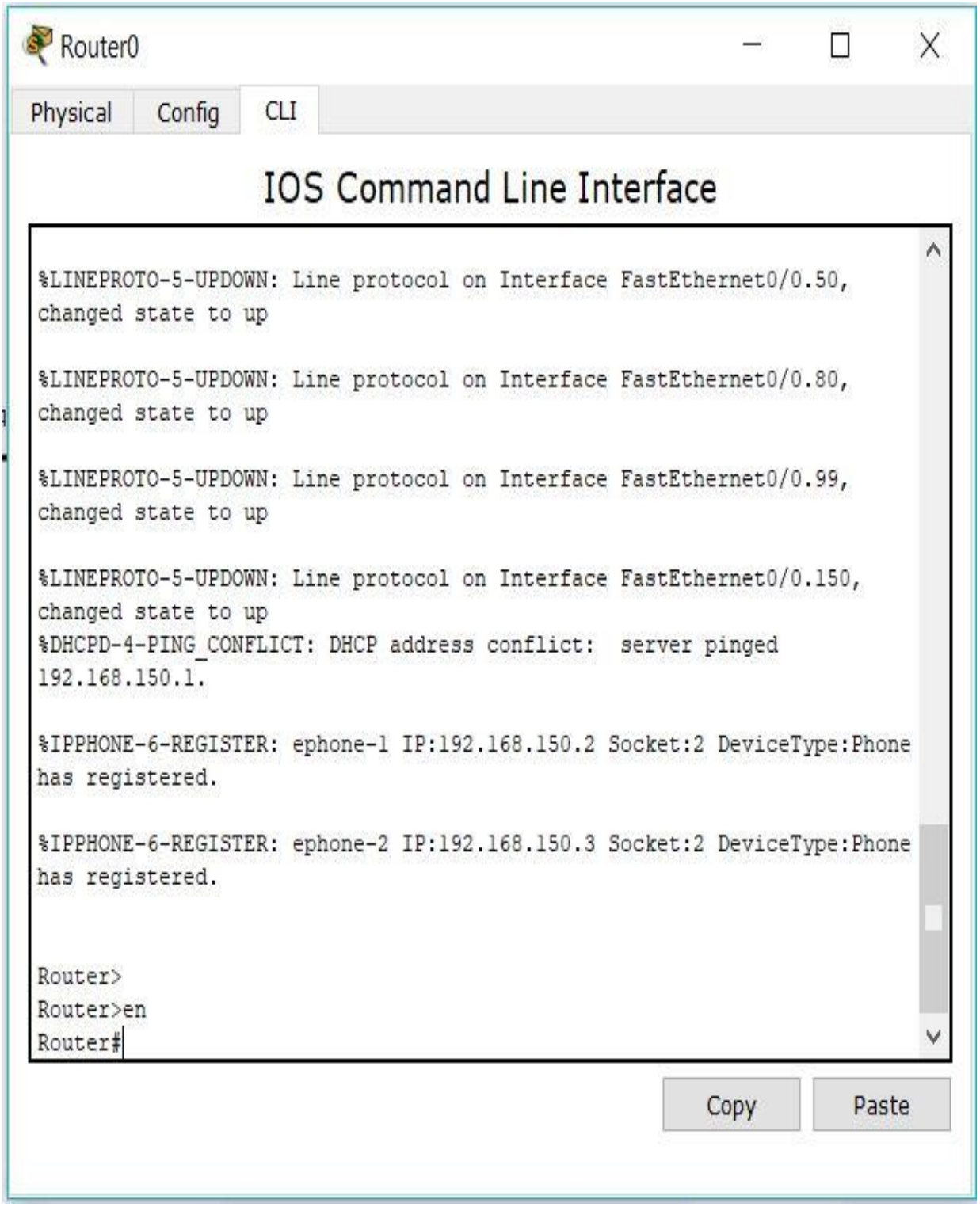

Figure 5:2.2 How to Router Configuration

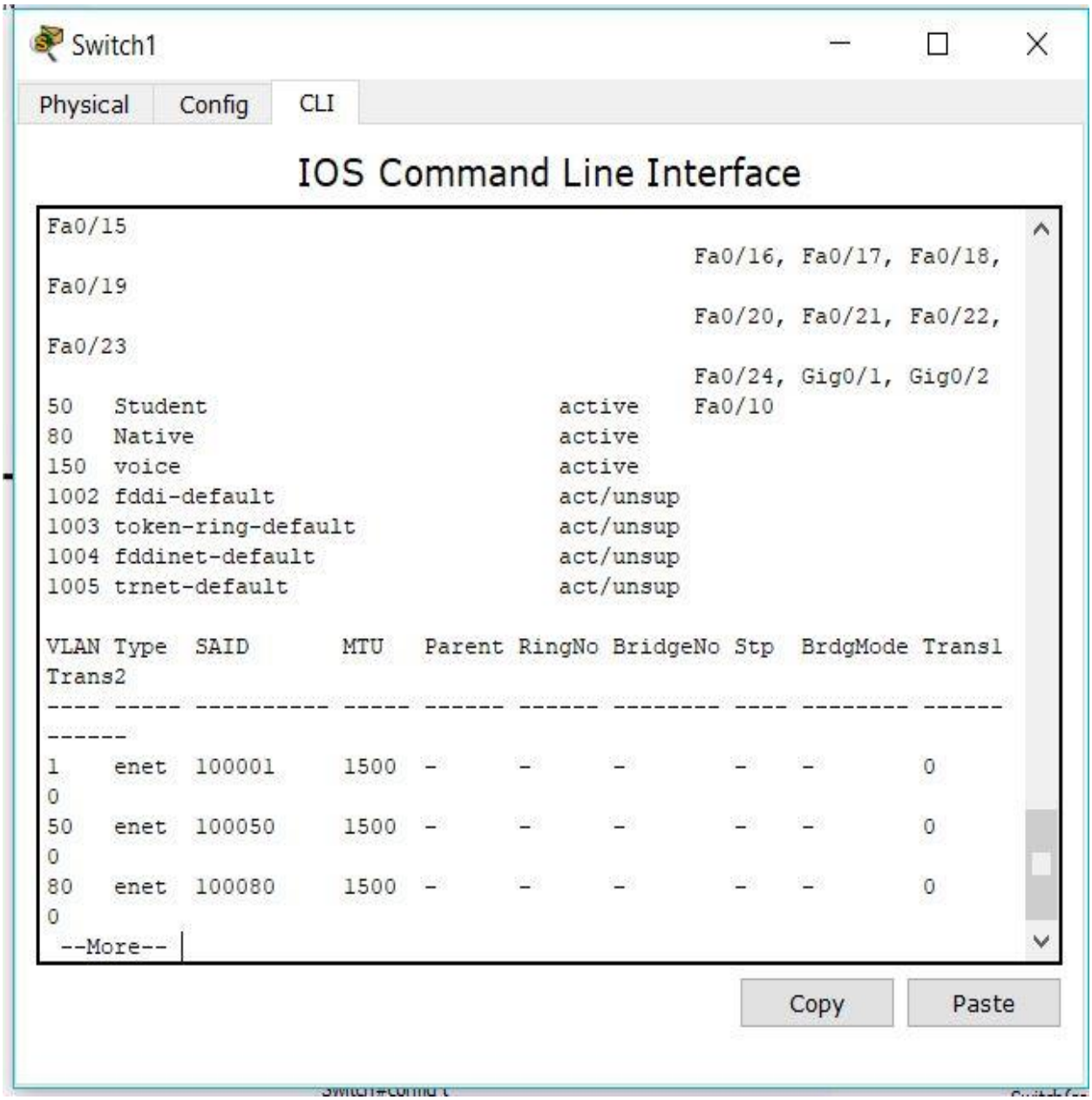

Figure 5:2.3 How to Switch Configuration

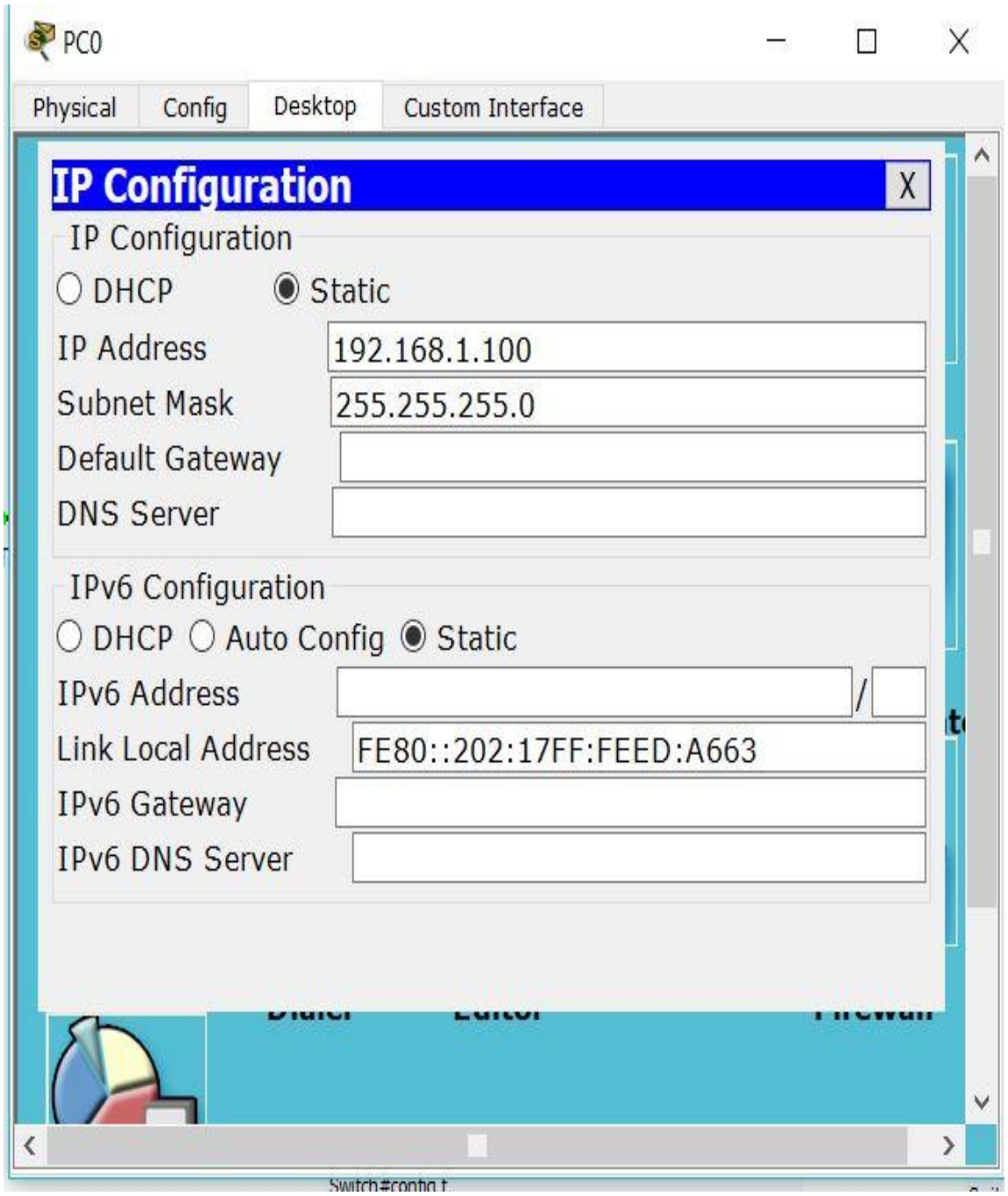

Figure 5:2.4 How to End Device Configuration

Figure 5:2.5 How to IP Phone Device Configuration

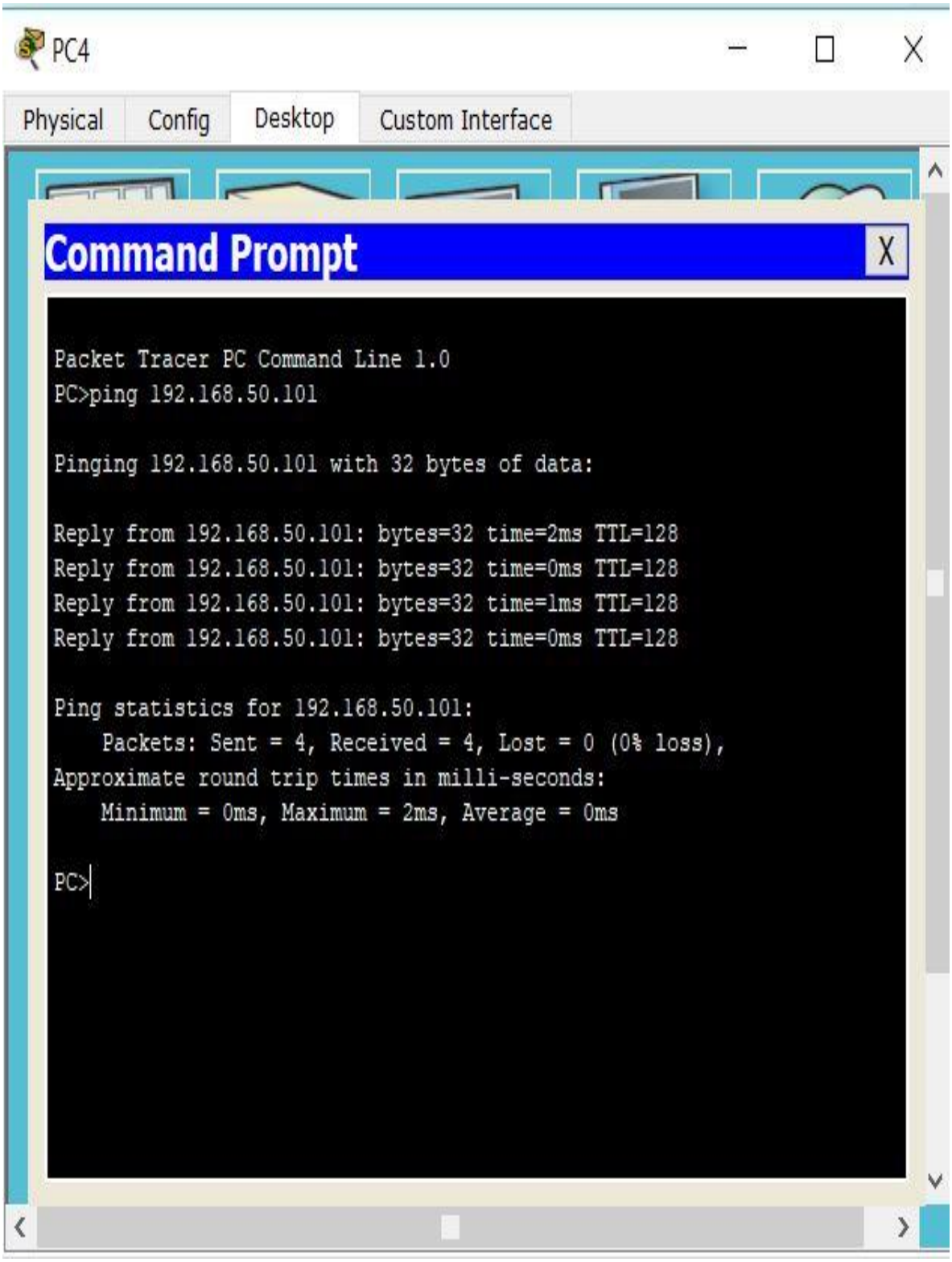

Figure 5:2.6 How to IP Address Ping

CHAPTER 6

Result & Output

6.1 Simulation Results

Packet Tracer PC Command Line 1.0

PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=17ms TTL=128

Reply from 192.168.1.100: bytes=32 time=0ms TTL=128

Reply from 192.168.1.100: bytes=32 time=0ms TTL=128

Reply from 192.168.1.100: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round-trip times in milli-seconds:

Minimum = 0ms, Maximum = 17ms, Average = 4ms

PC>ping 192.168.50.101

Pinging 192.168.50.101 with 32 bytes of data:

Reply from 192.168.50.101: bytes=32 time=0ms TTL=128

Reply from 192.168.50.101: bytes=32 time=0ms TTL=128

Reply from 192.168.50.101: bytes=32 time=0ms TTL=128

Reply from 192.168.50.101: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.50.101:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round-trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0msPackets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round-trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Every Inter-VLAN routing communication is zero percent loss or error. Main and sub branches communicate with each other by using Inter-VLAN Routing without any data frame loss. Every VLAN employees communicate with other VLAN employees with better security.

CHAPTER 7

CONCLUSION

7.1: Conclusion

In this paper I tried to find a suitable inter-vlan with OSPF routing protocol for my office or company network topology which is useful for real time communication. In real time communication there are few very important parameters that make it hard for normal packet based network to give as acceptable QOS. These parameters are End to End delay,link failure condition and throughput.

The OSPF protocol provides a high functionality open protocol that allows multiple vendor networks to communicate using the TCP/IP protocol family. Some of the benefits of OSPF are, fast convergence, VLSM, authentication, hierarchical segmentation, route summarization, and aggregation which are needed to handle large and complicated networks.

The basic reason for splitting a network into VLANs is to reduce congestion on a large LAN. To understand this problem, we need to look briefly at how LANs have developed over the years.

Initially LANs were very flat—all the workstations were connected to a single piece of coaxial cable, or to sets of chained hubs. In a flat LAN, every packet that any device puts onto the wire gets sent to every other device on the LAN.

As the number of workstations on the typical LAN grew, they started to become hopelessly congested; there were just too many collisions, because most of the time when a workstation tried to send a packet, it would find that the wire was already occupied by a packet sent by some other device.

7.2 Future Work Scope

As for future work, more realistic network topologies and routing polices can be employed to simulate genuine behavior of the internet. Additional features, such as route flap damping

, policy routing, and multiprotocol extension and evaluate new technologies that are based on the multiprotocol extension, such as OSPF, VPN, Gateway to gateway inter-vlan routing.

The only varying parameter in our analysis, other than routing protocol of course, was the size of the network topology. Improvement or future works for this project can include adding metrics on interfaces such as cost, bandwidth, distance, Bit Error Rate (BER), and delay. Furthermore, various network topologies (in terms of size, routers and links used) can

be implemented for comparison of performance between these routing protocols. Since OSPF is the most complex routing protocol, more time could be spent on analyzing it to find the value of parameters that need to be set in order for it to perform optimally. Another possibility is to implement real network topologies used, perhaps in a university campus a company office, or a larger network size while also modifying the network parameters, such as interfaces, to those of the actual scenario being analyzed.

7.3Adventages and Disadvantages

Advantages

1) Broadcast Control: Broadcasts are required for the normal function of a network. Many protocols and applications depend on broadcast communication to function properly. A layer 2 switched network is in a single broadcast domain and the broadcasts can reach the network segments which are so far where a particular broadcast has no scope and consume available network bandwidth. A layer 3 device (typically a Router) is used to segment a broadcast domain.
2) If we segment a large LAN to smaller VLANs we can reduce broadcast traffic as each broadcast will be sent on to the relevant VLAN only.
3) Security: VLANs provide enhanced network security. In a VLAN network environment, with multiple broadcast domains, network administrators have control over each port and user. A malicious user can no longer just plug their workstation into any switch port and sniff the network traffic using a packet sniffer. The network administrator controls each port and whatever resources it is allowed to use. VLANs help to restrict sensitive traffic originating from an enterprise department within itself.
4) Cost: Segmenting a large VLAN to smaller VLANs is cheaper than creating a routed network with routers because normally routers costlier than switches.
5) Physical Layer Transparency: VLANs are transparent on the physical topology and medium over which the network is connected.

Disadvantages

I. A VLAN is useful if you need to isolate traffic between subsets mad subsections of a subnet. Let's say you have two groups of workers and they must not use each other's shared printer or see other shared resources. You can do this with a VLAN.
II. You need a managed switch to make this work, but such switches have come down in price a lot in the last few years.
III. Well, if you do not need to isolate portions of your network, you do not turn this on. If you need it, you may also need additional routers and/or bridges to connect everything. So there are no real disadvantages.

REFERENCE

1. IP Addressing Guide by A. D. Smith; USA: CISCO Systems, 2010.
2. IP Addressing Guide by Alfed D. Smith; 2010 Cisco Systems, Inc.
3. Technology Energetic Information by Marc Tieso; Anno accademico-2009/2010
4. TCP/IP Cheat sheet v2.1 by Boson; 1999-2000
5. https://www.computerhope.com/, [Available] at 3rd October, 2017
6. http://www.webopedia.com/term/n/network.html, [Available] at 7th October, 2015
7. http://www.networkcomputing.com/718/718w1.html, [Available] at 9th October, 2015
8. http://www.networkcomputing.com/713/713workrip.html, [Available] at 23th October, 2015
9. http://www.tcpipguide.com/free/t_IPClassfulConventionalAddressing.htm, [Available] at 24th October, 2015
10. http://www.tcpipguide.com/free/t_Backgrounder DataRepresentationandtheMathematicsofC.htm, [Available] at 29th October, 2015
11. http://www.tcpipguide.com/free/t_IPSupernettingClasslessInterDomainRoutingCIDRHiera.htm, [Available] at 2nd November, 2015
12. http://www.ianswer4u.com/, [Available] at 9th November, 2015
13. http://www.computerhope.com, [Available] at 11th November, 2015
14. http://www.tutorialspoint.com, [Available] at 12th November, 2015
15. www.cisco.com/go/ipv6, [Available] at 16th November, 2015
16. http://www.google.com, [Available] at 25th November, 2015
17. http://wirelessinfo.be/category/MikroTik/] at 1st November, 2017

APPENDIX

```
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed 1-99
^
% Invalid input detected at '^' marker.
Switch(config-if)#switchport trunk allowed vlan 1-99
Switch(config-if)#end
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#enable secret cisco
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name Student
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name Management
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config-if)#end
Switch(config)#int fa0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
Switch(config-if)#ip address 192.168.99.2 255.255.255.0
Switch(config-if)#no shutdown
 Router(config)#ephone-dn
% Incomplete command.
```

Router(config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.2.
Router(config)#ephone-d%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.
n
% Incomplete command.
Router(config)#ephone-dn
% Incomplete command.
Router(config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.2.
Router(config)#ephone-dn 1%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
Router(config-ephone-dn)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.
Router(config)#ephone-dn 1%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.

Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.1.
n%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.150.2.
Configuring Trunk Port
S1#conf t
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#exit
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#exit
S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport mode trunk
S2#conf t
S2(config)#interface fastEthernet 0/1
S2(config-if)#switchport mode trunk
S3#conf t
S3(config)#interface fastEthernet 0/3
S3(config-if)#switchport mode trunk

onfiguring Sub-interfaces on Router's Physical Interface

```
R1#configure terminal
R1(config)#interface fastEthernet 0/1.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/1.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/1
R1(config-if)#no shutdown
S2#conf t
S2(config)#interface fastEthernet 0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface fastEthernet 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
S2(config)#interface fastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30

S3#conf t
S3(config)#interface fastEthernet 0/11
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#exit
S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#exit
S3(config)#interface fastEthernet 0/6
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 30
```

```
Switch>en
```

```
Password:
Password:
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Gig0/1, Gig0/2
50   Student                           active    Fa0/10
80   VLAN0080                          active
99   Management                        active    Fa0/24
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
80   enet  100080     1500  -      -      -        -    -        0      0
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
50   Student                           active    Fa0/10
80   Native                            active
150  voice                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```