

Performance Evaluation of Virtual Local Area Networks (VLANs)

By

Mousa Shafiq Ayyash

تعمد كلية الدراسات العليا
هذه النسخة من الرسالة
التوقيع... التاريخ 27/7/99

Supervisor

Dr. Souheil F. Odeh

Submitted in Partial Fulfillment of the Requirements for the

Degree of Master of Science in

Electrical Engineering/Communications

Faculty of Graduate Studies
University of Jordan

May 1999

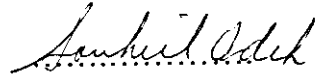
27/7/99

This thesis was successfully defended and approved on 26/5/1999

Examination Committee

Signature


Dr. Souheil Odeh



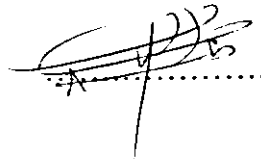
Dr. Andrawos Sweidan



Dr. Bassam Kahhaleh



Dr. Abdel-Rahman Odeh



Dedication

To my lovely parents.

To my brothers and sisters.

To everyone who looks desirably for my success.

Acknowledgement

I am really grateful to many people whose efforts have gone into the completion of this thesis.

A great gratitude and respect to my lovely parents for their continuous support, encouragement, and efforts which make me unable to express my deep gratitude. Also, my thanks to my supervisor *Dr. Souheil Odeh* for his support and advice. Moreover, I would like to thank the examination committee for their efforts in evaluating this work.

Finally, I want to express my appreciation to my close friends *Adel Faisal, Bashar Sadder, Dawood Daliah, and Yazeed Al-Sbou'*. Also, my special gratitude to my roommate *Ibrahim H. Juma'h* who didn't occlude any possible help.

Table of Contents

	Examination Committee	ii
	Dedication	iii
	Acknowledgement	iv
	Table of Contents	v
	List of Tables	viii
	List of Figures	ix
	Abstract (English)	xi
Chapter 1	Introduction	1
Chapter 2	Background	5
	2.1 Preview	5
	2.2 Local Area Networks Overview	5
	2.2.1 Generalization	5
	2.2.2 LANs Characteristics	7
	2.2.3 Demands on LANs	10
	2.2.4 Future LANs	11
	2.3 Virtual Local Area Networks	13
	2.3.1 Overview	13
	2.3.2 VLAN Definition	13
	2.3.3 VLAN Benefits and Features	15
	2.3.4 VLAN Components	22
	2.3.5 VLAN Membership Methods	24
	2.3.5.1 Preview	24

2.3.5.2	Clarifying VLAN Membership Methods	24
2.3.6	VLAN Membership Information Communication	33
2.3.6.1	Overview	33
2.3.6.2	Interswitch VLAN Communication	33
2.3.6.3	Frame Processing	35
2.3.7	Inter-VLAN Communication	41
2.3.8	VLAN and ATM	43
2.3.9	VLAN Standardization	43
Chapter 3	Simulation Models	46
3.1	Preview	46
3.2	Overview about COMNET III	46
3.3	Simulation Models	47
3.3.1	The Main Network	48
3.3.2	Employing the Main Network	49
3.3.3	Performance Measures	50
3.3.4	Defining VLANs	51
3.3.5	Case Studies	51
3.3.6	Implementing VLANs in a Switched Network	53
3.3.7	Mixed Network Model	55
Chapter 4	Simulation Results and Discussion	57
4.1	Preview	57
4.2	Simulation Results	57
4.2.1	Results of Simulating the Main Network	57

4.2.2 Results of Simulating the Switched Network	65
4.2.3 Results of Simulating the Mixed Network	67
Chapter 5 Conclusions and Recommendations	69
5.1 Conclusions	69
5.2 Recommendations for Future Work	71
References	73
Appendix	75
Abstract (Arabic)	78

List of Tables

Table (2.1)	Comparison of High-Performance LAN Technologies.	12
Table (2.2)	Port-based VLANs.	25
Table (2.3)	Assignment of MAC Address to Various VLANs.	27
Table (2.4)	Assignment of Protocol to Various VLANs.	28
Table (2.5)	VLAN Assignment Method Comparison.	32
Table (3.1)	Some Details of the University Network.	49
Table (3.2)	Defining Two VLANs in the University Network.	53

491719

List of Figures

Figure (2.1) VLANs in Comparison with the Traditional LANs.	15
Figure (2.2) Logical Workgrouping with VLANs.	19
Figure (2.3) Creating Port-based VLANs using a LAN Switch.	25
Figure (2.4) A Layer-2 VLAN.	26
Figure (2.5) Example of a VLAN Creation Based on IP Subnets.	29
Figure (2.6) Tag Header Structure.	38
Figure (2.7) Tag Control Information (TCI) Format.	39
Figure (2.8) Ethernet-encoded Tag Header.	40
Figure (2.9) SNAP-encoded Tag Header.	40
Figure (2.10) VLAN Architectural Model.	44
Figure (3.1) A University Campus Computer Network.	48
Figure (3.2) A University Campus Switched Computer Network.	54
Figure (3.3) A University Campus Mixed Computer Network.	56
Figure (4.1) Effect of Message Size on the CC Link Utilization in the Main Network.	58
Figure (4.2) Effect of the Message Size on the End-to-End Delay in the Main Network.	59
Figure (4.3) Effect of the Message Size on the Transmission Delay via the CC link in the Main Network.	59
Figure (4.4) Effect of the Number of Users on the CC Link Utilization in the Main Network.	60
Figure (4.5) Effect of the Number of Users on the	61

End-to-End Delay in the Main Network.	
Figure (4.6) Effect of the Number of Users on the Transmission Delay via the CC Link in the Main Network.	61
Figure (4.7) The CC Link Utilization in the Main Network in Case of Downloading.	62
Figure (4.8) Effect on the End-to-End Delay in the Main Network in Case of Downloading.	62
Figure (4.9) Effect on the End-to-End Delay in the Main Network in Case of Downloading.	63
Figure (4.10) Message Delay between Two VLANs.	64
Figure (4.11) The CC Link Utilization in Case of Defining Two VLANs.	65
Figure (4.12) Effect on the End-to-End Delay in the Switched Network.	66
Figure (4.13) Effect on the Test Link Utilization in the Switched Network.	66
Figure (4.14) Effect on Downloading Delay in the Switched Network.	67
Figure (4.15) Effect on the End-to-End Delay in the Mixed Network.	68
Figure (4.16) Effect on the CC Link Utilization in the Mixed Network.	68

Abstract**Performance Evaluation of
Virtual Local Area Networks (VLANs)**

By

Mousa Shafiq Ayyash

Supervisor

Dr. Souheil F. Odeh

The great evolution of computer networks field is directly related to the vast development in the networking technologies. This is due to the fact that these technologies try to present solutions that ameliorate the performance of recent and future networks. However, these networks are expected to deal with various applications which look continuously for more speed and more bandwidth. Also, we can't ignore the need for flexible working environment.

This thesis presents a new networking technology which represents a solution for some of the anticipated demands on networks. This technology is the VLAN technology.

The aim of this thesis is to evaluate the performance of VLANs. This is achieved by proposing several simulation models which are studied in terms of

two performance measures. These two performance measures are the end-to-end message delay and the link utilization. The VLAN models are compared with legacy LAN models in order to get clearer idea about the performance. Several figures are drawn to depict the behavior of the chosen performance measures in case of changing some parameters such as the message size and the number of users. Moreover, the performance of VLANs is studied in case of downloading, loading one of the LAN segments with a transient load, and defining more than one VLAN in a given network.

It is found that the VLANs performance is better in most cases for the two performance measures chosen. Moreover, it is possible to deduce that VLAN technology presents a distinguished solution for the problem of delay which is real deterrent against today's multimedia applications.

Finally, we can present that VLAN technology is a promising track in computer networks field, especially if we consider the anticipated progress in the switching technologies.

Chapter 1

Introduction

The nature of the world through its evolution stages shows that it passes through different ages and periods. However, the world nowadays enters the information era. This is due to the vital role of information which starts to be a kind of trade with the real meaning of the word (Smith, 1998). Moreover, information has become a part of all life aspects since it satisfies the recent and future needs of our life's environment. Hence, the future will clarify a huge progress and deployment in the field of computer networks and data communication technologies. This would happen to fulfill the evolution in information resources and systems. The anticipated progress could be sensed through the notable deployment in the technologies of networking.

If we consider the nature of today's working environment, we can notice the great demand of the bandwidth that is combined with the recent and future applications such as multimedia ones. Also, the technologies compel to satisfy the speed challenges in order to minimize the response times when using the *Information Technologies (ITs)* infrastructure. Therefore, we find that we are in need to consider the high-speed technologies in networking. There are some new disciplines that try to solve the problem of speed necessity such as the *Asynchronous Transfer Mode (ATM)*, *Fast-Ethernet*, and *Fiber Distributed Data Interface (FDDI)*. However, if we would like to contemplate the nowadays status, we find that the trend is towards switching. We can say that the networking field goes more and more to depend substantially on the

switched networks especially in the *Local Area Networks (LANs)* area, whether Ethernet or ATM switching (Smith, 1998).

Now, one can inquire about the reasons of considering switching discipline to that extent. It is possible to answer this inquiry by clarifying both the case prior to switching and the basic idea behind the switching principle. Most of the legacy LANs such as Ethernet or Token passing are dependent on a shared medium, e.g., a cable, which connects all the data terminals, nodes, such as *Personal Computers (PCs)*, servers, or workstations. Therefore, the whole available bandwidth is dedicated for the user who is in service. This will lead to inefficient usage of these LANs in case of highly congested environment in which a lot of users request to access the LAN. The inefficiency is due to the waiting periods that are spent before serving the users. Also, we see the dedication of the LAN for one user at a time, which is not suitable for today's needs. The problem of delay is debated strongly when we use routers to interconnect LANs. This is because of the inherent functions of the router such as determining the best route, which needs some calculations, followed by the incoming packets through the network. Of course, we can't claim that routers will be avoided totally in networking. However, it is expected to consider switching in the intranetworking area, i.e., networking devices within workgroups, departments, or buildings. On the other hand, routing would be the solution in case of internetworking (Ranjan, 1996).

As mentioned before, any proposed network must try to fulfill the needs for bandwidth and speed. But also the intended network must emulate the

dynamic nature of today's working environment, which requires flexible and easily manageable network. The flexibility is important to cope with the possible changes in the network, such as the movements of a network member from one location to another but he/she still needs to work in the same working group. Hence, it is necessary to build new LANs that help in defining workgroups, broadcast domains, regardless of the physical restrictions available in the legacy LANs (Ethernet, Token passing, FDDI).

Any legacy LAN is defined depending on connecting the information terminals that are in the same working place to a shared physical medium. But the new LAN is defined as the network that consists of the members, terminals, in the same broadcast domain without any restriction for being in the same working area (Varadarjan, 1997).

This new definition of LANs combined with the recent and prospective dependency on switching rather than on routing will help in satisfying the basic needs for speed, bandwidth, flexibility and other demands that will be discussed in the next chapter such as security and simplicity in management and administration. Currently, a new promising solution is suggested and expected to lead the future of networking to some extent. This solution is called *Virtual Local Area Networks (VLANs)*. A VLAN is a logical grouping of PCs, servers, and other network resources. This logical grouping opposes the physical grouping which requires the users to be in the same geographical area (Seifert, 1998). Members of the VLAN communicate as if they are on the same wire or LAN.

The VLAN topic is still under research and study because it is a new track in computer networks. Therefore, most of the issues related to VLANs are still in the phase of recommendations preparation to be accredited through the *Institute of Electrical and Electronics Engineers (IEEE)* committees. There are few installations of VLANs due to the lack of standards, but there is no published work on performance evaluation of VLANs. Thus, the main objective of this thesis is to complete that lack of performance evaluation which is essential in any decision making process.

In the way of achieving the purpose of this research, this thesis is divided into five chapters. This chapter is an introductory chapter which presents a general idea about the stages prior to the VLAN discipline and a brief overview on VLANs. Also, the statement of the problem is stated. Chapter two represents an essential background about LANs and VLANs. The simulation models, performance measures, and relevant ideas about the used simulation package, *COMNET III*, are available in chapter three. The simulation results are found in chapter four. Also in this chapter the discussion of the results is presented. Chapter five presents the conclusions of this work and recommendations for future research work.

Chapter 2

Background

2.1 Preview

The discussion of *Virtual Local Area Networks (VLANs)* topic imposes a need for debating the *Local Area Networks (LANs)* basics. This is due to the clear relationship between VLANs and LANs. Therefore, a brief introduction of LANs will be stated before presenting the main purpose of this chapter. Thereafter, this chapter will present a vital background about VLANs. *VLAN meaning, VLAN benefits and features, VLAN components, VLAN membership methods, VLAN membership information communication, interswitch VLAN communication, inter-VLAN communication, VLAN and ATM, and VLAN standardization* are important topics to demystify the main points about the VLAN subject.

2.2 Local Area Networks Overview

2.2.1 Generalization

Ever since the early stages of life on earth, the communication among people have been considered as an essential need in which the human can cooperate in building the civilization architectures. Therefore, several methods are continually devised in order to investigate the required communication between life's activities. Currently, we hear about the term *network* as a method by which the information can be conveyed between different sources. Data, voice, and video are the basic forms of information that any suggested networking solution should handle in order to contemplate present and future

communication demands. Hence, the term *network* is used to represent *any set of communication links which are required to interconnect the information terminals such as computers, telephones, printers, digital cameras, or any other type of data-communicating and data-handling devices (stations)* (Keiser, 1989).

Generally, networks are used for different reasons such as communication, resource sharing, security, management control, and cost effectiveness (Stamper, 1998).

Normally, data networks are classified into three major categories: *Local Area Networks (LANs)*, *Metropolitan Area Networks (MANs)*, and *Wide Area Networks (WANs)*. This classification is made depending on the geographical area in which each network is accomplished and the speed used for conveying data.

A LAN, as its name implies, covers a limited geographical area, less than 10km but more than 1m, at high speed usually 10Mbps or higher. It is also owned by a certain organization such as LANs in universities, factories, or even office buildings. A MAN serves wider distances of approximately 200km. Also, a MAN is a high-speed network, typically 100Mbps or higher. FDDI is the common implemented MAN. A WAN generally spans a wide geographical area such as a state, country, or multiple countries. The speed of transmission in WANs is lower than that in LANs or MANs. Also, the transmission protocols are different (Stamper, 1998). WANs exploit *the public data*

networks (PDNs), such as the public switched telephone networks (PSTNs), in order to interconnect different dispersed LANs (Halsall, 1996).

2.2.2 LANs Characteristics

LANs are generally characterized depending on various aspects and they have characteristics such as transparent use, mixed hardware and software, limited geographical area, high speed, *LAN transmission media, media access control (MAC), and network topology* (Stamper, 1998). These characteristics will be clarified briefly through the following lines.

- **Transparent Use**

Due to the transparency, members of a LAN don't find substantial differences between using a stand-alone microcomputer and using one connected to a LAN. For example, printing using a network printer is done in the same manner as printing using a local printer.

- **Mixed Hardware and Software**

If we consider the LANs operation today, we find that they are mostly microcomputer-based LANs. But this doesn't prohibit using large computing systems to be on the same LAN with the microcomputers of various types. Usually, large computers function as *servers*. As a result, it is logical to find a variety of operating systems and applications are being put to use. As a consequence of mixed hardware and software, the LAN administration and management become complex, and sometimes costly.

- **Limited Geographical Area**

As mentioned before, a LAN is prepared to serve limited geographical

is called *topology*. Therefore, the term *topology* refers to the way that LAN members are connected to a shared medium.

Bus, ring, and star layouts are the common topologies that are used in today's LANs. Each methodology has its advantages and restrictions in terms of *reliability, expandability, and performance characteristics* (Keiser, 1989).

- **LAN Media Access Control Protocols**

Any network has its specific ways by which users gain access to the communication medium, transmit data over the media, and route messages (Stamper, 1998). In the bus topology, for instance, the LAN members connection to the same shared medium imposes a need for certain protocols which are necessary to benefit from the network properly. There are two famous techniques that are utilized to access the common LAN transmission medium, bus and ring topologies. The two access methods are *Carrier-Sense Multiple-Access with Collision Detection (CSMA/CD)* and *Token Passing*.

The CSMA/CD technique is used with bus networks, while the token passing technique is usually used for ring networks and rarely for bus networks. Details about the operation of these common access methods, data frame formats, advantages and disadvantages, and other related topics can be found in different texts (Halsall, 1996; Keiser, 1989).

- **Internetworking and Interworking**

Generally, any LAN needs to interconnect to other LANs as a way to integrate services and dispersed resources such as printers and file servers. However, the stand-alone nature of the networks became a major problem.

Concurrently, new network devices were created to satisfy the interconnection between LANs in order to provide *interoperability*. The *interoperability* term involves both *internetworking* and *interworking*. Usually, the term '*internetworking*' refers to the physical connectivity and the term '*interworking*' is applied to the protocols, management, and applications controlling data transfer between DTEs on different LANs.

The network devices, relays, are classified depending on the layer of the *Open Systems Interconnection (OSI) reference model* by which we need to perform the communication. Therefore, several network devices were devised such as *repeaters, hubs, bridges, routers, brouters, and switches*. Each of these devices has different capabilities and functionalities, and therefore, it is necessary to choose the one best suited to task under scrutiny (Smythe, 1995b).

To debate the details of these network devices is out of the scope of this thesis. Hence, for detailed idea the reader is suggested to consider references (Halsall, 1996; Held, 1997; Smythe, 1995b; Stamper, 1998).

2.2.3 Demands on LANs

Recent and future applications such as video, audio, or high-resolution graphics are representative examples of the drastic increase in data traffic. Also, the *client/server applications* grow considerably as the method by which information is exchanged across networks. Moreover, the total number of users per network augments notably. Hence, data networks are in inevitable need to emulate these changes in users number and applications type. Consequently, new demands on LANs request are being fulfilled. These demands are on large

available bandwidth requirement, throughput enhancement, and delay times decrease. However, the new demands impose certain criteria by which new LAN products are chosen in the network's design process. A list of criteria includes the following: *Increasing the LAN capacity, reduction of operating costs, expandability to accommodate future technological developments, efficiency in meeting customer requirements, and reduction of initial purchasing cost of products.* In other words, customers look for technologies and products which satisfy the performance requirements of users quickly and easily, and minimize the management and administrative costs by demanding minimal staff and support resources (Hein and Griffiths, 1997).

2.2.4 Future LANs

After presenting the anticipated demands on LANs, we can't claim that the existing LANs, *legacy LANs* (e.g., Ethernet, Token Passing), will be able to cope with these demands properly. Therefore, customers are ought to upgrade their existing LANs in a way that can emulate the future necessities. To resolve the user's network problems, the network administrator can consider one of three approaches:

a) Division of networks into smaller LAN segments.

As a logical result of reducing the number of users per subnetwork, delay times are dramatically reduced, timeouts situations are minimized, and the number of users accessing the applications on the server, due to the client/server model, is limited.

b) Installation of a faster networking technology (FDDI, or Fast Ethernet).

In other words, VLANs are an outgrowth of switching technology (Salamone, 1995). The rest of this chapter concentrates on the VLANs technologies.

2.3 Virtual Local Area Networks

The intent of this section is to present a basic background about VLANs. This section is subdivided in a way which will help the reader in understanding the relevant topics on VLANs in an informative manner.

2.3.1 Overview

Once again, VLAN technology utilizes from the recent notable development in LAN switching technologies. Also, VLANs emulate the new definition of LANs in which a LAN is defined as a single broadcast domain. The dynamic nature of today's working environment imposes a need for a technology which helps information technology managers in adapting to several possible changes in the work hierarchy easily and effectively without affecting the performance requirements (Varadarajan, 1997).

In addition to the above, it is helpful and reasonable to create workgroups which gather members who are working in the same specialization area. For instance, in a number of companies, it is required to form a product development team that includes a system engineer, a design engineer, a product marketing person, and someone responsible for the financial management of the projects (Salamone, 1995; Intel Corporation, 1998).

2.3.2 VLAN Definition

A VLAN is *"a logical grouping of users, as opposed to the physical grouping imposed by the geography or network topology"*. This logical

segmentation is commonly applied to switched (as opposed to routed) network environment (Seifert, 1998). However, the logical segmentation is achieved depending on functions, working teams, or applications regardless of the physical locations of network members. In the past, network managers had to go into wiring closets and physically connect all users work in the same working field to the same LAN segment in order to create such groupings. This was enough and fine if groups were permanent (Salamone, 1995). In addition, we can say that VLAN is substantially a limited *broadcast domain*. The need for broadcast domains is stringent because of the fact that *flooding networks*, large-size or even medium-size networks, with traffic storms leads dramatically to congested networks and consequently to slow networks.

Broadcast domain term means that all members in a VLAN receive every broadcast traffic packets transmitted by members on the same VLAN but not packets sent by members of other VLANs. Therefore, VLAN discipline represents a promising solution by which the traffic packets are prohibited from being propagated to all network members. This means that the traffic is confined necessarily to those consisting the same VLAN but not to be sent arbitrarily to every connected user to the network. Most importantly, we need to remember the solution in the *legacy LANs* (shared medium LANs). In legacy LANs, the traffic is bounded from being flooded by using *routers*. Routers are introduced to create *Internet Protocol (IP) subnets* in order to stop the broadcast storms. Currently, the usage of routers is neither enough nor satisfactory since routers are much slower than the speed required by today's

LANs, and are unable to allocate individual users dedicated bandwidth. Incidentally, switches continually replace routers. Switches, the anticipated components for the infrastructure of present and future computer networks, can efficiently limit broadcasts by occluding them from propagating across the entire network if the switches are aware of VLANs, *VLAN-aware switches* (Smith, 1998).

VLAN segmentation method, in comparison with the traditional LANs, is clarified in Figure (2.1).

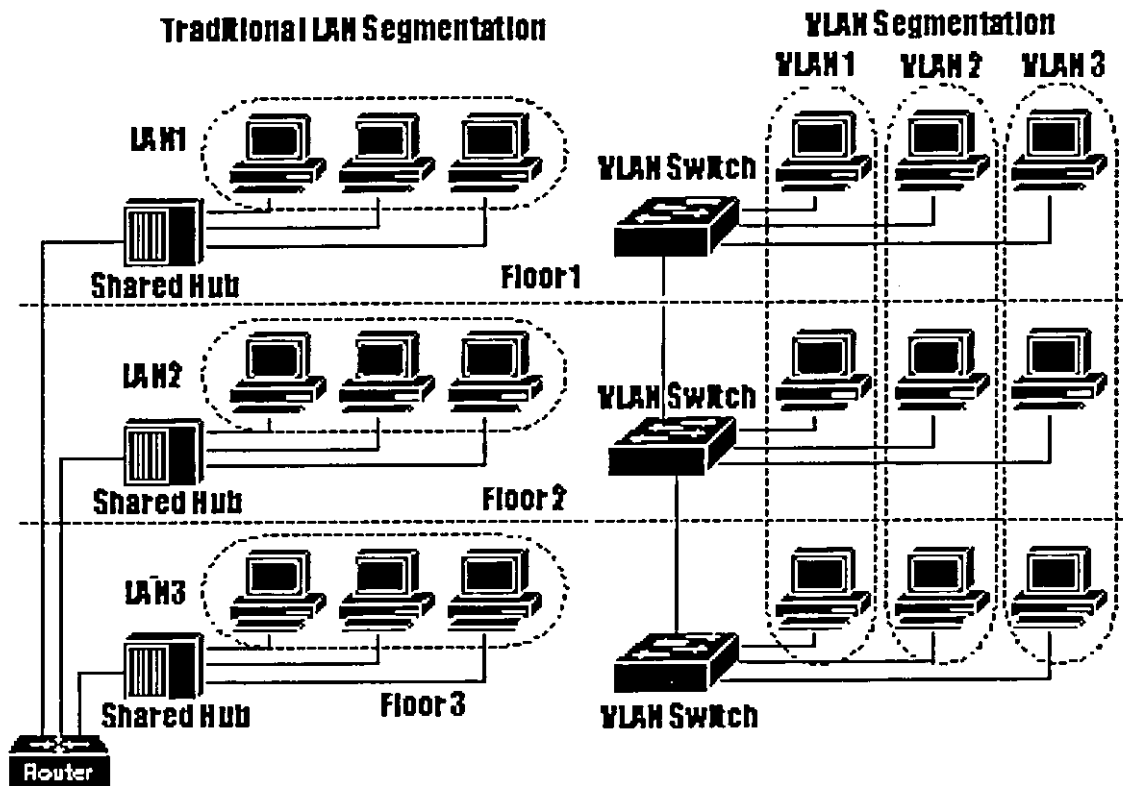


Figure (2.1) VLANs in Comparison with the Traditional LANs.

2.3.3 VLAN Benefits and Features

The VLAN technology refers basically to the ability to create *virtual workgroups*. With virtual workgrouping, members of the same department appear as if they are on the same physical LAN, and most of the network

traffic, therefore, stays in the same broadcast domain. All of this is accomplished regardless of the location of the network member across the enterprise. A network member in a VLAN can move physically for any reason but there is a need to keep working in the same department. This movement should not affect the VLAN membership and there is no need to go into an elaborated workstation reconfiguration. In addition to this interesting primary feature of VLANs, there are other benefits. The benefits will be debated through the following points:

2.3.3.1 Containment of Broadcast Traffic

There is a basic networking principle that is continually emulated nowadays. This principle states that "*Switch when you can, Route when you must*". Although normal switching ameliorates substantially the network performance if compared with routing, simple switches don't filter LAN broadcast traffic, in general, they replicate it on all ports. Therefore, large switched LAN structure will be flooded with broadcasts and a great waste of bandwidth will be notable. Hence, users have traditionally been forced to utilize routers in order to partition their networks. There are reasons for utilizing VLANs, i.e., switching dependant networks, to reduce the need for routing in the network:

- **Higher Performance and Reduced Latency**

As the number of routers increases, delay begins to degrade network performance especially for recent delay-sensitive and interactive multimedia applications.

- **Ease of Administration**

Routers are administratively rich. This means routers require much complex configuration than switches.

- **Cost Considerations**

Switch ports are cheaper than router ports. Therefore, the increased dependency on switching and VLANs allows networks to be segmented at a lower cost if compared with routing segmentation.

The primary benefit of VLANs, which are dependant on switched networks, is that LAN switches supporting VLANs (*VLAN-aware switches*) can be used to minimize the broadcast traffic. This reduces the need for routing to the edge of the network and to move *inter-VLAN* traffic. The broadcast traffic in a VLAN needs only to be replicated on switches ports connected only to end-stations belonging to the same VLAN. Consequently, VLANs participate in creating the same type of broadcast *firewalls* that were usually provided by routers (Passmore and Freeman, 1998).

2.3.3.2 Reduction the Cost of Moves, Adds, and Changes

One of the most attractive features of VLAN implementation is the reduction in the cost of handling user moves and changes. These costs are really substantial and deserve being under debating. This is due to the fact that the traditional ways prepared to handle administrative management and operation usually represent the main expenses over the life of networks. However, capital costs such as purchasing the hardware and software represent an increasingly smaller proportion, usually below 20 percent.

Also, if we consider the dynamic nature of today's working environment which needs vast amounts of moves, adds, and changes, we find that the administration and management costs will become the dominant factors on the whole budget prepared for any network. There are several ways for minimizing the above vastly increasing costs (Smith, 1998).

VLAN implementation is a primary solution, which helps in handling these changes in the network effectively. Normally, in the traditional ways, when a network member moves to a different subnet, IP addresses must be manually updated in the workstation. The updating process consumes a considerable amount of time, and time is money, that could be employed in other productive endeavors such as developing new network services. VLANs, in one of its implementation types, solve this problem because VLAN membership is not tied to the location of the workstation. Therefore, moved workstations will retain their original IP addresses and subnet membership. The choice of the VLAN implementation type, which will be discussed in the following sections, is also important. The incorrect, inappropriate, choice of VLAN type may add extra costs to cope with the added complexities caused by the necessity to manage another layer of *virtual connectivity*, virtual workgroups, in conjunction with *physical connectivity*. Therefore, organizations must carefully choose the VLAN type, and must be sure that it doesn't generate more network administration than it saves (Passmore and Freeman, 1998). Moreover, VLANs eliminate the need for expensive routers if compared with switches used to construct the infrastructure VLANs. This

argument about switches is also true even for the new switches with routing functions, i.e., layer 3 switches (Varadarajan, 1997).

2.3.3.3 Formation of Virtual Workgroups

If we consider the definition of VLANs again, we can conclude the ability of VLANs to create *virtual workgroups*. Currently, it is common to form workgroups, which are composed of members from different departments, who work in the same team and have the same objectives.

To clarify the idea behind workgroups, consider teams consisting of members from departments such as marketing, sales, accounting, research, and engineering. Figure (2.2) presents the logical workgrouping with VLANs.

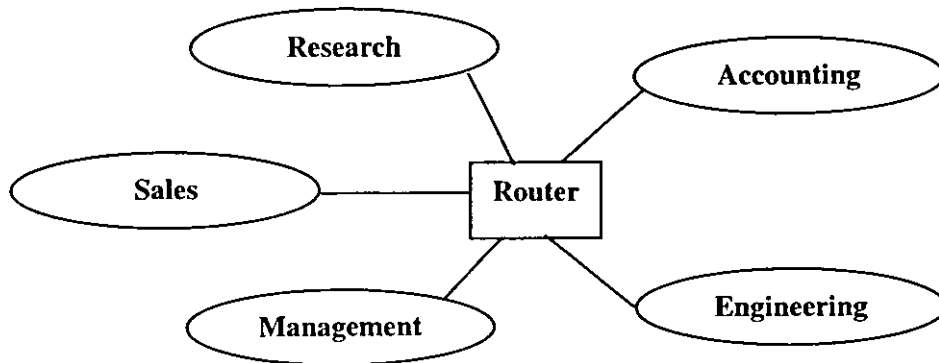


Figure (2.2) Logical Workgrouping with VLANs.

These workgroups are usually formed temporarily for a short period of time. In this period, VLANs are easily utilized to create these virtual workgroups (Netreference Inc., 1995).

2.3.3.4 Security Enhancement

Security enhancement represents an extremely vital demand in life in general and in the networking era as a special case. Currently, network vendors

realize the increasing importance of security considerations, especially as the *Internet* plays a bigger role, and especially as the working environment becomes more fragmented and flexible (Smith, 1998). Therefore, the security issues become more and more valuable assets that should be considered to protect the network resources from being accessed by any *eavesdropper* who doesn't have the accessing rights. However, the VLAN technology has outstanding capabilities that can be resorted to for enhancing the security needs. This enhancement is achieved without great need for extensive use of more complex, more expensive, router-based *firewalling* techniques. This important feature of VLANs comes from the ways by which the VLANs are defined throughout the network. These methods of definition will be discussed later in this chapter.

As a good example, in *port-based* VLANs configuration method, when used in combination with architectures depending on a single user per switch port, this will represent a powerful deterrent to unauthorized access. This is due to the fact that unauthorized users have no physical way of '*listening*' to broadcast or unicast traffic belonging to VLANs of which they are not a member, because that traffic never physically transverses their segment. Therefore, VLANs help in protecting development groups running sensitive, experimental, and risky applications (3Com Corporation, 1996).

To sum up, VLANs provide more security than broadcast networks since *frames* (packets) are delivered to their intended destinations rather than the whole network (Kawaguchi, 1996).

2.3.3.5 Keeping the 80/20 Rule

As mentioned earlier, VLAN supports the formation of virtual workgroups. This virtual workgrouping is often tied to support the '80/20 Rule', i.e., 80 percent of the traffic is 'local' to the workgroup while 20 percent is remote 'global' or outside the workgroup. Therefore, with virtual workgrouping by VLANs, only 20% of the traffic that is non-local will need to transverse a router. Incidentally, 80% of the local traffic between the workgroup members will not need to pass through routers depending on what is afforded by the VLAN technology (Netreference Inc., 1995).

All of the above is true if the 80/20 rule is applicable. But, this is not totally true for today's requirements since nowadays more of the traffic goes out of the workgroup than in the past. This is related to the introduction of *Internet, email, and client/server* environments (Smith, 1998).

2.3.3.6 Leveraging Network Monitoring

In general, network monitoring is inevitable in networking so as to help network managers to best segment their networks by keeping track of, for example, who is talking to whom. This is afforded by collecting and reporting network traffic statistics.

In *LAN-based* networking environment, *Remote Monitoring (RMON) protocol* is the widely used monitoring protocol. This protocol was created in 1991 as an extension of *Simple Network Management Protocol (SNMP)*. RMON is used for the retrieval of network statistics from remote devices. It consists of two elements: an *agent*, which is a remote 'sensor' placed on each

LAN segment to be monitored; and a *client*, which provides the management interface.

VLAN technology provides an efficient and cost-effective mechanism for monitoring. This intent of monitoring in VLANs is not achieved by RMON protocol primary version. This is due to the need for centralizing RMON agents at the network switch which becomes an inefficient and costly method of collecting network traffic data. As a result, new versions of RMON such as *distributed RMON (dRMON)* and RMON2 are invented to solve the problem of monitoring in the switched networks and VLANs.

In dRMON, the remote agents are attached to workstations rather than the switches. This will obviously leverage the processing power at the workstations, which will concurrently augment switches performance. However, the performance of the switches is enhanced because of the fact that RMON is *bandwidth-hungry* and *processor-intensive*. With RMON2 version, the role of monitoring is optimally fulfilled by enabling optimal configuration of VLANs (3Com Corporation, 1996; Smith, 1998).

2.3.4 VLAN Components

Networks that define VLANs contain one or more of the following networking components:

2.3.4.1 Switches

The VLAN technology is directly related, as discussed earlier, to the development in the switching technology. Switches represent the basic parts of any switched network. Hence, switches are really very important to construct

VLANs. Switches can group users, end-stations, or logical addresses into common communities or workgroups. Of course, this can be achieved if the intended switches are *VLAN-aware*, i.e., they understand how to define VLANs. VLAN-aware switches use frame identification, or *tagging*, to satisfy the interswitch communications in networks that define VLANs. The method of defining VLANs can be found in the following section. Generally, we can say that defining any VLAN depends on the availability of a suitable switching infrastructure.

2.3.4.2 Routers

The usage of routers in the virtual networking era is minimal and they are limited for satisfying the communications between VLANs.

2.3.4.3 Transport Protocols

These protocols are required to carry VLAN traffic across shared LANs and also on ATM backbones. ATM technology is considered here due to the anticipated deployment of this promising technology. With the help of these VLAN transport protocols, information can be exchanged between interconnected switches residing on the corporate backbone. However, VLAN information and identification between switches, routers, or other necessary devices are conveyed through that backbone by certain transport protocols.

2.3.4.4 Interoperability with Legacy LAN Systems

This should be taken into account because of the widespread installation of the legacy LANs. Therefore, VLANs need to provide compatibility with previously installed LAN systems. In addition, users need to be able to share

traffic and network resources that attach directly to switching ports with VLAN designation (Cisco Systems Inc., 1998).

2.3.5 VLAN Membership Methods

2.3.5.1 Preview

There are several techniques for defining VLANs. However, the four basic methods by which VLAN membership can be defined are:

1. Membership by switch port group.
2. Membership by *media access control (MAC)* address.
3. Membership by network layer information.
4. Rule-based grouping.

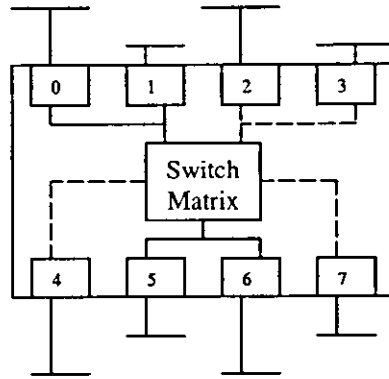
Most importantly, to choose a membership method, we need to consider the user needs and the network environment in which the VLAN will reside (3Com Inc., 1996). The importance of choosing the membership method comes from the advantages and disadvantages combined with any of the above methods. Therefore, it is possible to suggest a method, which may be suitable for certain situations, but, to some extent, is inappropriate for others. These basic methods will be clarified in the rest of this section.

2.3.5.2 Clarifying VLAN Membership Methods

2.3.5.2.1 Membership by Switch Port Group

In this method, VLANs are implemented depending on ports assignment of the switch(es). This means that, to form a VLAN, the administrator assigns each port of the switch(es) to a VLAN. The data is only directed to the required destination in the same broadcast domain, VLAN, by noting the port on which

packets arrive. This membership method can be easily understood from Figure (2.3) (Intel Corporation, 1998).



Legend: n Port (n) VLAN 1: Ports 0, 1, 5, 6
 LAN Segment VLAN 2: Ports 2, 3, 4, 7

Figure (2.3) Creating Port-based VLANs Using a LAN Switch.

The port assignment is done by means of an internal table in the switch (Hein and Griffiths, 1997). An example for these assignment tables is depicted in Table (2.2).

Table (2.2) Port-based VLANs.

Port	VLAN
1	Marketing
2	Marketing
3	Marketing
4	Engineering
5	Engineering
6	Engineering
7	Administration
8	Administration
9	Administration

Although this membership method is still the most common membership method due to its simplicity as a principle, it has some drawbacks (Passmore and Freeman, 1998). The most significant drawback is the inability to associate multiple VLANs to a network segment connected to a switch port (Held, 1997).

Hence, more ports are required which is directly related to increasing the cost of LAN switches. Also, as a primary disadvantage, the network manager must reconfigure VLAN membership when a user changes the switch port, i.e., it does not allow for user mobility (Varadarajan, 1997).

2.3.5.2.2 Membership by Media Access Control (MAC) Address

The VLANs that are composed here are totally dependent on the MAC addresses, which are universally given for each and every device (workstation) to be a part of its *network interface card (NIC)*. Therefore, these VLANs are referred to as *MAC-based VLANs* or as *layer-2 VLANs*, since the VLAN creation is done at the *data link layer* of the OSI reference model. Figure (2.4) gives a basic idea about this membership method (Held, 1997).

Legend:

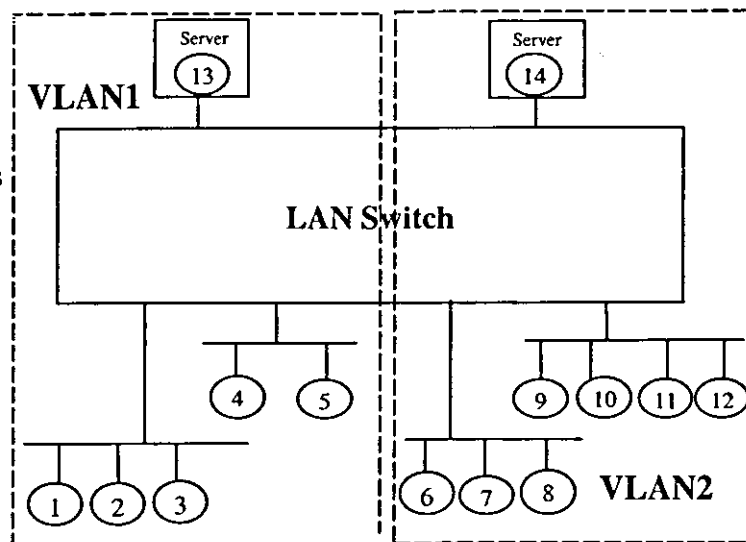
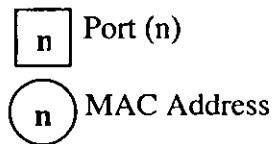


Figure (2.4) A Layer-2 VLAN.

This switch must be a VLAN-aware switch, i.e., it needs to track the MAC-addresses which belong to each VLAN. Every VLAN is given an allottee of the MAC-addresses and all these allocations are inserted into tables that are stored

in the LAN switch. Table (2.3) illustrates an example on these tables (Varadarajan, 1997).

Table (2.3) Assignment of
MAC Addresses to Various VLANs.

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

The notable significant advantages of layer-2 VLANs are the mobility and flexibility. The cause of these advantages is from the reality that MAC-addresses are parts of the NICs. Therefore, when a workstation is moved from one part to another, no reconfiguration is needed to reserve the VLAN membership. This is not always true for some *notebooks* and *laptops* with some *docking stations*, which keep the MAC-address on the desktop while these devices move all over the network. The mentioned advantages interact with the dynamic nature of nowadays business. Also, this method of VLANs definition is more secure than port-based defining method.

The main drawback of MAC address-based VLANs is the need to the initial assignment of the VLAN membership. However, this will lead to great problem in networks with great number of users, since this will become a time consuming task. In addition, a single MAC-address cannot easily be a member of multiple VLANs. The reason is that it is possible to cause serious problems with existing bridging and routing, which may produce confusion in switch *forwarding tables* (Intel Corporation, 1998; Varadarajan, 1997).

2.3.5.2.3 Membership by Network Layer Information

Network layer information (OSI reference model) can be exploited to define VLANs in two approaches. The VLAN membership of a packet is defined either by *protocols* used such as *Internet Protocol (IP)*, *Internet Packet Exchange (IPX)*, *Network Basic Input/Output System (NetBIOS)*, etc. or layer-3 (*Network layer*) *addresses*. It is necessary to demonstrate that the dependency on layer-3 information is not to be confused with network layer routing, i.e., no routing functions or calculations are needed (Passmore and Freeman, 1998).

- **Protocol-based VLANs**

Basically, the VLAN-aware switch decides that a frame belongs to a certain VLAN based on a certain field, which is usually used to indicate the protocol type within the frame (See Table (2.4)).

Table (2.4) Assignment of Protocols to Various VLANs.

Protocol	VLAN
IP	1
IPX	2

Generally speaking, like port-based VLANs, protocol-based VLANs are administrative-based. The intent of this defining approach is to make the networks run more effectively rather than to cope with the business movability and flexibility needs (Smith, 1998).

- **IP-based VLANs**

To clarify the idea behind defining VLANs depending on layer-3 IP-addresses, Figure (2.5) depicts the definition of two VLANs, as an example, on a suitable LAN switch (Smith, 1998). This figure refers to a vital interesting

point, which shows that the given switch supports the assignment of more than one VLAN per port. This is shown in port (1) of the LAN switch (Held, 1997).

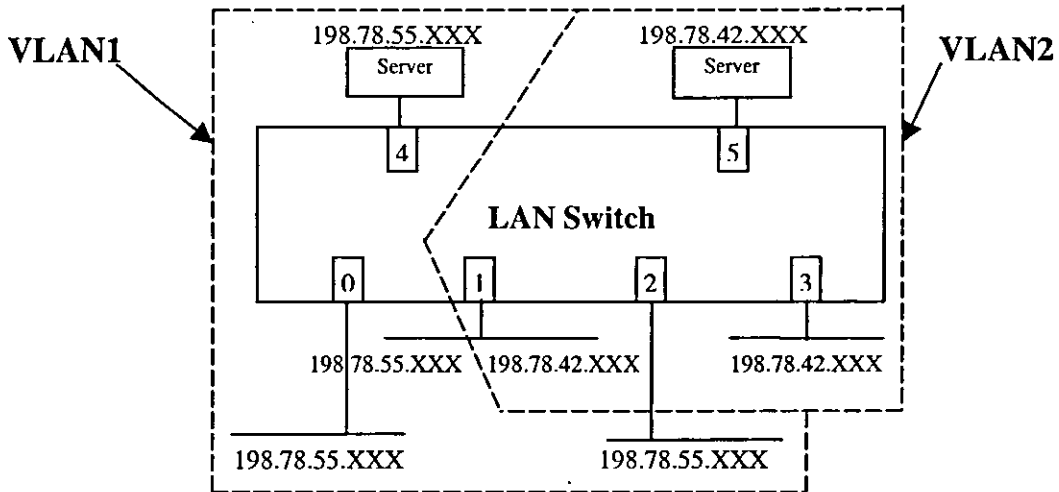


Figure (2.5) Example of a VLAN Creation Based on IP Addresses.

It is important to assert again on that the switches prepared for this type of VLANs shouldn't be confused with routers, i.e., no routing functions are done inside these layer-3 switches. Furthermore, layer-3 switches or multi-layer switches usually have the packet-forwarding function of routing built into an *Application-Specific Integrated Circuit (ASIC)* chip sets, which greatly ameliorates performance over central processing unit (CPU)-based routers. The packets are forwarded to their VLANs after inspecting the IP-addresses from the packets (Smith, 1998).

There are several advantages in the definition of VLANs with layer-3 information:

- a) It offers the ability to partition based on the protocol type. This may be attractive for network managers who are interested in *service-* or *application-based* VLANs.

- b) It contemplates the flexibility and mobility needs, since users can physically move without having to reconfigure each workstation's network address. This is suitable and effective in pure *Transmission Control Protocol/Internet Protocol (TCP/IP)* networks. This stems from the fact that some protocols, e.g., IPX, don't involve manual configuration at the desktop. Moreover, end-stations running '*non-routable*' protocols, e.g., NetBIOS, can't be differentiated, and thus, can't be defined as a member of a layer-3 VLAN.
- c) It eliminates the need for *frame tagging* (debated below) in order to handle interswitch VLAN communication, i.e., to communicate VLAN membership between switches. This will reduce the transport overhead.

Despite of the above major advantages, some drawbacks are mentioned in the literature. The most significant disadvantage is the performance degradation possibility, since inspecting IP-addresses in packets is more time consuming than looking at the MAC addresses in frames. As a result, VLANs based upon layer-3 information are generally slower than those using layer-2 information (Passmore and Freeman, 1998). Also, the speed problem is related to the necessity that the VLANs defined at layer-3 include configuration which is required to ensure that the network stations are operating with the correct protocol and network address (Held, 1997).

2.3.5.2.4 Rule-based Grouping VLANs

The new VLAN creation method is based on the ability of LAN switches to inspect the packets and utilize predefined fields, portions of fields,

or even individual bit settings as a mechanism for defining VLANs.

One of the *rule-based* methods that is usually discussed is what is called *IP-multicast* grouping method. The term '*multicast*' is unlike *broadcast* term, which travels everywhere on a network, and also contrasts *unicast* term, which is *point-to-point*. Therefore, multicast traffic is *point-to-multipoint* or *multipoint-to-multipoint*. IP-multicast method is accomplished by the use of *Class D* IP- addresses (224.0.0.0 to 239.255.255.255).

All workstations that join an IP-multicast group can be used to form the same broadcast domain although IP-multicast groups aren't actually VLANs, as they are set up and broken down automatically for short periods of time only (Held, 1997; Smith, 1998).

These VLANs enables a very high degree of flexibility and application sensitivity. Also, as a good feature and with this defining method, VLANs would inherently be able to span routers and thereby WAN connections (Passmore and Freeman, 1998).

On the other hand, major disadvantages can be identified. First, the complexity caused by the need to consider, for example, the value of a bit within a field of a packet. However, this will become a laborious task to correctly configure a complex VLAN. Second, as the number of *rules* associated with the creation of a VLAN increases, the packets flowing through a switch would suffer from notable latency due to the great effort required to examine the necessary fields within these packets (Held, 1997).

In order to complete the discussion of VLAN membership methods, many vendors suggest taking benefit from multiple methods of VLAN definition. Therefore, by using a combination of these methods, it is fruitful to produce a network, which enables network managers to fulfill efficiently their particular network environment. For instance, in an establishment that utilizes both IP and NetBIOS protocols, IP VLANs can be built depending on the preexisting IP subnets, and VLANs for NetBIOS end-stations by grouping with MAC-layer addresses (Passmore and Freeman, 1998). Anyway, Table (2.5) provides a summary comparison of the features and operational capability of VLAN creation methods (Held, 1997).

Table (2.5) VLAN Assignment Method Comparison.

Feature	Port Grouping			
	Switch	MAC-based	Layer-3-based	Rule-based
Connectivity beyond the workgroup	No	No	Yes	Yes
Ease of station assignment	Easy	Difficult	Easy-Difficult	Easy-Difficult
Flexibility	None	Moderate	Moderate	High
Improved workgroup bandwidth	Yes	Yes	Yes	Yes
Multicast support	Inefficient	Inefficient	Efficient	Efficient
Multiple VLANs per port	No	Possible	Possible	Possible
Security	High	Low-High	Low-High	Selectable
VLAN spanning switches	Possible	Possible	Yes	Yes

2.3.6 VLAN Membership Information Communication

2.3.6.1 Overview

The main intent of this section, after presenting the various methods for defining VLANs, is to answer a logical question. The question is: "*What is best*

for communicating VLAN membership information across multiple switches throughout the entire network

To answer this question, two general approaches are considered to convey VLAN membership information across multiple switches, either *implicit* or *explicit*. Normally, for layer-2 VLANs which are defined by port or MAC addresses, the explicit method is employed to communicate their VLAN memberships. On the other hand, in layer-3 VLANs, the memberships are communicated implicitly.

There are two methods that are prepared to fulfill the explicit method. The first standardized method is via an ATM backbone by considering what is called *LAN Emulation (LANE)*. The second, the method is formulated under the *IEEE 802.1Q VLAN Standard*. The latter method deals with *frame tagging*, i.e., adding tags to packets headers to distinguish VLAN membership (3Com Corporation, 1996; Intel Corporation, 1998).

2.3.6.2 Interswitch VLAN Communication

If we ignore having ATM infrastructure (backbone) there are three methods used to investigate the interswitch communications in VLANs. These methods are:

2.3.6.2.1 Table Maintenance via Signaling

Layer-2 switches, like bridges, have cached address tables. These tables are used to determine the VLAN membership by considering the receiving port or the MAC address. Therefore, a frame arrives at the layer-2 switch for the

attached port number. Then, this new information is broadcast continuously to all other switches where there are many switches adds, and networks expansions, the constant updating and signaling of these cached tables of each switch can cause so much backbone congestion. This, of course, converses the expected minimization of congestion, to some extent, with the VLAN technology. Consequently, the signaling method is neither scalable nor practical.

2.3.6.2.2 Time-Division Multiplexing (TDM)

In order to satisfy interswitch communications, channels are dedicated for each VLAN. Although this approach cuts out some of the problems in signaling and in frame tagging (see VLAN Trunk Tagging below), it is not suitable due to the fact that a time slot reserved to one VLAN can't be utilized by another VLAN, even when the channel is idle. Therefore, the TDM method is the less commonly used method.

2.3.6.2.3 VLAN Trunk Tagging

In this approach, a header is typically added into each frame on interswitch trunks to uniquely determine to which VLAN the frame belongs. *Trunking* is the process by which the devices within the network read and understand the virtual geography of the network. These headers are inserted immediately after the destination and source addresses of the conventional frames (IEEE 802.1Q, 1997). The addition of these headers into the frames causes overhead to the network traffic. This technique of trunk tagging helps the switches to know where each VLAN lies and not which users are in which

VLAN. The determination of VLAN membership is achieved by what is called *internal tagging* which is done inside the intended switch (Passmore and Freeman, 1998; Smith, 1998).

2.3.6.3 Frame Processing

Once again, VLAN-aware switches can determine to which VLAN the received data belongs. This is done either explicitly or implicitly. In explicit tagging, a *tag* is inserted into each frame. Also, every switch has a *filtering database* by which it can decide where to send the data. However, this subsection will be employed to discuss three main topics: the filtering database, the tagging process, and the structure of the tag header.

2.3.6.3.1 Filtering Database

This database contains the membership information for VLANs. It consists of two types of entries:

a) Static Entries:

These entries are added, modified, and deleted by *management* only. They are classified into two classes:

i) Static Filtering Entries

This type of entries is used to decide whether to forward or to discard the arriving frames after inspecting their MAC destination addresses and their intended VLAN.

ii) Static Registration Entries

The intent here is to specify whether frames to be sent to a specific VLAN are to be tagged or untagged and the ports registered for that VLAN.

b) Dynamic Entries:

These entries are found as a result of a *learning process* and can't be created or changed by management. However, entries are updated in the database as a result of aging, i.e., after elapsing a certain amount of time specified by management (10 sec –1,000,000 sec).

The learning process observes the port on which a frame, with a given source address and VLAN identifier (VID), is received, and then updates the filtering database. Generally, there are three types of dynamic entries:

i) Dynamic Filtering Entries

They are used to decide whether the frames which are to be sent to a certain VLAN member, i.e., certain MAC address on it, should be forwarded or discarded.

ii) Group Registration Entries

These are employed to indicate for each port whether frames which are to be sent to a group MAC address, and on a certain VLAN, should be filtered or discarded. The entries of this type are updated using *Group Multicast Registration Protocol (GMRP)* (IEEE 802.1Q, 1997).

iii) Dynamic Registration Entries

They determine which ports are registered for a specific VLAN. These entries are updated using *GARP VLAN Registration Protocol (GVRP)*, where GARP is *Generic Attribute Registration Protocol* (IEEE 802.1Q, 1997). GVRP allows both VLAN-aware workstations and switches (bridges) to issue and revoke VLAN-memberships.

In a network that consists of different bridges, switches, and LAN segments, we find ourselves in need to debate what is called '*active network*' concept. The active network topology is determined with the help of the *spanning tree algorithm*. This algorithm prevents the formation of loops in the networks by disabling certain ports. This is done when the bridges are turned on or when a bridge in the current network topology is perceived. Once an active topology is established, an active topology for VLAN is also obtained (Varadarajan, 1997).

2.3.6.3.2 Frame Tagging

The IEEE 802.1Q Standard specifies the purposes of the frame tagging as follows (IEEE 802.1Q, 1997):

- a) It allows *IEEE 802 LAN MAC frames* to carry *user-priority information*, since these frames have no inherent ability to signal priority information at the MAC protocol level.
- b) It allows the frame to determine the format of MAC address information carried in MAC user data.
- c) It allows VLANs to be supported across different MAC types.
- d) It allows MAC frames to carry VLAN identification (VID) information, which is used to determine to which VLAN the frame belongs.

Generally, the tagging process requires:

- a) The addition of a *tag header* to each frame format. This header is added directly following the destination MAC address and source

address (routing, if present) fields.

b) If the source and destination media access methods differ, tagging the frame may involve translation or encapsulation of the remainder of the frame. This is clarified through *Annex C* of *IEEE 802.1Q Standard*.

c) Recomputation of the *Frame Check Sequence (FCS)*.

2.3.6.3.3 Structure of the Tag Header

The tag header consists of two components as shown in Figure (2.6). The following points presents what is meant by the fields of the tag header.



Figure (2.6) Tag Header Structure.

i) **Tag Protocol Identifier (TPID)**, which identifies the frame as a tagged frame.

ii) **Tag Control Information (TCI)**. It consists of the following elements:

a) **User-Priority Information**. It is a 3-bit field, which allows priority information to be encoded in the frame. Eight levels of priority are allowed, where level *zero* is the lowest priority and level *seven* is the highest priority.

b) **Canonical Format Identifier (CFI)**. It is used to indicate that all MAC addresses present in the MAC data field are in canonical format. This is interpreted differently depending on whether it is an *Ethernet-encoded tag header* or a *Subnetwork Attachment Point*

(SNAP)-encoded tag header. SNAP is an encapsulation scheme that is utilized in conjunction with the *Logical Link Control (LLC)* of the OSI Reference Model (Handel, et al., 1998). In Ethernet-encoded TPID, CFI refers to the presence of the *Source-Routing Information Field (RIF)* after the length field. The RIF field refers to routing on Ethernet frames. On the other hand, in SNAP-encoded TPID, the CFI indicates the presence or absence of the canonical format of addresses.

- c) **VLAN Identifier (VID)**. It is used to uniquely identify the VLAN to which the frame belongs (IEEE 802.1Q, 1997; Varadarajan, 1997).

Figure (2.7) presents the TCI format:

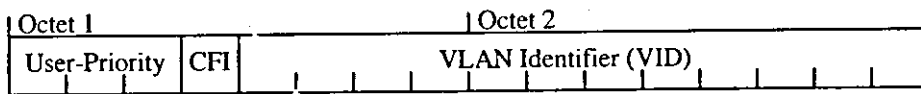


Figure (2.7) Tag Control Information (TCI) Format.

Again, there are two forms of the tag header, depending on the type of encoding used for the TPID. These two types are:

i) Ethernet-Frame Tag Header (Ethernet-encoded TPID):

The overall structure of the header is shown in Figure (2.8).

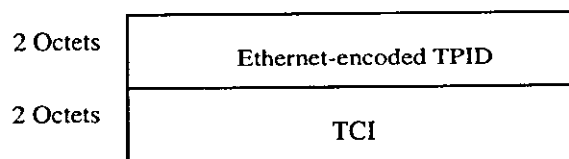


Figure (2.8) Ethernet-Encoded Tag Header.

This form of tag header is used when the tagged frame is to be transmitted on IEEE 802.3/Ethernet media. In case of Ethernet media, this tag header has the unfortunate effect of increasing the potential maximum frame size to over that which is allowed by Ethernet. Up till now, the IEEE 802.1Q committee has come up with no definite answers to this problem, while other committees within the IEEE 802 group are currently discussing modifying the standards to allow an increase in the maximum frame size by several *octets*. Incidentally, this would mean a change in the very basic networking standards under usage today, thereby, more interoperability problems associated with this intent to change the current standards.

ii) Token Ring and FDDI Tag Header (SNAP-encoded TPID):

The overall structure of the header is illustrated in Figure (2.9).

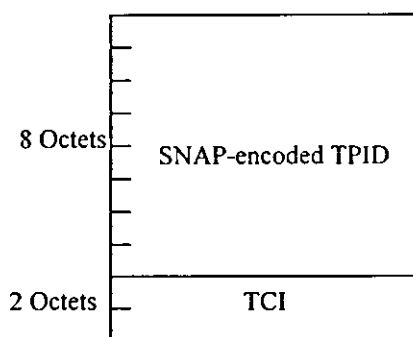


Figure (2.9) SNAP-Encoded Tag Header

Finally, we can perceive that the TCI field is 2 octets in length, and 12 bits are allocated for the VID field. Hence, there can be a maximum of $(2^{12}-1)$ VLANs. Zero is used to indicate no VLAN ID, but the user priority information is always present. This allows priority to be encoded in non-priority LANs (Smith, 1998).

To summarize, when a packet enters its local switch, the VLAN membership can be determined by any of the above mentioned VLAN defining methods. When the packet travels to other switches, the determination of VLAN membership for that packet can be either implicit or explicit. Generally, port-based VLANs are almost always implicit. As a final note, when the packet exits the switched network, the switch strips the header and forwards the frame to interfaces that match the VLAN identifier (Intel Corporation, 1998; Cisco System Inc., 1997).

2.3.7 Inter-VLAN Communication

Usually, it is expected to define various VLANs throughout the entire network. Hence, it is required to answer an important question. This question is “How is traffic transported between these various VLANs?” The quick answer to this question is by *routing*. This means that routing is still required for inter-VLAN traffic (Passmore and Freeman, 1997). There are various protocols which are available for routing between VLANs:

a) Inter-Switch Link (ISL)

Inter-Switch Link (ISL) is a packet-tagging protocol that contains a standard Ethernet, FDDI, or Token Ring, frame and the VLAN information. Currently, ISL is supported only over Fast Ethernet links, but a single ISL can carry different protocols from multiple VLANs.

b) IEEE 802.10 Protocol

This protocol provides connectivity between VLANs. Originally, it is developed to contemplate the growing need for security within shared

LAN/MAN networks. Additionally, by functioning at layer 2, it is well suited to high-throughput, low-latency switching networking environment.

c) ATM LAN Emulation (LANE) Protocol

The ATM *LAN Emulation (LANE)* protocol provides a methodology by which legacy LAN users can utilize from the ATM features without demanding modifications to end-stations hardware or software. In other words, LANE provides the basic functionality of Ethernet and Token Ring, while sacrificing some ATM benefits and a few LAN features. Therefore, with the help of LANE, legacy LANs traffic can be conveyed through an ATM network which will function like a LAN. Also, VLANs take use of LANE. To accomplish this, special software is installed on an ATM client workstation, called the *LAN Emulation Client (LEC)*. The client software communicates with a central point called a *LAN Emulation Server (LES)*. A *Broadcast and Unknown Server (BUS)* acts as a central point to distribute broadcasts and multicasts. The *LAN Emulation Configuration Server (LECS)* has a database of LECs and their *Emulated LANs (ELANs)* (Cisco Systems Inc., 1997; Finn, et al., 1996).

Finally, although routing is the primary method for inter-VLAN communication, it is not the only method. As another method, it is possible that a VLAN member (usually a server) be a member of more than one VLAN, effectively providing an application-layer gateway between VLANs (3Com Corporation, 1996).

2.3.8 VLAN and ATM

The development in ATM technology is notable worldwide. This

technology is primarily dependent on switching. Also, the concept of VLANs is originated with LAN switching principles. Therefore, it is logical to anticipate that the usage of VLANs may need to be extended to environments where ATM networks and ATM-based devices are present. Eventhough, combining VLANs and ATM networks is fruitful in some situations, however, this creates a new set of issues for network managers such as relating VLANs to ATM ELANs, and deciding where to place the routing function.

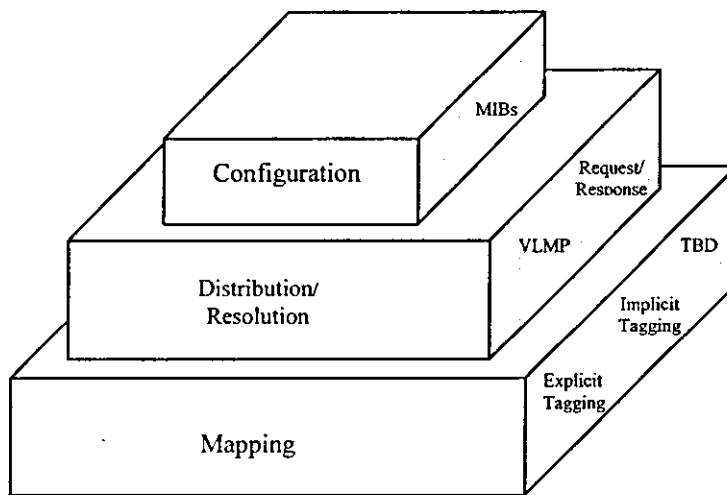
As an example on how VLANs can be made transparent to ATM in an environment where ATM exists only in the backbone, i.e., there are no ATM-connected end-stations, ATM *permanent virtual circuits (PVCs)* may be set up to carry intra-VLAN traffic between multiple LAN switches. In this case, ATM switches don't have to be VLAN-aware, i.e., ATM backbone switches could be selected regardless of VLAN functionality (Passmore and Freeman, 1998; Smith, 1998).

2.3.9 VLAN Standardization

Generally, any technology needs to be standardized in order to be universal and widespread. Before *August 1998*, the date in which the IEEE committees accredited the *VLANs Standards*, many vendors have developed their own proprietary VLAN solutions and products. However, since products have been proprietary, anyone wanted to install VLANs needed to purchase all products from the same vendor.

The work on the VLANs standards, known as IEEE 802.1Q, began in *March 1996* with the issuance of a *Project Authorization Request (PAR)* entitled

“Standards for Virtual Bridged Local Area Networks”. The PAR was given the 802.1Q project number (Held, 1997; Varadarajan, 1997). Under the umbrella of IEEE 802.1Q, a three-level model framework for VLANs is proposed. Figure (2.10) illustrates the general format of the 802.1Q architectural model. A detailed discussion about the VLAN architectural model can be found in (IEEE, 1997).



where:

MIB Management Information Base
 VLMP Virtual LAN Mapping Protocol
 TBD To be determined

Figure (2.10) VLAN Architectural Model.

Finally, before completing this background chapter about VLANs, the reader may ask about the possibility of defining *VLANs over WANs*. Theoretically, VLANs can be extended across the WAN, however, this is generally not recommended, since VLANs defined over the WAN will permit LAN broadcast traffic to consume expensive WAN bandwidth. However, if WAN bandwidth is available and free for a particular organization, then extending VLANs over a WAN can be utilized. Also, depending on how

VLANs are defined, IP-based VLANs can be effectively extended across the WAN (Passmore and Freeman, 1998).

Chapter 3

Simulation Models

3.1 Preview

In this thesis, since we are concerned in evaluating the performance of VLANs, several *simulation models* are proposed. These simulation models are studied depending on some *performance measures*. In order to perform the simulation, a computer simulation tool is used. This simulation tool is called *COMNET III*.

This chapter presents a basic overview about COMNET III and the proposed simulation models. The performance measures (i.e., simulation parameters) taken into consideration are discussed in the simulation models section.

3.2 Overview about COMNET III

As computer networks become larger and of more complex design, their analysis becomes an ever-challenging task. However, evaluating the performance of these networks depending on the analytical modeling is difficult and sometimes impossible. Therefore, system designers and network planners are increasingly looking for tools by which they can analyze their networks in order to enrich their decision making criteria.

COMNET III is a performance prediction tool for computer and communication networks. Depending on the description of the network, its control algorithms and workload, COMNET III simulates the operation of the network and provides measures of its performance.

The user of this simulation tool can notice that it is integrated into a single windowed package which performs all functions of model design, model execution, and presentation of results. Any model which needs to be simulated can be built and executed using the following steps:

- a) *Nodes, links, and traffic sources* are selected from a library and then brought into position on the screen.
- b) These elements are connected using a connection tool.
- c) The user double clicks on nodes, links, or traffic sources. A dialog box with all adjustable parameters appears and the user specifies the parameters for the chosen item.
- d) Network operations and protocol parameters are set in additional boxes.
- e) The model is verified and executed, after which the results are predicted in a report which can be read and analyzed.

This multipurpose computer simulation tool is a trademark of the *CACI Products Company*. This American company is famous in the field of developing computer and communication simulation tools (CACI, 1995).

To satisfy the purpose of this thesis, COMNET III is employed to predict the performance of VLANs.

3.3 Simulation Models

The purpose of this section is to illustrate the simulation models on which the performance evaluation of VLANs is done. In this respect, this section is partitioned in a way through which the reader can understand the

methodology by which these models are employed to satisfy the purpose of this research.

3.3.1 The Main Network

Without loss of generality, it is assumed that the suggested computer network which is examined in simulation is prepared to represent a university campus computer network. This network is illustrated in Figure (3.1).

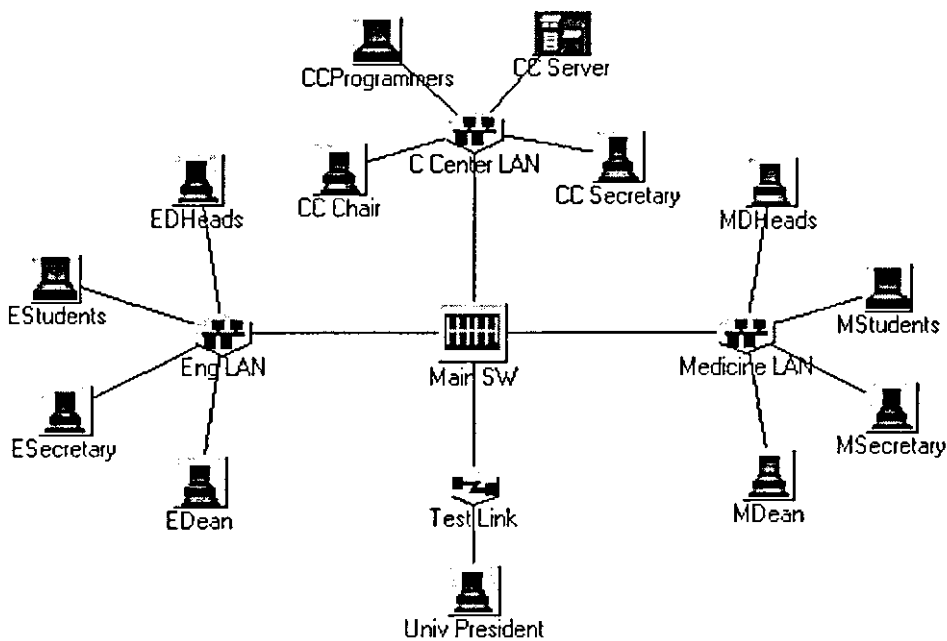


Figure (3.1) A University Campus Computer Network.

Figure (3.1) shows that the network consists of three main LAN segments. These LAN segments are *the engineering LAN (E LAN)*, *the medicine LAN (M LAN)*, and *the computer center LAN (CC LAN)*. A main switch connects the shown LAN segments to each other. The number of members in any LAN segment is assumed to be the same in all segments. This equality isn't necessary, but this is assumed to simplify preparing the traffic profile of the network. All nodes (PCs or servers) can be either VLAN-aware or VLAN-unaware. It depends on the model to be simulated. Similarly, the

main switch can be either VLAN-aware or VLAN-unaware. It also depends on the model to be simulated. Finally, the *test link* that connects the university president with the main switch is chosen to cause no bottleneck. Table (3.1) presents some details of the university network.

Table (3.1) Some Details of the University Network.

LAN Segment	Members	Link Type
CC LAN	CC Chair CC Secretary CC Programmers* CC Server	CSMA/CD**
M LAN	M Dean M Secretary M Students* M Departments Heads	CSMA/CD
E LAN	E Dean E Secretary E Students* E Departments Heads	CSMA/CD

* It represents a group of users. It is used to be able to change the number of users in the LAN segments.

** The link type will be changed in other simulation models.

3.3.2 Employing the Main Model

The network that is presented in Figure (3.1) will be used in the performance evaluation process. This will be done by using it as a legacy model in one stage and as a VLAN model in another stage. Therefore, the main model will be referred to as a legacy model or as a VLAN model. This is done for comparison purposes between legacy LANs and VLANs performance. Incidentally, the comparison will be employed in judging on the VLANs performance.

In this respect, several case studies are considered throughout the simulation process. These case studies are related to the effect of defining

VLANs on the university network performance by considering the behavior of some performance measures. The behavior of the chosen performance measures is perceived by changing some parameters such as message size conveyed through the network and number of users connected to a LAN segment.

3.3.3 Performance Measures

There are several performance measures that can be chosen in studying computer networks. In this thesis, the performance measures that are taken into consideration are:

- a) End-to-End Message Delay
- b) Link Utilization

End-to-End message delay refers to the time needed to receive a response for a message sent from a certain point in the network. This measure is really important due to the effect of delay on today's applications. However, we define link utilization as how much the link (e.g., CSMA/CD link) is busy throughout the simulation time. On other words, it can be used to determine to what degree the link is free or idle during simulation.

For our purposes, the links are assumed to be error free, i.e., no retransmission of messages is required by the destination nodes since any message arriving at its destination is assumed to be errorless. The study of error effect is out of the scope of this thesis.

To sum up, in all simulation models that are tested, we will concentrate on these performance measures in our journey to predict the performance of VLANs.

3.3.4 Defining VLANs

The reader of section (2.3.5) of this thesis can easily deduce that there are several methods to define VLANs. However, in this thesis we concentrate on IP-based VLANs. In this method of VLANs definition, the switch can support the assignment of more than one subnet per port, therefore, this enables VLANs to cooperate with legacy technologies (see Figure (2.5)). Consequently, to be able to define VLANs in the university campus computer network, the main switch should be chosen to be layer-3 VLAN-aware switch. The packets are forwarded to their VLANs after inspecting the IP-addresses from the packets.

For explanation purposes, we will define one VLAN in the main network of Figure (3.1). The members of this VLAN are the university president, the engineering dean, the medicine dean, and the computer center chairperson. This VLAN will be used in most of our performance studies in comparison with the legacy model. Let us call this VLAN as the *university committee VLAN (UC VLAN)*.

3.3.5 Case Studies

Once again, the behavior of the chosen performance measures will be noticed by changing some parameters in the network. This will be clarified in the following case studies.

3.3.5.1 Changing the Message Size

After defining the background traffic of the university network and the traffic profile of the whole network has become stable and balanced, a message is chosen to be conveyed from the university president to the university deans and the computer center chairperson. This message is needed for testing purposes and represents the foreground traffic. The effect of changing this message size on computer center link utilization, as an example, and the end-to-end message delay will be studied in case of the legacy model and after defining the UC VLAN. Also, the effect of message size will be clarified by considering the transmission delay imposed by the CC link. CC link is only chosen as a case study.

3.3.5.2 Changing the Number of Members in All LAN Segments

We will change the number of members in every LAN segment by changing the number of members in the group nodes. These nodes are the E students node, the M students node, and the CC programmers. The effect of changing the number of LAN members will also be studied in terms of link utilization and end-to-end message delay.

3.3.5.3 The Effect on Downloading

The performance of VLANs will be tested if the university president needs to download a file from the CC server. A message will be sent from the president and the CC server will respond by a greater file. The effect on downloading will be seen by considering the change in the CC link utilization

and the end-to-end message delay. This is done by changing the size of the downloaded file.

3.3.5.4 One of the Links Becomes Busier Transiently

We assumed that the medicine LAN segment suffers from a transient traffic and its utilization becomes higher. What is the effect of this on the communication between the president and the M Dean in both legacy model and VLAN model. Here, the message size will also be changed.

3.3.5.5 Communication between Two VLANs

In this case study, we will assume that there are two VLANs defined as depicted in Table (3.2).

Table (3.2) Defining Two VLANs in the University Network.

VLAN 1	CC Chairperson	E Dean	M Dean	University President
VLAN 2	CC Programmers	E Students	M Students	-

A message needs to be conveyed between the CC programmers and the CC chairperson. Although they are in the same LAN segment but they are members of different VLANs, therefore, a routing function is required to satisfy the communication between these two VLANs. The effect of this will be studied by changing the message size parameter.

3.3.6 Implementing VLANs in a Switched Network

The network suggested in Figure (3.1) will be modified to be able to define VLANs in a switched infrastructure. This will be implemented by means of changing the legacy LAN segments (CSMA/CD segments) with switching fabrics. This is depicted in Figure (3.2).

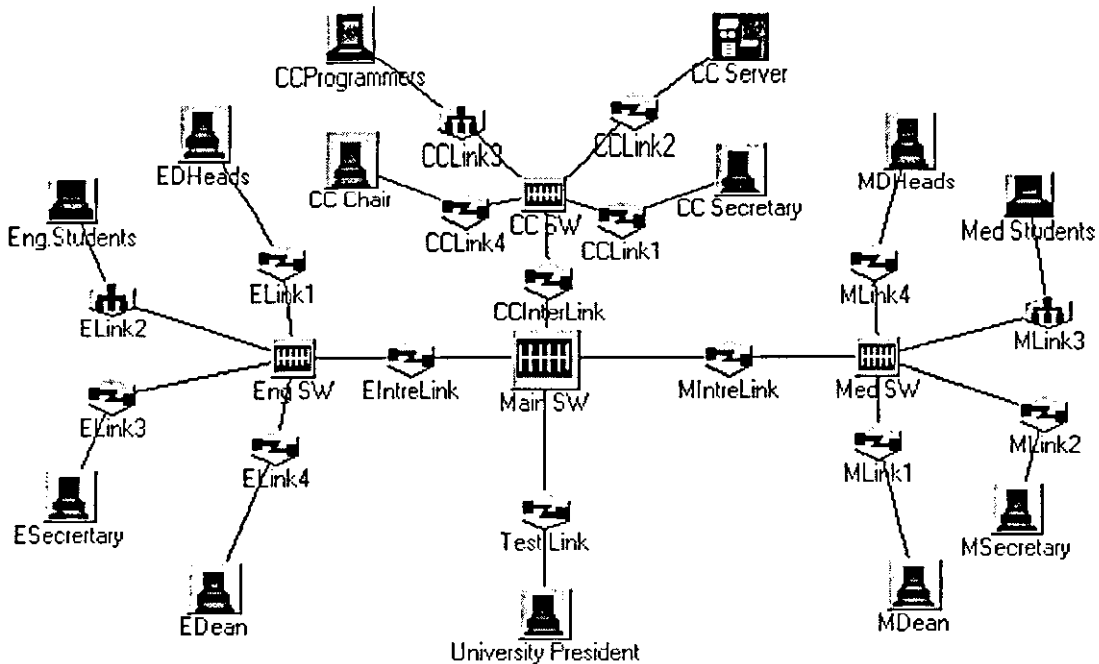


Figure (3.2) A University Campus Switched Computer Network.

Figure (3.2) shows that in every LAN site we have a switch. Therefore, there are three switches connected via suitable links to a switch (main switch). This presents a switched network. The tendency to examine VLANs in case of switched networks is suggested to emulate current demands on switching.

As a result, we will employ the suggested network in Figure (3.2) to deduce the effect of defining VLANs in a switched infrastructure which is chosen to be VLAN-aware in contrast with an ordinary (VLAN-unaware) switched infrastructure. This means that switches chosen in case of VLANs will be VLAN-aware to be able to understand the VLAN memberships. The reader of section (2.3.6.2) can find that there are three methods to satisfy the interswitch communications. However, we would use the method which is dependent on the maintenance via signaling which satisfies our purposes. Therefore, the switches chosen in case of defining VLANs will have cached address tables. These tables are used to determine the VLAN membership.

Two case studies are chosen to study the performance of the new switched network.

3.3.6.1 Effect of Changing Message Size

A message will be chosen to travel between the university president and the CC chairperson. The size of this message will be changed in order to see the effect on the selected performance measures. The VLAN defined will be the same UC VLAN.

3.3.6.2 Downloading Case Study

The university president will download a file from the CC server. The size of the downloaded file will be changed to predict the effect on the performance measures. The defined VLAN will embrace the CC chairperson, the CC server, the engineering dean, and the medicine dean.

3.3.7 Mixed Network Model

The model which will be studied here is of mixed infrastructure. This means that we will change one of the used LAN segments of Figure (3.1) with a suitable switch. This is clarified in Figure (3.3). The new model is proposed in order to cope with the practical situation in which we find ourselves in need to deal with a mixed network.

Again, the performance analysis of this network will be done with the same criteria followed in the previous models. In this respect, when we study VLANs performance in terms of end-to-end message delay and link utilization, the UC VLAN will be defined.

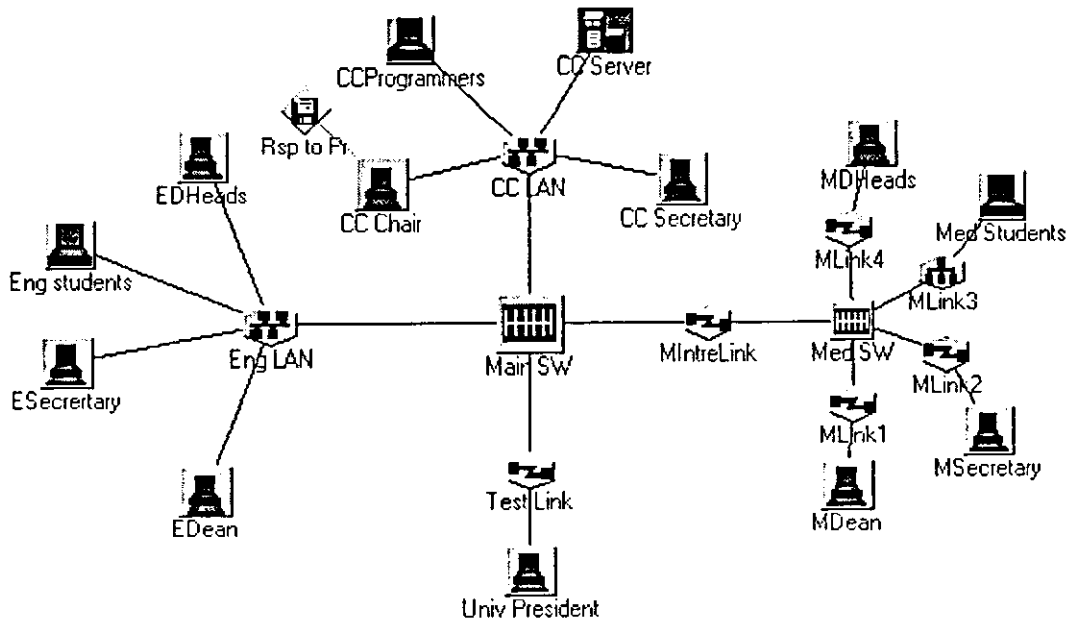


Figure (3.3) A University Campus Mixed Computer Network.

Chapter 4

Simulation Results and Discussion

4.1 Preview

The simulation models proposed in the previous chapter are tested in order to predict the behavior of the suggested performance measures. This chapter presents the simulation results in terms of graphs. For comparison purposes, every graph is used to show the behavior of a certain performance measure for both the legacy model (or VLAN-unaware switched model) and the VLAN model. Furthermore, this chapter presents the discussion of the simulation results. Therefore, every graph is put under the scrutiny of discussion.

4.2 Simulation Results

4.2.1 Results of Simulating the Main Network

All graphs discussed in this part are related to the simulation results of the University Campus Computer Network shown in Figure (3.1). Therefore, the same case studies debated throughout section (3.3.5) are considered.

4.2.1.1 Changing the Message Size

A message is conveyed from the university president to the CC chairperson. The size of this message affects several aspects. This is illustrated in the following points:

4.2.1.1.1 Effect on the CC Link Utilization

The CC link utilization is affected by changing the message size. Figure (4.1) illustrates this effect for the legacy model and the VLAN model.

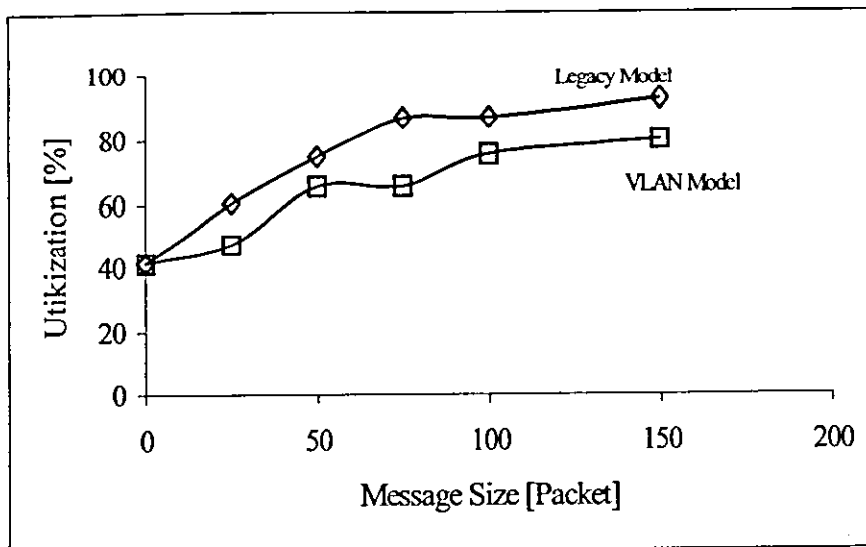


Figure (4.1) Effect of the Message Size on the CC Link Utilization in the Main Network.

Figure (4.1) shows that the CC link utilization for the legacy model is higher than that for the VLAN model. This means that the link will be free for other users if we define the UC VLAN. Also, it is obvious that as we increase the message size, the utilization increases until it reaches a steady state for a network with or without VLAN definition.

4.2.1.1.2 Effect on End-to-End Message Delay

For both the legacy model and the VLAN model, as we increase the message size the time consumed as an end-to-end delay also increases. This is due to the fact that the increase in the message size imposes a need for more time to be elapsed before accessing LAN segments. Also, it is found that in VLAN models the delay imposed is less than that in legacy models. This can be explained depending on that the number of members in the VLAN broadcast domain is less. This is shown in Figure (4.2).

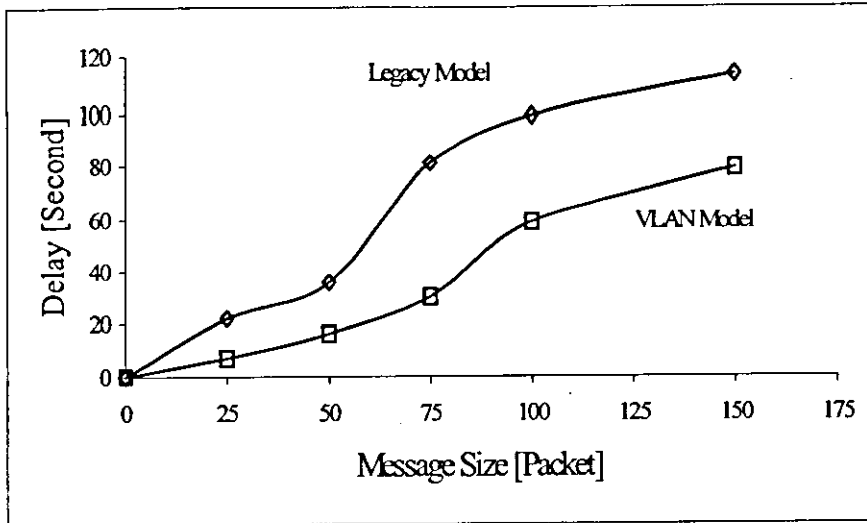


Figure (4.2) Effect of the Message Size on the End-to-End Delay in the Main Network.

4.2.1.1.3 Effect on the Transmission Delay via the CC Link

The CC link segment imposes some delay on any message using the link. This delay versus the message size is illustrated in Figure (4.3).

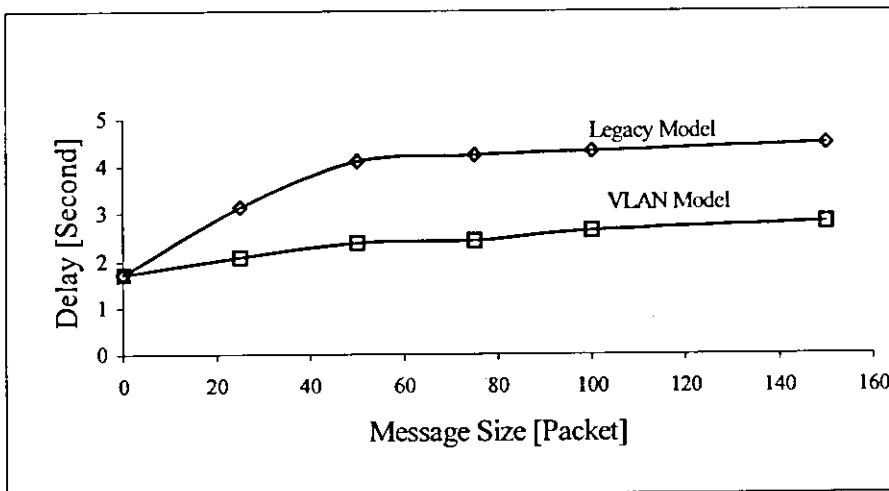


Figure (4.3) Effect of the Message Size on the Transmission Delay via the CC Link in the Main Network.

It is easy to perceive that if we define VLANs the transmission delay via the links (CC link for example) becomes less if we compare this with the legacy model. Also, the transmission delay in both cases reaches a steady state which is related to the behavior of the link utilization presented in Figure (4.1).

4.2.1.2 Changing the Number of Members in All LAN Segments

The addition of more users to the main network LAN segments has its reflection on different aspects in either the VLAN model or the legacy model.

4.2.2.2.1 Effect on the CC Link Utilization

The relation between the CC link utilization as a case study and the number of added users is clarified throughout Figure (4.4).

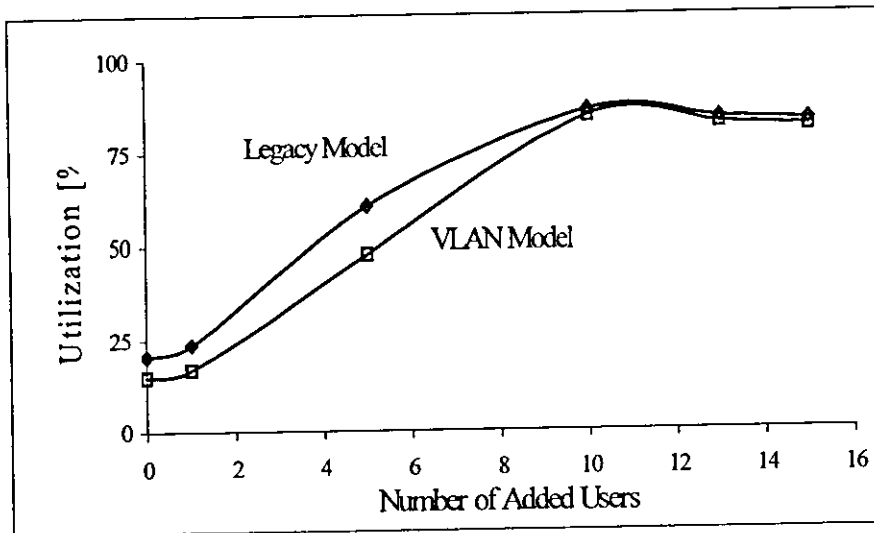


Figure (4.4) Effect of the Number of Users on the CC Link Utilization in the Main Network.

This figure shows that the utilization increases as we increase the number of users and also reaches a steady state for certain number of users. Moreover, we can deduce that although the utilization in the case of the VLAN model is less than that in the legacy model, the difference is not generally large and even disappears after adding certain number of users, say 15 user. This is related to the fact that defining VLANs in busy links doesn't represent a panacea for the problem of utilization since links are originally busy.

4.2.1.2.2 Effect on End-to-End Message Delay

The story of the CC link utilization is nearly repeated for the end-to-end message delay. The VLAN model and the legacy model behave nearly the same in case of adding users. It is obvious that the delay increases as a result of adding more users. This is depicted in Figure (4.5).

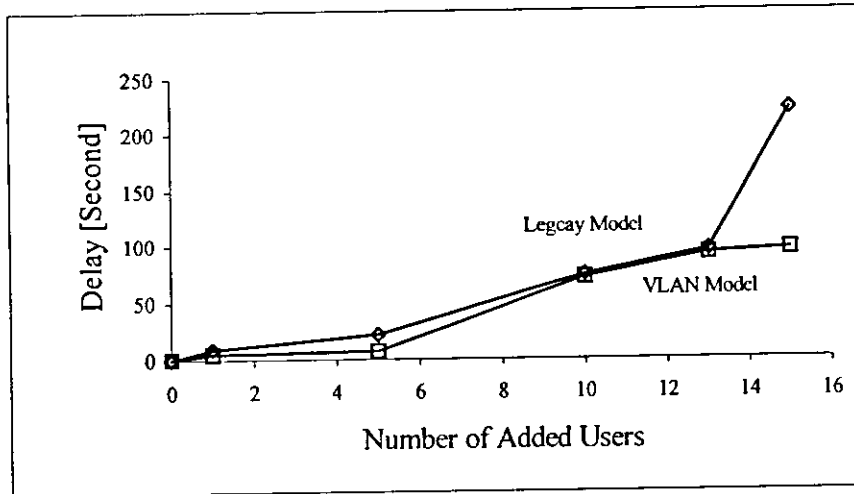


Figure (4.5) Effect of the Number of Users on the End-to-End Delay in the Main Network.

4.2.1.2.3 Effect on Transmission Delay via the CC Link

The relation between the transmission delay via the CC link and the number of added users is illustrated in Figure (4.6).

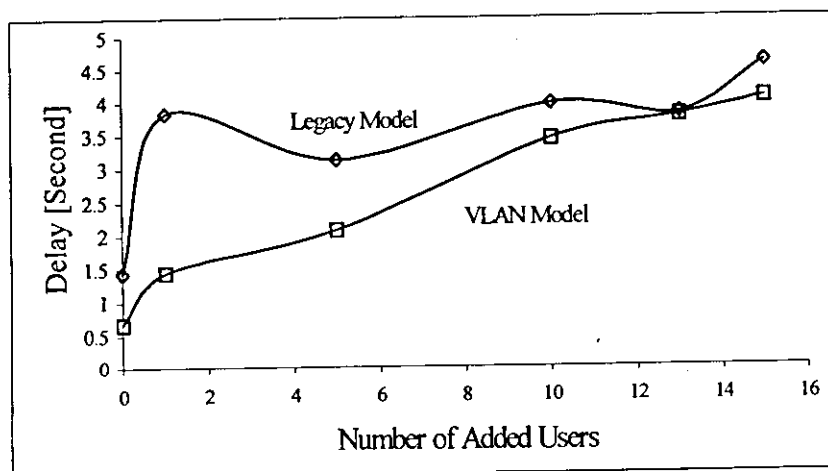


Figure (4.6) Effect of the Number of Users on the Transmission Delay via the CC link in the Main Network.

4.2.1.3 Effect on Downloading

The effect on downloading can be perceived from Figures (4.7) and (4.8).

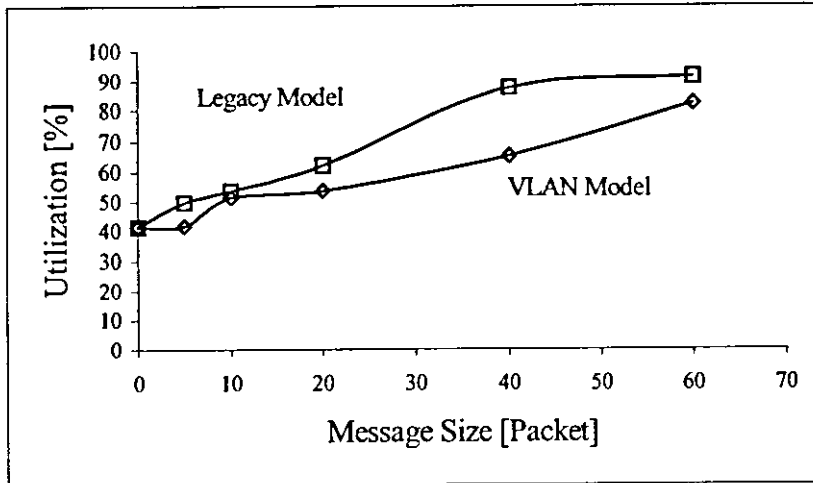


Figure (4.7) The CC Link Utilization in the Main Network in Case of Downloading.

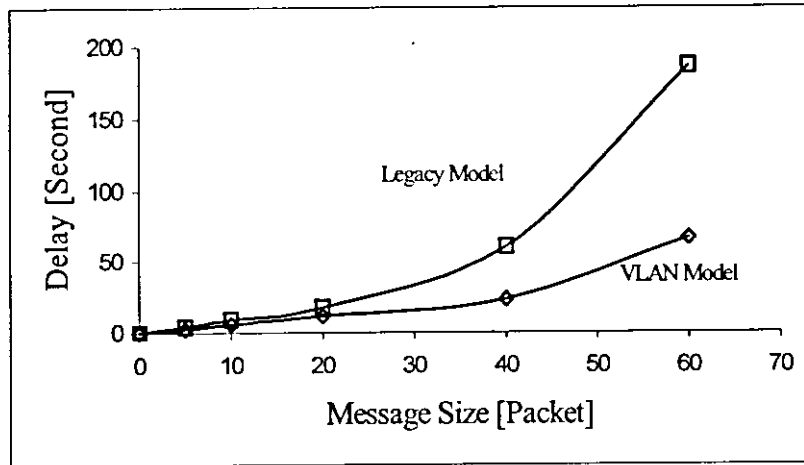


Figure (4.8) Effect on the End-to-End Delay in the Main Network in Case of Downloading.

Figure (4.7) shows that the CC link utilization increases as we increase the size of the downloaded file. The utilization in case of the legacy model increases and reaches a steady state as we increase the message size. The same thing occurs in the VLAN model but with less link utilization values. This is directly related to the number of members in the VLAN broadcast domain.

Figure (4.8) illustrates the effect on the end-to-end message delay which is very important for those who are concerned in downloading. The delay increases as the size of the downloaded file becomes larger. It is easy to notice that there is a difference between the VLAN and the legacy LAN especially for large message sizes, i.e., the VLAN model becomes preferable for downloading large files.

4.2.1.4 One of the Links Becomes Busier Transiently

Making one of the links (e.g., M LAN) busier transiently has its effect on the delay when a communication link needs to be established with one of members in this LAN. This is shown in Figure (4.9). This figure shows that the VLAN model imposes less delay if we compare it with the legacy model. This becomes noticeable as the message size becomes larger.

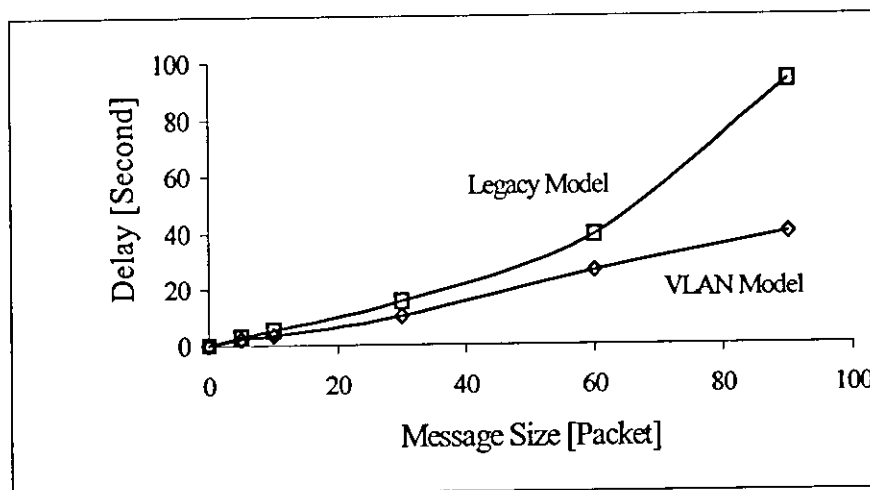


Figure (4.9) Effect on the End-to-End Delay in the Main Network in Case of Downloading.

4.2.1.5 Communication between Two VLANs

The two performance measures are affected by defining more than one VLAN. Two VLANs are defined in this case study. The effect of this case

study is shown in the following points:

4.2.1.5.1 Effect on the CC Link Utilization

The effect on CC link utilization is studied by changing the message size. This is clarified in Figure (4.10). This figure shows that the inter-VLAN traffic raises the utilization of the CC link because of the need to transverse a router to satisfy the inter-VLAN communication. The utilization in case of the legacy model is less than that in the VLAN model.

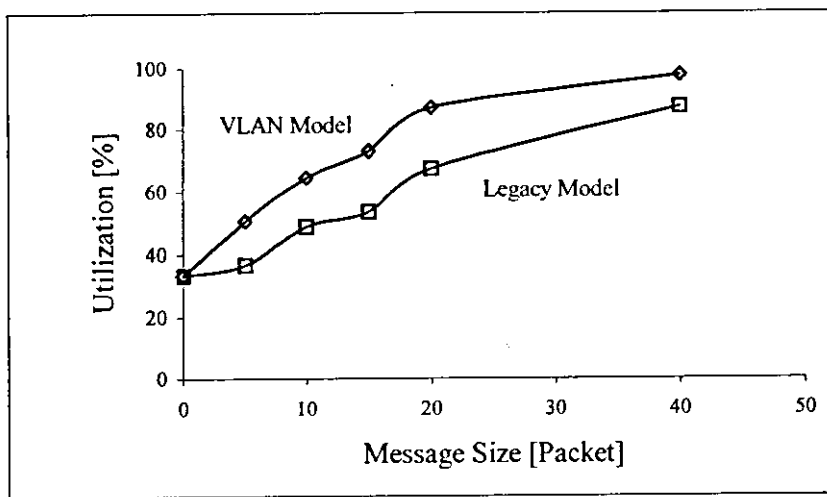


Figure (4.10) The CC Link Utilization in Case of Defining Two VLANs.

4.2.1.5.2 Effect on End-to-End Message Delay

Inter-VLAN communication imposes more delay if compared with the legacy model. This is shown in Figure (4.11). From this figure we can perceive the notable differences in terms of delay between the VLAN model and the legacy model. This is due to the fact that passing routers imposes more time delay.

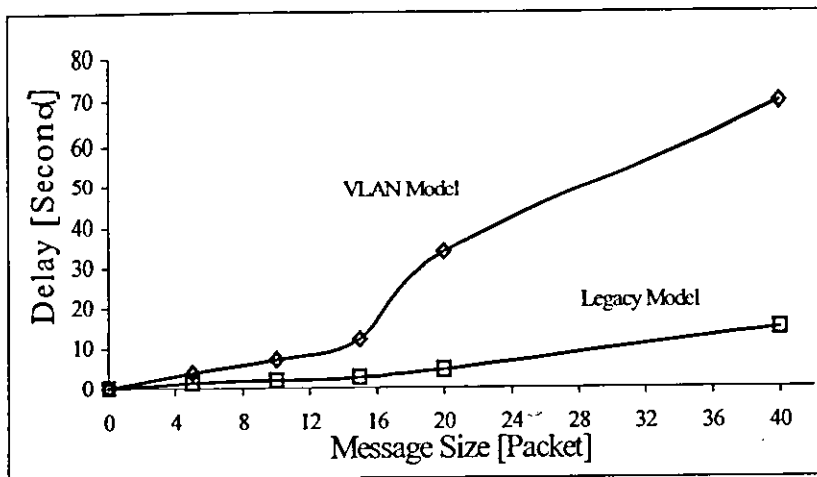


Figure (4.11) Message Delay between Two VLANs.

4.2.2 Results of Simulating the Switched Network

All graphs discussed in this part are related to the simulation results of Figure (3.2).

4.2.2.1 Changing the Message Size

The effect of changing the message size is considered in the following two cases:

4.2.2.1.1 Effect on End-to-End Message Delay

A message from the university president to the CC chairperson is considered. The relation between the delay and the message size in the legacy model and the VLAN model is illustrated in Figure (4.12).

This figure shows that there is an increase in the delay in the two models as we increase the message size. The VLAN imposes less delay on messages if we compare this with the VLAN-unaware model. This stems from the fact that the switches in case of the VLAN model don't need to direct the message to a great number of users.

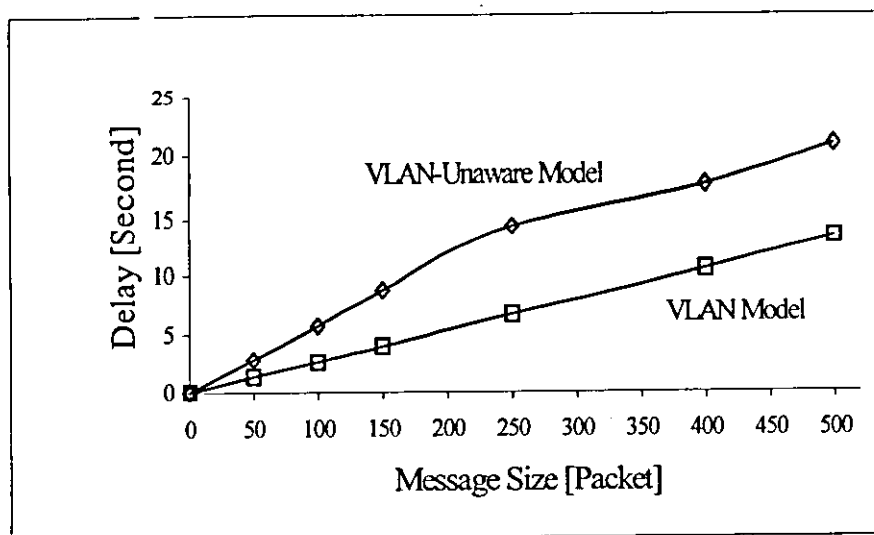


Figure (4.12) Effect on the End-to-End Delay in the Switched Network.

If we compare Figure (4.12) with those figures drawn from Figure (3.1), we can deduce that the switched infrastructure minimizes the end-to-end delay for the same message size.

4.2.2.1.2 Effect on the Test Link Utilization

The utilization of the test link is related to the model that is implemented. The utilization increases as we increase the message size. Also, the utilization in case of implementing the VLAN model is less than that in the VLAN-unaware model. This is depicted in Figure (4.13).

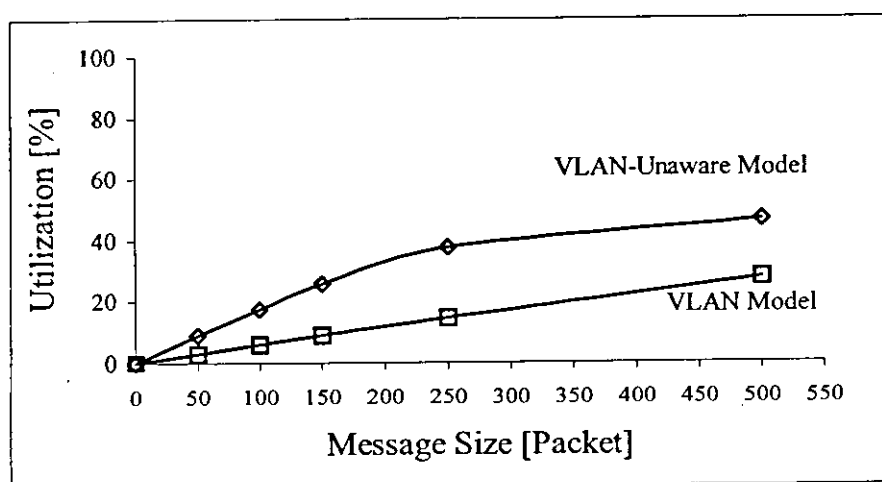


Figure (4.13) Effect on the Test Link Utilization in the Switched Network.

4.2.2.2 Effect on Downloading

The model under scrutiny affects the downloading process. The relationship between the end-to-end message delay and the message size for the VLAN model is shown in Figure (4.14). The delay in the VLAN model is smaller than that in the VLAN-unaware model.

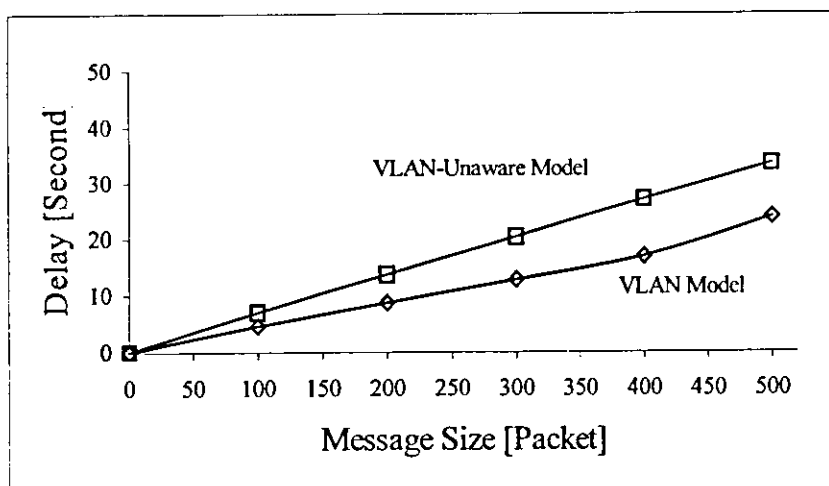


Figure (4.14) Effect on Downloading Delay in the Switched Network.

4.2.3 Results of Simulating the Mixed Network

All graphs discussed in this part are related to the simulation results of Figure (3.3).

4.2.3.1 Changing the Message Size

The effect of changing a chosen message size is clarified in the following two cases:

4.2.3.1.1 Effect on End-to-End Message Delay

The following figure, Figure (4.15), clarifies that the end-to-end delay is inevitably related to the implemented model. VLAN model imposes less delay if compared with the VLAN-unaware model. This is due to the fact that the

number of users after defining a VLAN is less, i.e., the message doesn't need to be broadcast to all nodes in the network.

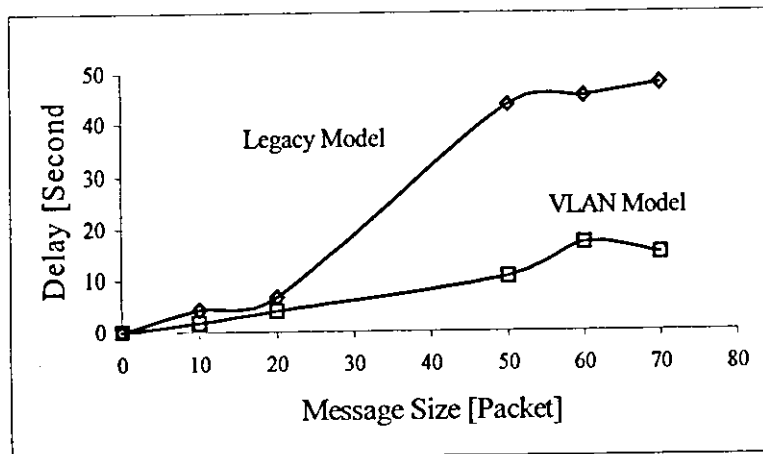


Figure (4.15) Effect on the End-to-End Delay in the Mixed Network.

4.2.3.1.2 Effect on the CC Link Utilization

The utilization of the CC link is presented in Figure (4.16). This figure shows that the VLAN model has a priority over the VLAN-unaware model because it leaves the link more free. On the other hand, in the VLAN-unaware model the CC link utilization is higher and approaches the 100% for high message sizes. This can be explained depending on the fact that the broadcast domain in the VLAN model contains only the required members.

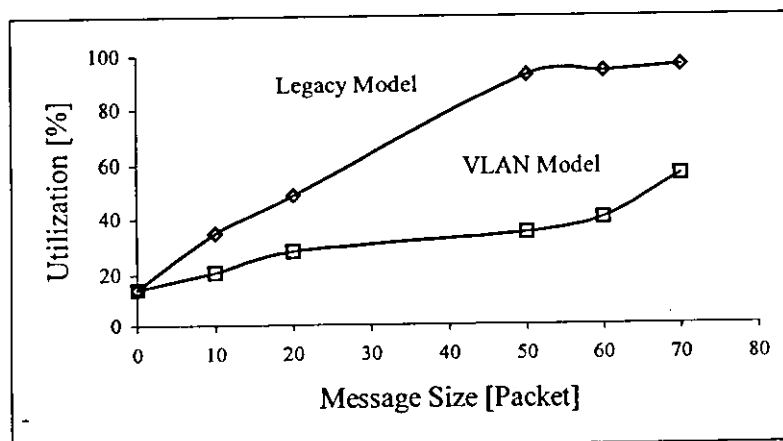


Figure (4.16) Effect on the CC Link Utilization in the Mixed Network.

Chapter 5

Conclusions and Recommendations

The aim of this thesis is to evaluate the performance of VLANs. In order to satisfy this aim, several simulation models are prepared and studied in terms of two performance measures, the end-to-end message delay and the link utilization. This chapter concludes this research. Also, some recommendations for future work are presented.

5.1 Conclusions

This work can be concluded in the following points:

- Before deciding whether to define VLANs or not we must consider the network infrastructure which is of direct influence on the performance of any defined VLAN. The effect of the network infrastructure can be deduced from the simulation results of the proposed simulation models.
- Defining VLANs in a network enhances the overall performance of the network. This is decided depending on the behavior of the selected performance measures. If we consider one of the LAN segments, it is found that the definition of VLANs minimizes the link utilization which means that the LAN segments (e.g., CSMA/CD) become more free if this is compared with legacy models. The contribution of VLANs in minimizing the link utilization is notable when we change the message size. Also, to some extent, VLANs contribute in minimizing the utilization in case of changing the number of users attached to the LAN segments. It is illustrated that when we increase the number of users above certain value, the VLAN

technology isn't able to minimize the utilization below the value offered by the legacy model.

- Generally, it is found that the end-to-end message delay can be reduced if we implement VLANs. It is found that the VLAN model imposes less delay in comparison with the legacy model. This feature is vital in case of multimedia applications. The contribution of VLANs in resolving the delay problem is considerable in networks which are not originally busy.
- The imposed transmission delay by the network links becomes smaller when we define VLANs. It is shown that defining VLANs in busy links is not of great contribution in resolving the problem of the transmission delay via the links.
- The role of VLANs in the downloading process is distinguished if we compare this with legacy LANs. The VLAN technology shows interesting results regarding the two performance measures under scrutiny.
- When one of the links becomes busier for any reason, the VLAN model minimizes the delay time elapsed to convey messages to one of these link members.
- The inter-VLAN communications imposes more delay because of the need to transverse a router. This makes the legacy model preferable over the VLAN model if members from different VLANs but on the same LAN segment need to communicate.
- Since VLAN technology is directly related to the development of the switching technology, we have defined VLANs in a completely switched

infrastructure. It is found that the performance of the VLAN-aware switched networks is better than that in the VLAN-unaware switched networks. This is true for the end-to-end message delay, the link utilization, and the downloading process.

- The same conclusions about VLANs performance are also drawn in case of defining VLANs in mixed network infrastructure. This is due to the fact that the behavior of the selected performance measures in VLAN-aware networks is better than that in VLAN-unaware networks.

To sum up, VLAN technology is a promising technology in the field of networking.

5.2 Recommendations for Future Work

Depending on the fact that the VLAN technology is a new track in the field of networking, there are several points that need to be put under research. Some of these points are summarized in the following points:

- The effect of defining VLANs on the security aspects is of great importance. Therefore, it is recommended to study the performance of VLANs in the field of security. This is due to the notable great role of security in the networking era.
- It is important to study the effect of defining VLANs on the network management aspects. This is due to the fact the definition of VLANs imposes another layer of complexity.
- This thesis is concentrated on the VLANs, but the virtual technology has a role to play in WANs. Therefore, it is important to study the virtual

491719

technology in WANs especially if we consider the great deployment of the Internet.

- Finally, it is also important to study the performance of VLANs when they are required to deal with the new networking technologies such as Gigabit Ethernet.

References

- 3Com Corporation Report. 1996. *3Com Transcend: Leveraging Virtual LAN Technology to Make Networking Easier*. 3Com Corporation.
- Cisco Systems Inc. 1997. *Overview of Routing between Virtual LANs*. Cisco Systems Inc.
- Cisco Systems Inc. 1998. *Virtual LANs*. Cisco Systems Inc., USA.
- Finn, N. and T. Mason. 1996. *ATM LAN Emulation*. IEEE Communications Magazine. 34(6): 96-100, USA.
- Ghane, K. 1995. *Internetworking with ATM-based Switched Virtual Networks*. Neda Communications, Inc.
- Halsall, F. 1996. *Data Communications, Computer Networks and Open Systems*. 4th edition. Addison-Wesley, UK.
- Handel, R., M. Huber, and S. Stefan. 1998. *ATM Networks: Concepts, Protocols, and Applications*. 3rd edition. Addison-Wesley, UK.
- Hein, M. and D. Griffiths. 1997. *Switching Technology in the Local Networks: From LAN to Switched LAN to Virtual LAN*. International Thomson Computer Press, UK.
- Held, G. 1997. *Virtual LANs: Construction, Implementation, and Management*. John Wiley and Sons, USA.
- Higginbottom, G. 1998. *Performance Evaluation of Communication Networks*. Artech House Book, UK.
- IEEE Standard P802.1D/D15. 1997. *Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Common Specifications – Part 3: Media Access Control (MAC) Bridges: Revision*. Institute of Electrical and Electronics Engineers, USA.
- IEEE Standard P802.1Q/D8. 1997. *Draft standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*. Institute of Electrical and Electronics Engineers, USA.
- Intel. 1998. *Virtual LANs: Flexible Network Segmentation for High-Speed LANs*. Intel Corporation, USA.

- Kawaguchi, K. 1996. *VLAN Information and Implementation (Draft ver 1.03)*. UC Davis Information Technology.
- Keiser, G. E. 1989. *Local Area Networks*. Mc-Graw Hill, USA.
- Netreference, Inc. Staff Member. 1995. *The Big Fuss about Virtual LANs*. Business Communications Review, USA.
- Passmore, D. and J. Freeman. 1998. *The Virtual LAN Technology*. 3Com Corporation, USA.
- Ranjan, I. 1996. *Network Switching*. Media India Ltd., India.
- Salamone, S. 1995. *Virtual LANs Get Real*. Core Technologies, USA.
- Seifert, R. 1998. *Gigabit Ethernet*. Addison-Wesley, USA.
- Smith, M. 1998. *Virtual LANs: Construction, Operation and Utilization*. Mc-Graw Hill, USA.
- Smith, S. 1997. *Summarizing Switched and Virtual LANs*. Data-Tech Institute.
- Smythe, C. 1995a. *Internetworking, Designing Right Architectures*. Addison-Wesley, USA.
- Smythe, C. 1995b. *Local Area Network Interoperability*. Electronics and Communication Engineering Journal, 7 (4): 141-153, UK.
- Stamper, D. 1998. *Local Area Networks*. Addison-Wesley, USA.
- Varadarajan, S. 1997. *Virtual Local Area Networks*. Ohio State University, USA.

Appendix

Simulation Models Settings

The three simulation models which are tested in this thesis have the same background traffic which is prepared before preparing the foreground traffic. The foreground traffic is used to study the simulation models.

The background traffic of the tested simulation models is prepared by setting the simulation models nodes. These settings are clarified through the following points:

1. CC Chairperson, Engineering Dean, and Medicine Dean Nodes:

Settings:

Message schedule:	Received message
Received message delay:	Uniform distribution [0,1] Second
Destination type:	Multicast list
Message size unit:	Packet
Message Size:	10 Packets
Priority:	1

2. CC Server Node:

Settings:

Message schedule:	Received message
Received Message Delay:	Uniform distribution [0,1] Second
Destination type:	Multicast list
Message size unit:	Packet

3. CC Secretary, Engineering Secretary, Medicine Secretary, EDHeads, and MDHeads Nodes:

Settings:

Message schedule:	Received message
Received message delay:	Uniform distribution [0,1] Second
Destination type:	Multicast list
Message size unit:	Packet

4. University President Node:

Settings:

Message schedule:	Iteration time
Interarrival time:	Exponential (30.0) Second
Destination type:	Multicast list
Message size unit:	Packet
Message size:	Variable

5. CC Programmers, Engineering Students, and Medicine Students

Nodes:

Settings:

Message schedule:	Iteration time
Interarrival time:	Exp (20.0) Second
Destination type:	Multicast list
Message size unit:	Packet
Message size:	10
Priority:	1

Type: Group node

Number in group: Variable

6. Main Switch:

Settings:

Parameter set name: Default

7. CC Link, Engineering LAN, and Medicine LAN:

Settings:

Type: CSMA/CD

Parameters: 802.3 CSMA/CD 10BaseT

8. Test Link:

Settings:

Type: Point-to-Point

Number of circuits: 1

Bandwidth: 155Mbps

ملخص

تقييم أداء شبكات الحاسب المحلية الافتراضية

إعداد

موسى شفيق عياش

المشرف

د. سهيل عودة

إن التطور الهائل في حقل شبكات الحاسب مرتبط بالتقدم الحاصل في تقنيات الشبكات والتي تحاول وضع حلول مناسبة لتحسين أداء شبكات الحاسب الحالية والمستقبلية. لعل السبب الحقيقي وراء الحاجة لتلك الحلول هو مجاراة حاجة الشبكات الحاسوبية للتعامل مع تطبيقات متعددة تحتاج بشكل واضح للسرعة والعرض الحزمي (Bandwidth). هذا بالإضافة إلى طبيعة العمل اليومية التي تتطلب تقنيات تتعاطى مع متطلبات المرونة في جو العمل.

تعرض هذه الرسالة لتقنية جديدة في عالم الشبكات، والتي تمثل استجابة لبعض المتطلبات المتوقعة من شبكات الحاسب. هذه التقنية تدعى "تقنية شبكات الحاسب المحلية الافتراضية".

تهدف هذه الرسالة إلى تقييم أداء هذا النوع من الشبكات من خلال اقتراح عدد من نماذج المحاكاة، والتي درست بالاعتماد على مقياسين لقياس أداء الشبكات. المقياس الأول متعلق بالزمن

الذي تفرضه الشبكة لإيصال الملفات من نقطة إلى أخرى، أما المقياس الثاني فهو مرتبط بدراسة حالة وسائط تشبيك الحواسيب من حيث كونها مشغولة أو عدمه خلال زمن التشغيل. ولأجل أخذ صورة واضحة عن أداء هذا النوع من الشبكات الافتراضية، لقد تمت مقارنتها مع الأنواع الموجودة أصلا في عالم الشبكات. ولقد تم عرض هذا التقييم في الأداء في رسوم توضيحية تأخذ بنظر الاعتبار حالة مقاييس الأداء المقترحة إذا ما تم تغيير أحد العناصر كأحجام الملفات المنقولة عبر الشبكة وأعداد المستخدمين للشبكة، بالإضافة لذلك لقد تمت دراسة الأداء في حالة وجود أحمال غير متوقعة على أحد أجزاء الشبكة. هذا بالإضافة إلى دراسة أثر تعريف أكثر من شبكة حاسب محلية افتراضية خلال الشبكة الكلية.

لقد وجد أن أداء هذه النوع الجديد من الشبكات وفي معظم الحالات المدروسة هو أفضل بالنسبة لمقاييس الأداء المقترحة. ولقد أظهرت النتائج تميزه في مجال تقليل زمن التأخير والذي له أثر واضح في عالم تطبيقات اليوم.

إن تقنية شبكات الحاسب المحلية الافتراضية هي تقنية واعدة في عالم الشبكات، وخصوصا إذا ما اعتبرنا التقدم المتوقع والواضح في تقنيات التحويل (Switching Technologies).