ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Simulations and Performance Investigations of Database and E-mail Traffic for Hybrid Routing Schemes over Virtual LAN

Vasudha Bahl
Department of Information Technology,
Maharaja Agrasen Institute of Technology,
New Delhi, India
Vasudha.bahl@gmail.com

Abstract: In this paper, performance analysis of the computer networks for combination of conventional model of RIP and OSPF with VLAN is evaluated through simulation which has been attempted using OPNET as simulating tool. In order to participate in optimizing the network performance by minimizing broadcast and collision domains, a proposed network for the Engineering College based on VLAN technique has been developed using the network simulator software (OPNET IT GURU). High throughput with minimum delay is the ultimate demand being required from any network. Traffic congestion is the major problem that deteriorates the performance of a given network. VLAN switches play important roles in further improvements of network performance. Internet traffic effect on the network performance is shown in the paper. It presents the point-to-point delay reduced from 533msec to nearly 494msec. Again the application of VLAN switches shows a better network performance as compared with the existing network. A significant improvement in maximum possible throughput is recognized when using VLAN concept and proposed protocol which shows significant improvement from 1.979packets/sec to 2.0275packets/sec.
The results being obtained represent the optimum possible improvements in terms of queuing delay, throughput and minimizing unnecessary traffic to avoid network congestion.

Keywords: Network Simulation, RIP, OSPF, VLAN and OPNET.

I. INTRODUCTION

A. Introduction:

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

B. What are VLAN's?:

In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network.

The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area shown in Figure1.

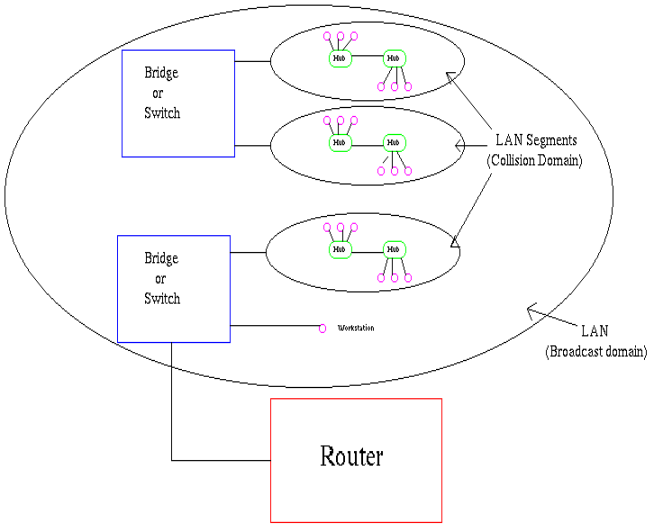
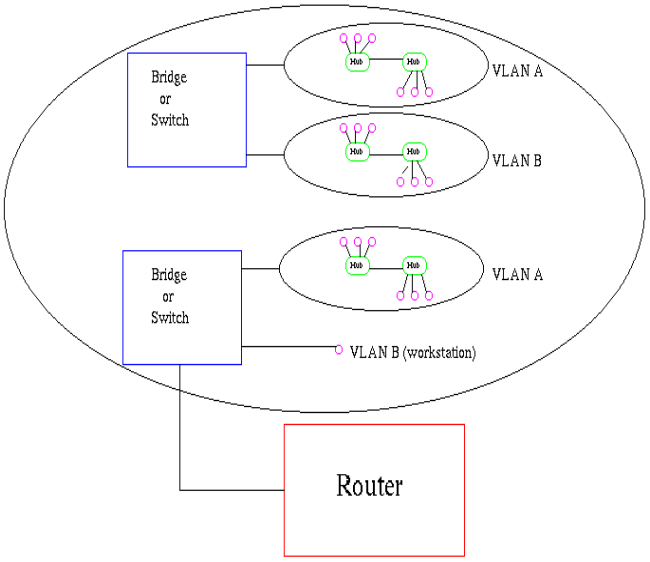


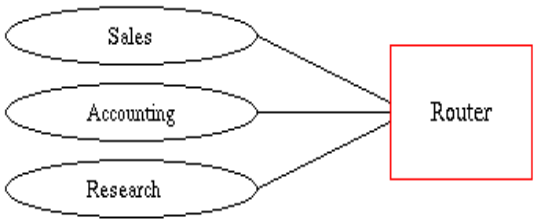
Figure 1: Physical view of a LAN

VLAN's allow a network manager to logically segment a LAN into different broadcast domains shown in Figure2. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together.

Users on different floors of the same building, or even in different buildings can now belong to the same LAN.



Physical View



Logical View

Figure 2: Physical and logical view of a VLAN.

VLAN's also allow broadcast domains to be defined without using routers. Bridging software is used instead to define which workstations are to be included in the broadcast domain. Routers would only have to be used to communicate between two VLAN's [1].

VLAN's offer a number of advantages over traditional LAN's. They are:

a) ***Performance:*** In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic [2].

Compared to switches, routers require more processing of incoming traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance. The use of VLAN's reduces the number of routers needed, since VLAN's create broadcast domains using switches instead of routers.

b) ***Formation of Virtual Workgroups:*** Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them. With VLAN's it is easier to place members of a workgroup together. Without VLAN's, the only way this would be possible is to physically move all the members of the workgroup closer together.

However, virtual workgroups do not come without problems. Consider the situation where one user of the workgroup is on the fourth floor of a building, and the other workgroup members are on the second floor. Resources such as a printer would be located on the second floor, which would be inconvenient for the lone fourth floor user.

Another problem with setting up virtual workgroups is the implementation of centralized server farms, which are essentially collections of servers and major resources for operating a network at a central location. The advantages here are numerous, since it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building. Centralized server farms can cause problems when setting up virtual workgroups if servers cannot be placed on more than one VLAN. In such a case, the server would be placed on a single VLAN and all other VLAN's trying to access the server would have to go through a router; this can reduce performance .

c) ***Simplified Administration:*** Seventy percent of network costs are a result of adds, moves, and changes of users in the network [3]. Every time a user is moved in a LAN, recabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated. However the full power of VLAN's will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLAN's or to set up aliases. Despite this saving, VLAN's add a layer of administrative complexity, since it now becomes necessary to manage virtual workgroups[2].

d) ***Reduced Cost:*** VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

e) ***Security:*** Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion [2].

On the campus network the implementation of the VLAN technology can enhance the network management efficiency, the performance, the band width and the flexibility, meanwhile can control the broadcast storm, enhance the campus net security performance. This article introduces the VLAN technology applied in the network construction. Simulation is becoming an increasingly popular method for network performance analysis. Software simulator is a valuable tool especially for recent networks with complex architectures and topologies. A typical simulator can provide the programmer with the necessary information of how to

control and manage the performance of a computer network. Functions and protocols are described either by finite state machine, native programming code, or a combination of the two [4]. Network simulators have developed since they first appeared as performance, management and prediction tools. They are normally used as network management tools, for which packet level analysis is not commonly employed. The most known network simulator OPNET (OPNET stands for OPtimum NETwork performance) from OPNET Technologies Inc. [5] is superior compared with other network simulation packages in terms of user interface, flexibility, scalability, and accuracy [6,7].

The early types of switches are designed to work at layer two of the Open System Interconnection OSI network model. This means that switches are allowed to investigate the data link layer header, which contains the MAC destination and source addresses, followed by forwarding the packet to the port which is devoted to the MAC destination address. Switches also have lookup tables that map each port to the different MAC address(es) of the users. Building a lookup table is made through a process called transparent bridging [8]. This technology allows the switch to learn every thing about the location of computers on the network without the help of the network administrator having to do any thing. This packet switching technique eliminates collisions and thus more and more computers can be added with the result of one big broadcast domain. Every network, whether controlled by effective network segmentation or by modifying an application's behavior has broadcast traffic which depends on the following [9]:

a. Types of applications.
b. Types of servers.
c. Use of network resources.

Although applications have been restricted to few users, but there are still multimedia applications that are both broadcast- and multicast-intensive. Broadcasts can also occur as a result of faulty network interface cards and communication devices. If incorrectly managed, they can seriously degrade network performance or even bring down an entire network. So the need of re-segmenting the big flat network is necessary. This can be done by applying virtual local area networks (VLANs) technique. It is a group of devices that function as a single Local Area Network segment (broadcast domain). The devices that make up a particular VLAN may be widely separated. The creation of VLANs allows users located in separate areas or connected to separate ports to belong to a single VLAN group. Users that are assigned to such a group will send and receive broadcast and multicast traffic as though they were all connected to a single network segment [10]. VLAN aware switches isolate broadcast and multicast traffic received from VLAN groups, keeping broadcasts from stations in a VLAN confined to that VLAN only. When stations are assigned to a VLAN, the performance of their network connection is not changed. Stations connected to switch ports do not affect the performance of the dedicated switched link due to participation in the VLAN. Finally VLANs have the following advantages: flexible network segmentation, simple management, increased performance and better use of same resources [11].

II. NETWORK CONFIGURATION

A. Inter-VLAN communication:

Different VLANs can communicate with each other via a router, because the VLAN information is not carried when going through IP. If a router is connected to a VLAN- aware bridged-network via an access port with PVID 1 (Default VLAN), then packets arriving from this router will be associated with VLAN 1. Hence, they will be forwarded to any port in the bridged-network along their path to their destinations as long as these ports are also a member of VLAN.

"Building1" can get emails from the email server in "Building2" even though the email server doesn't belong to the same VLAN as the client in "Building1", since the connection is established via a router and the ports of these clients support the PVID of the access port to the router.

However, packets coming from the router in "Building2" are given the VLAN membership 10. It means that clients and servers with VLAN membership 30 in "Building2" can never communicate with stations outside the "Building2" and vice-versa. For instance, the request of FTP client in "Building2" are dropped by "Switch2" since the FTP server resides in "Building1".

In "Building2", stations with VLAN membership 10 will never be able to connect to the server "Confidential Database", because the server belongs to the VLAN 30. That's why "Switch3" is dropping many packets.

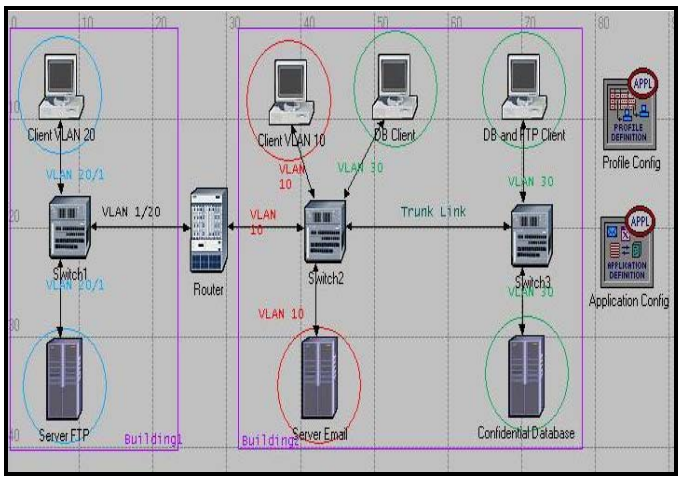


Figure 3: Network Model

III. RESULTS AND DISCUSSION

Figure 4 and 5 shows the simulation result of the E-Mail Download Response Time (Sec) and E-Mail Upload Response Time (Sec) traffic forwarded for all the scenarios being applied. It is obvious that the results being obtained represent the instantaneous variation of the statistic as a function of the simulation (actual) time. The E-Mail Download Response Time for network has been reduced from 97msec to 93mSec with the proposed protocol in Virtual LAN. The figure reveals the fact that the performance with VLAN improves the results as compared with the case of the existing network.

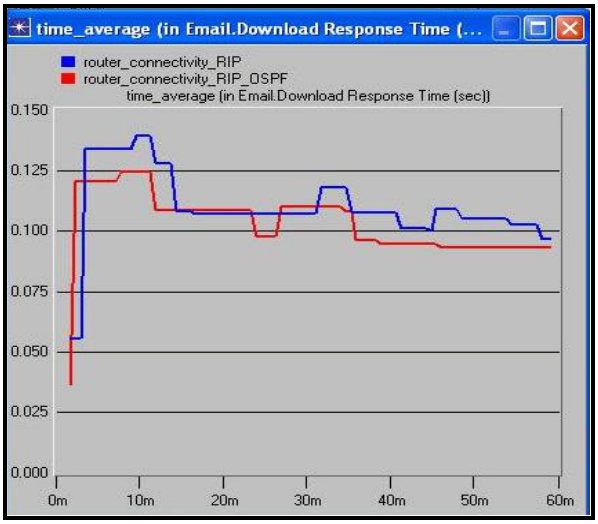


Figure 4: E-Mail Download Response Time (Sec)

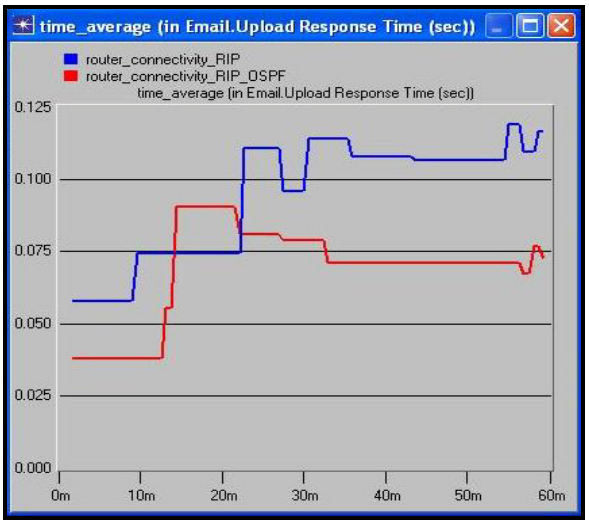


Figure 5: E-Mail Upload Response Time (Sec)

Figure 6 and 7 shows the relationship between the traffic forwarded and the offered load. The Database traffic sent and received in bytes/sec is represented in the figures 4 and 5 respectively which shows same performance with both the protocols with VLAN. Figure 8 presents the database traffic response time in Sec which shows significant improvement from 162msec to 168msec with the new proposed protocol.

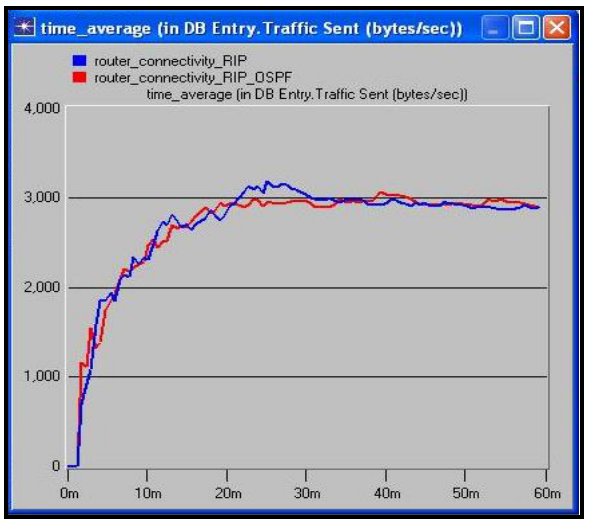


Figure 6: DB Entry Traffic Sent (bytes/sec)

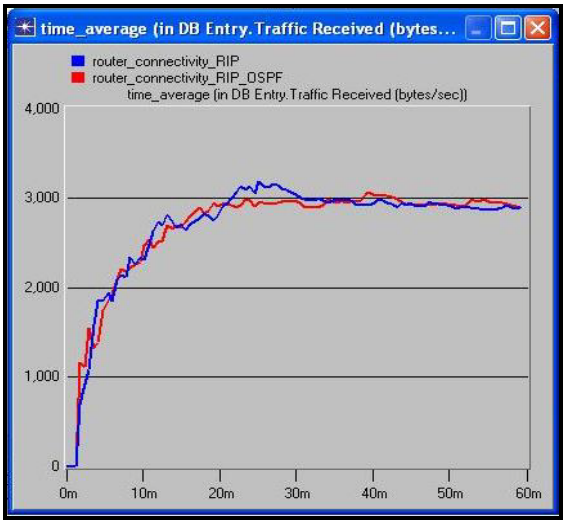


Figure 7: DB Entry Traffic Received (Bytes/sec)

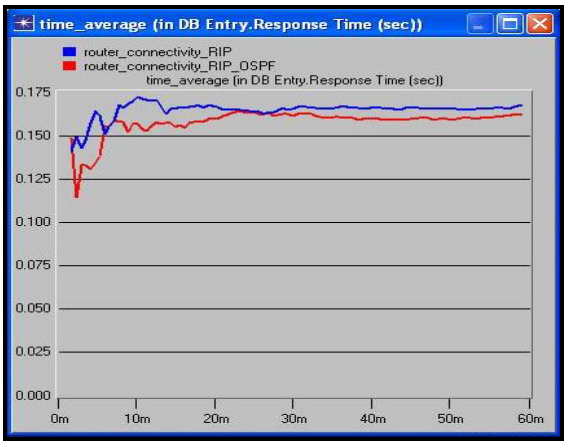


Figure 8: DB Entry Response Time (Sec)

Packets dropped is an important factor in determining the performance of any Network. Figure 9 shows the relationship between packet dropped and offered load for the existing and proposed networks. The use of VLAN technique and proposed protocol reduced packets dropped from 57 µSec to nearly 53 µSec for the cases of high offered loads.

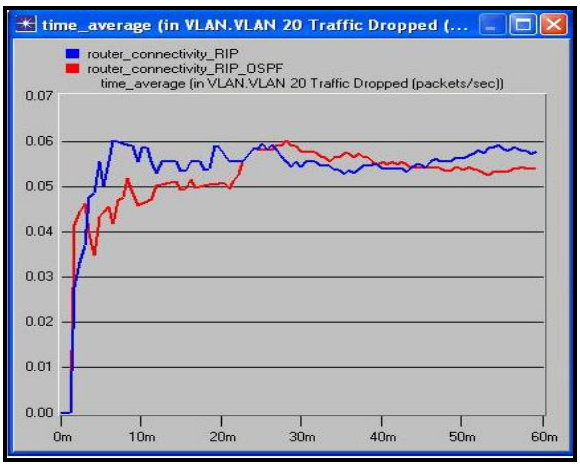


Figure 9: VLAN Traffic Dropped (packets/sec)

Another important factor related to the performance of networks is throughput. This criterion measures the information rate of a channel in a network. Figure 10 shows VLAN Point-to-Point Throughput (packets/sec), the relationship between throughput and offered load. A big

improvement in maximum possible throughput is recognized when using VLAN concept and proposed protocol which shows significant improvement from 1.979packets/sec to 2.0275packets/sec.

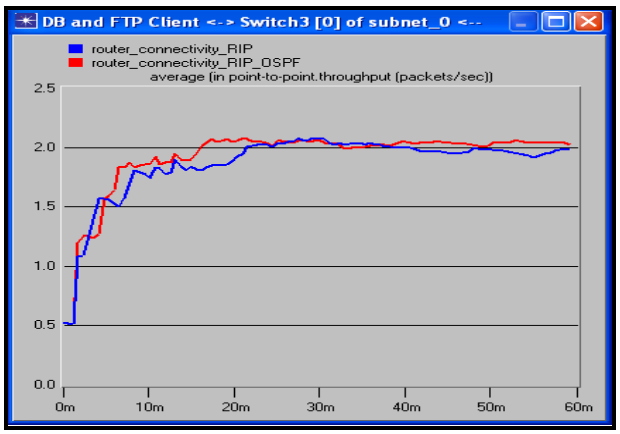


Figure 10: VLAN Point-to-Point Throughput (packets/sec)

Finally, the Internet traffic effect on the network performance is shown in figure 11. It presents the point-to-point queuing delay reduced from 533msec to nearly 494msec. Again the application of VLAN switches shows a better network performance as compared with the existing network.

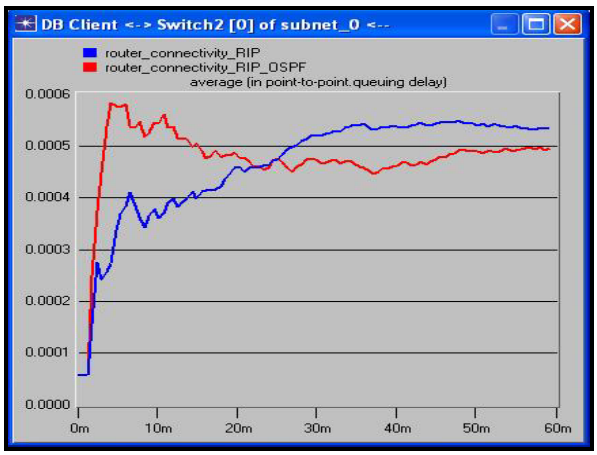


Figure 11: Point-to-Point Queuing Delay

IV. CONCLUSIONS

The results obtained in this paper show that the application of VLAN concept with the proposed protocols which helps in decreasing unnecessary traffic, queuing delay, and increasing network throughput. This is due to segregating the single large broadcast domain that exists now into multiple limited broadcast domains for each VLAN. A delay performance improves from 533msec to 494msec with the use of VLAN technique and proposed protocol and the throughput has shown significant improvement for large offered load. On the other hand, simulation study shows that Internet traffic response time has been decreased to approximately half that of the existing LAN.

V. REFERENCES

[1] Mathias Hein, David Griffiths, Orna Berry, ``Switching Technology in the Local Network: From LAN to Switched LAN to VirtualLAN,"February1997.

[2] David Passmore, John Freeman, ``The Virtual LAN Technology Report," March 7, 1997, http://www.3com.com/nsc/200374.html

[3] David J. Buerger, ``Virtual LAN cost savings will stay virtual until networking's next era," Network World, March 1995.

[4] Xinjie Chang, "Network Simulations with OPNET", Proceedings of the 1999 Winter Simulation Conference, P. A. Farrington, H. B. Nembhard, D. T. Sturrock, and G. W. Evans, eds.PP 307-314.

[5] WWW.OPNET.COM

[6] G. F. Lucio, M. P. Farrera, E. Jammeh, M. Fleury, and M. J. Reed, “OPNET Modeler and Ns-2: Comparing the Accuracy Of Network Simulators for Packet-Level Analysis using a Network Testbed”, http://privatewww.essex.ac.uk/~fleum/weas.pdf

[7] C. Burns, and K. Shaw, "Network Management", Network World, 28/2/2005,http://www.nwfusion.com/best/2005/022805tests3.

[8] H. Osterloh, ”Switching and Routing”, Que a division of Macmillan, Indianapolis, Indiana, USA, 2000.

[9] Cisco Systems,”Broadcast Storms”, http://www.cisco.com/warp/public/96/9.html.

[10] J. Martillo, "Routing in a Bridged Network", Telfoird Tool inc, white paper, 1997.

[11] D. Passmore, and j. Freeman, "The Virtual LAN Technology Report", 3 COM Whitepaper, 1996.