Asian Journal of Information Technology 6 (10): 1003-1009, 2007
ISSN: 1682-3915

Analysis on the Virtual Local Area Network to Reduce Collision Domain and Manage Broadcast Domain

Mohammad Rohul Amin
Department of Computer Science and Engineering,
Daffodil International University, Dhaka, Bangladesh

Abstract: This is the age of communication technology. Effectively data communication is a big aspect for the business development. The concept of Virtual Local Area Network (VLAN) technology holds the potential for harmonizing many of today's organizational and managerial changes with the structural and technological developments in the network. Despite the promise of this vision, VLAN implementation must solve the real-world problems in order to be financially justified. Organizations those have deployed or are planning to deploy the large numbers of switch ports, dividing the network into the smaller segments to increase the bandwidth per user, can make a very strong case for the VLAN implementation in order to contain the broadcast. This study tries to present an effective solution which will increase the performance of a Local Area Network (LAN). In the real-world, there is a lot of transmission impairments are occurred which hampering the data transmission processes. Collision domain is one of the major problems which decrease the performance of a network. The proposed network tries to reduce the collision domain using the VLAN and also implements the Spanning Tree Protocol (STP) which manages the broadcast storms. For an efficient data transmission purpose, the network administrator needs an effective solution which is scalable and easy to mange depends on the network architecture.

Key words: Virtual Local Area Network (VLAN), Collision Domain, Spanning Tree Protocol (STP), broadcast domain, switches, bridges and routers

INTRODUCTION

As the Internet becomes ever more pervasive, computer network environments day by day increase for effective data transmission. Many protocols and technologies are developed for reliable data communication (ANIXTER, 2007; CISCO, 2007; IBM, 2007). There is an emerging consensus among the researchers that an implementation of a new architecture and dynamic infrastructure is an appropriate way to address the problems and produce an idea for which technology is efficient for data communication (Minli *et al.,* 2004; Shinichi *et al*., 2005; Tarek *et al*., 2005; Tomohiro *et al*., 2006). This research provides a descriptive and mathematical analysis of the VLAN attributes such as collision domain, packets upload and download, packets passing rate and authentication.

Network administrator must anticipate and manage the physical growth of networks. Network designers must choose the address schemes allow for growths. When a network is scalable, it is able to grow in a logical, efficient and cost-effective way (NI, 2007). An important feature of Ethernet switching is the ability to create VLANs (Fig. 1). Switches and bridges forward unicast, multicast and broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs. Routers provide the connectivity between different VLANs. VLANs increase the overall network performance by logically grouping users and resources together. Businesses often use the VLANs as a way of ensuring that a particular set of users are logically grouped regardless of the physical location. VLANs can enhance scalability, security and network management. Routers in the VLAN topologies provide broadcast filtering, security and traffic flow management (Vanessa, 2005). Properly designed and configured VLANs are powerful tools for the network administrator. VLANs improve the network security and help the control Layer 3 broadcasts (David, 1995; Passmore and John, 1997).

EXISTING NETWORK

At present the existing network (Fig. 2) has large number of collision domain which decreases the performance of the network. Also redundancy of the existing network is not quite efficient. The existing

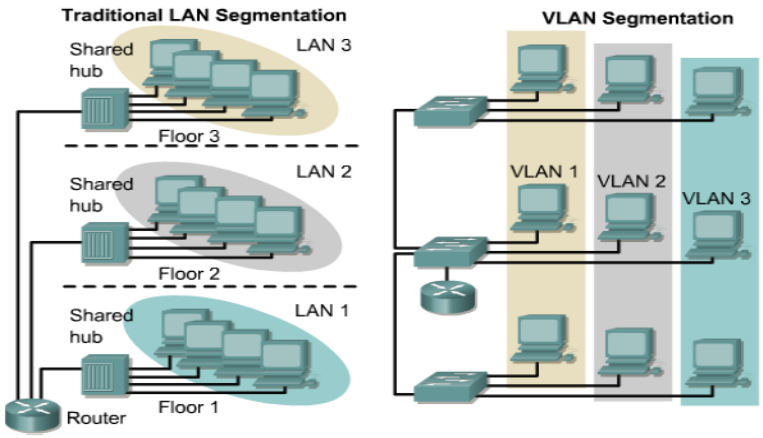

Fig. 1: VLANs and physical boundaries

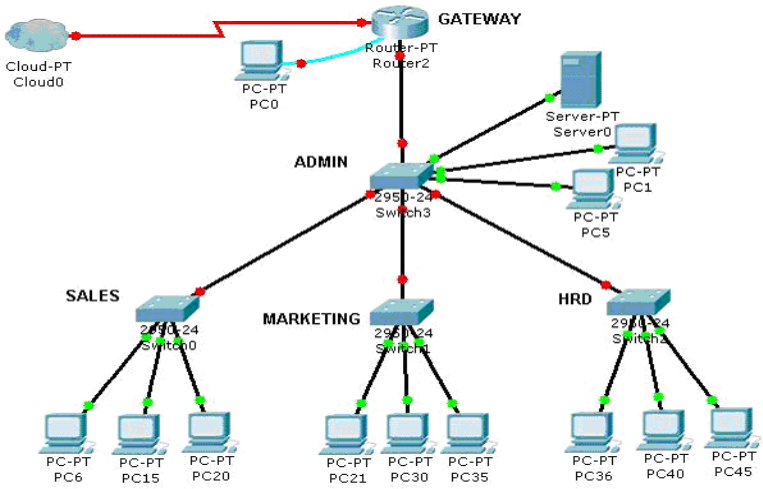

Fig. 2: Existing network

Table 1: Existing network information

Network (Department)	Need workstation	Sub-network address
Admin	5	172.168.1.32
Sales	15	172.168.1.64
HRD	10	172.168.1.96
Marketing	15	172.168.1.128

network performances depend on some of the issues which perform explicitly and implicitly.

Collision domain issues: Based on the existing network's workstations (IP address 172.168.1.1), the Admin network has 5 collision domains, same as the Sales network has 15 collision domain, the HRD network has 10 collision domains and the Marketing network has 15 collision domains (Table 1) (CISCO, 2007).

Broadcast domain issues: Network administrator can not control the broadcast. The sales department workstation wants to send a message to the HRD department then the Sales department switch broadcast the message. After receiving the broadcast, the Admin department switch again broadcast the message to the whole network. This broadcast will continue until the appropriate destination is found (CISCO, 2007).

Segmentation issues: Five segments are found. The Segmentation issues are related with the manageability of network (CISCO, 2007; NI, 2007). If a Marketing network workstation wants to add the Sales network then it physically moves to the Sales network which is very costly to manage in a large enterprise network.

Bandwidth problem in LANs: LANs in many organizations have to deal with the increased bandwidth demands (ANIXTER, 2007). More and more users are

being added to the existing LANs. If this was the only problem, it could be solved by upgrading the backbone that connects various LANs. The routers and switches can be used to keep the optimal number of users per LAN. However, with the increase in speed of workstation the bandwidth requirement of each machine has grown more than five times from the last few years. Coupled with the bandwidth hungry multimedia applications and unmanaged bursty traffic, this problem is further aggravated. With the increasing use of client-server architecture in which most of the software is stored in the server, the traffic from workstations to the server has increased. Further, the use of a large number of GUI applications means more pictures and graphics files need to be transferred to the workstations. This is another cause of increased traffic per workstation.

Flow control problem: Flow control is necessary when the destination port is receiving more traffic than it can handle. Since the buffers are only meant for absorbing peaks traffic, with excessive load frames may be dropped (NI, 2007). It is a costly operation as delay is of the order of seconds for each dropped frame. Traditional networks do not have a layer 2 flow control mechanism and rely mainly on higher layers. The Switches come with various flow control strategies. Some switches upon finding that the destination port is overloaded will send the jam message to the sender. Since the decoding of Media Access Control (MAC) address is fast and a switch can respond with a jam message in very little time, the collision or packet loss can be avoided. The jam packet is like a virtual collision to the sender, so it will wait a random time before retransmitting. This strategy works as only those frames that go to the overloaded destination ports are jammed and not the others.

Possible solutions: The conventional approach would be to install a faster network technology, replacing Ethernet with Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI) and Fast Ethernet with VLAN. Although these are great technologies, such a move is expensive, needs new equipment, the staff training and the network downtime also takes its toll. Another approach would be to segment the network into the smaller parts using the switches and routers (IBM, 2007). This too is expensive, although not as much as complete migration to the new networking technology and would only work if the traffic between segments is low. Otherwise, the switches and routers would act as the network bottlenecks and the frame loss may occur. The LAN switching is considered to be a solution to this problem and has been adopted by the many organizations. Besides making more bandwidth available, it can also form an intermediate step in moving to faster networks such as VLAN.

PROPOSED NETWORK

VLANs facilitate easy administration of the logical groups of stations and servers that can communicate as if they were on the same physical LAN segment. They also facilitate easier administration of moves, adds and changes in members of these groups. The VLANs logically segment switched networks based on job functions, departments or project teams, regardless of physical location of the users or physical connections to the network. The VLANs are created to provide the segmentation services traditionally provided by the physical routers in the LAN configurations. The proposed network (Fig. 3) is designed with some of the issues like collision domain and broadcast domain.

STP is used in the switched networks to create a loop free logical topology from a physical topology that has loops. The Links, ports and switches that are not part of the active loop free topology do not forward the data frames. The STP is a powerful tool for the network administrators gives the security of a redundant topology without the risk of problems caused by the switching loops (STP, 2007).

Collision domain issues: Proposed network has four VLAN and hence four collision domains exist according to the collision domain definition (Table 2).

Broadcast domain issues: Switches normally do not filter the LAN broadcast traffic. In general, they replicate it on all the ports. This not only can cause that large switched LAN environments to become flooded with the broadcasts, it is also wasteful of the precious Wide Area Network (WAN) bandwidth. As a result, the users have traditionally been forced to partition their networks with the routers that act as the broadcast "firewalls." One of the primary benefits of the VLANs is that LAN switches supporting VLANs can be used to effectively control the broadcast traffic, reducing the need for routing. The broadcast traffic from servers and end-stations in a particular VLAN 10 is replicated only on those switch ports connected to the end-stations belonging to that VLAN. The broadcast traffic is blocked from the ports with no end-stations belonging to that VLAN, in effect creating the same type of broadcast firewall that a router provides. Only the packets that are destined for addresses outside the VLAN need to proceed to a router for forwarding.

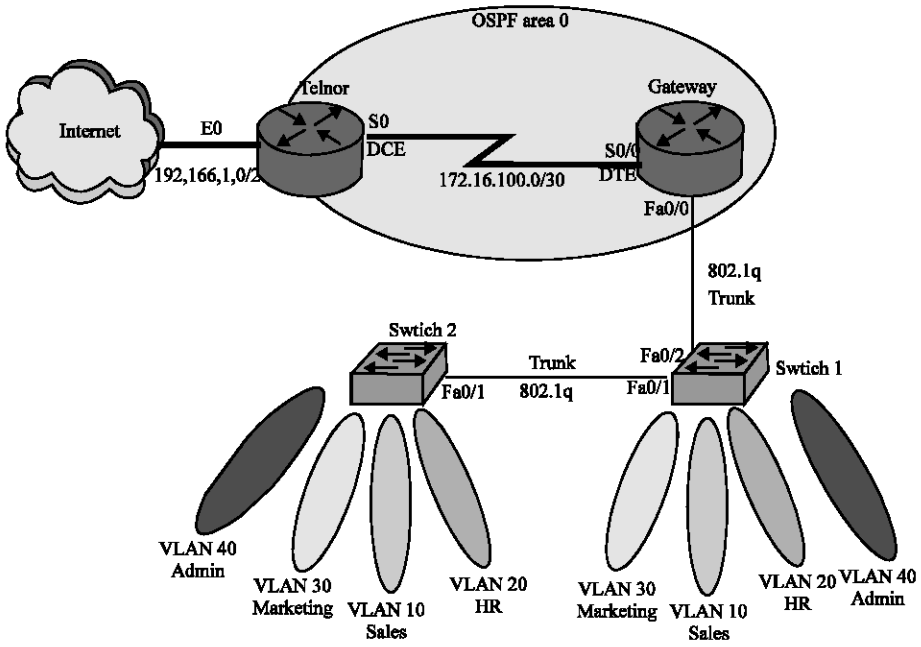

Fig. 3: Proposed network

Table 2: Inter-VLAN information

	VLAN 10	VLAN 20	VLAN 30	VLAN 40	VLAN 1	Trunk
Switch 1	Fa0/3-Fa0/7	Fa0/8-Fa0/11	Fa0/12-Fa0/21	Fa0/22-Fa0/24	All remaining port	Fa0/1, Fa0/2
Switch 2	Fa0/2-Fa0/11	Fa0/2-Fa0/17	Fa0/18-Fa0/22	Fa0/23-Fa0/24	All remaining port	Fa0/1

Segmentation issues: The reason for segmentation most often given for VLAN implementation is a reduction in the cost of handling the user moves and changes. Since these costs are quite substantial, this argument for VLAN implementation can be compelling. Normally, when a user moves to a different subnet, the IP addresses must be manually updated in the workstation. This updating process can consume a substantial amount of time that could be used for more productive endeavors such as developing the new network services.

VLANs eliminate that hassle, because the VLAN membership is not tied to a workstation's location in the network, allowing moved workstations to retain their original IP addresses and subnet membership. However, not just any VLAN implementation will reduce these costs. The VLANs themselves add another layer of virtual connectivity that must be managed in conjunction with the physical connectivity. This is not to say that VLANs cannot reduce the costs of moves and changes if properly implemented, they will. However, the organizations must be careful not to simply throw the VLANs at the network and they must make sure that the solution does not generate more network administration than it saves.

Maintaining the 80/20 rule: VLAN support for the virtual workgroups is often tied to support of the "80/20 rule", that is, the 80% of the traffic is "local" to the workgroup while the 20% is remote or outside of the workgroup. Properly configuring the VLANs to match workgroups, only the 20% of the traffic that is non local will need to pass through a router and out of the workgroup, improving performance for the 80% of the traffic that is within the workgroup (Passmore and John, 1997).

Higher performance and reduced latency: As the network expands, more and more switches are required to divide the network into the broadcast domains. As the number of switches increase, the latency begins to degrade the network performance. A high degree of latency in the network is a problem now for many legacy applications, but it is particularly troublesome for newer applications that feature the delay-sensitive multimedia and the interactivity. The Switches that employ the VLANs can accomplish the same division of the network into the broadcast domains, but can do so at latencies much lower than those of routers. In addition, the performance, measured in packets per second. However, it should be noted that there are some switches supporting the network layer-defined VLANs that may not perform substantially faster than the routers. Additionally, the latency is also highly correlated to the number of hops a packet must traverse, no matter what internetworking device (switch or router) is located at each hop.

Easy of administration: Routers require much more complex configuration than the switches. They are "administratively rich". Reducing the number of routers in the network saves time spent on the network management.

Security: The ability of VLANs to create the firewalls (Access Control List) can also satisfy more stringent security requirements and thus replace much of the functionality of routers in this area. This is primarily true when the VLANs are implemented in conjunction with the private port switching. The only broadcast traffic on a single-user segment would be from that user's VLAN (that is, traffic intended for that user). Conversely, it would be impossible to "listen" to broadcast or unicast traffic not intended for that user (even by putting the workstation's network adapter in promiscuous mode), because such traffic does not physically traverse that segment (Vanessa, 2005).

Cost: Router ports are more expensive than the switch ports. Also, by utilizing the cheaper switch ports, switching and VLANs allow the networks to be segmented at a lower cost than would be the case if the routers alone were used for the segmentation. In comparing VLANs with routing, the VLANs have their disadvantages as well. The most significant weakness is that VLANs have been, to date, single-vendor solutions and therefore may lead to switch vendor lock-in. The primary benefits of the VLANs over routing are the creation of broadcast domains without the disadvantages of routing and a reduction in the cost of moves and changes in the network.

RESULTS AND DISCUSSION

In order to evaluate the performance of VLANs, first step to configure the VLAN by the simulation software. The network information tables are designed to have three attributes named collision domain, packets upload and download and packet passing rate.

In this study, the system which is used for the server is Intel(R) Pentium III, CPU 1.8 MHz processor, 256MB RAM, Windows XP Professional operating system with Advanced Service Pak2, RouterOSwinbox, Net Visualization version 5, 32 Kbps shared media.

Simulation software experiment result: After complete all the experiment the result of the simulation software is being calculated. Table 3-7 and Fig. 4-8 contain five tests where data has been taken from five different situation of the network.

Table 3: Collision domain

No. of network	No. of workstation	No. of collision domain
10	50	50
	100	100
	150	150
	200	200
	250	250

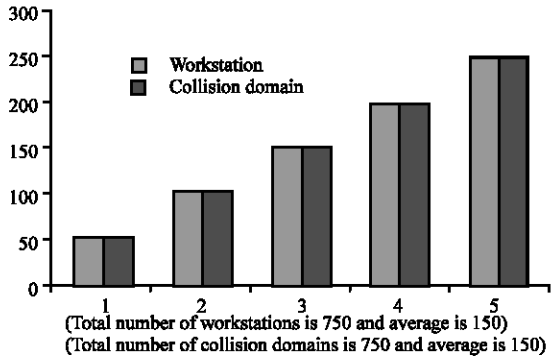

Fig. 4: Collision domain is dependent on workstation

Table 4: Collision domain

No. of VLANs domain	No. of workstation	No. of collision
10	50	10
	100	
	150	
	200	
	250	

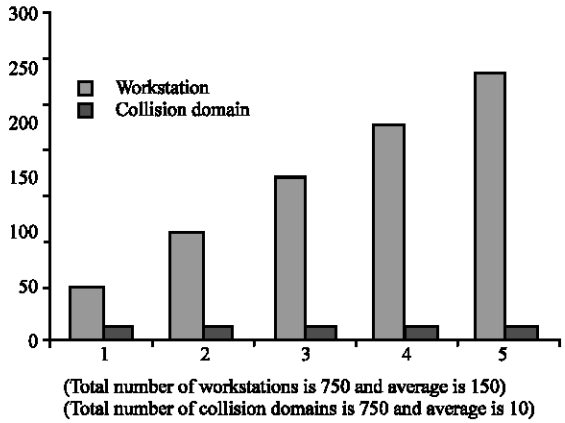

Fig. 5: Collision domain is dependent on VLAN

Technical error analysis: Average packets passing (Experimental 5: Table 7 and Fig. 8) in existing network is 495.6 and in proposed network is 723.8.

This graph (Fig. 9) represents the percentages of proposed network packet passing is 59% which is little far from the theoretical result. Transmission impairment is the main issue for this value. On the other hand, these values are calculated in a few moments because packets are

Table 5: Packets upload and download

Bandwidth (Shared)	Packets upload	Packets download
32kbps	17134	16724
	18457	17967
	21038	20901
	22432	21674
	23156	22473

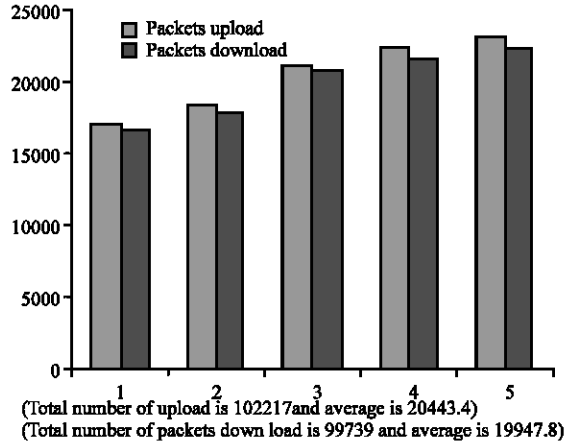

Fig. 6: Packets upload and download

Table 6: Packets upload and download

Bandwidth (Shared)	Packets upload	Packets download
32kbps	18614	17952
	21873	20974
	22356	21942
	24057	23187
	26741	25967

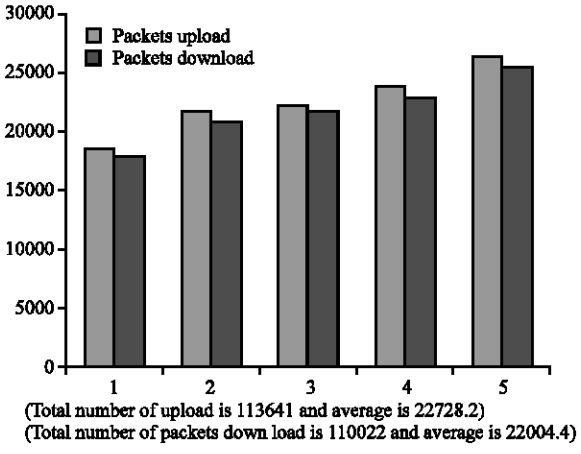

Fig. 7: Packets upload and download

passing so quickly. This error is not counted for research work because the rate of error very little. So, this can be avoided:

- VLANs create logical broadcast domains and these cause the broadcast storms problems in a switched network. But this work reduces this problem by implementing the spanning tree protocol. The broadcast traffic is blocked from ports with no end-stations belonging to that VLAN, in effect creating the same type of broadcast firewall (ACL) that a router provides. Only packets that are destined for the addresses outside the VLAN need to proceed to a router for forwarding.
- The virtual workgroup concept may run into the simple problem that users must sometimes be physically closed to the certain resources such as printers. A user is in the Marketing VLAN, but is physically located in an area populated by the members of the Sales VLAN. The local network printer is also in the Sales VLAN. Every time this Marketing VLAN member prints to the local printer, the print file must traverse a router connecting the two VLANs. This problem can be avoided by making that printer a member of both VLANs. Then, the print

Table 7: Packets passing

Test No.	Existing network	Proposed network
Test 1	410	662
Test 2	490	899
Test 3	137	414
Test 4	758	870
Test 5	683	774

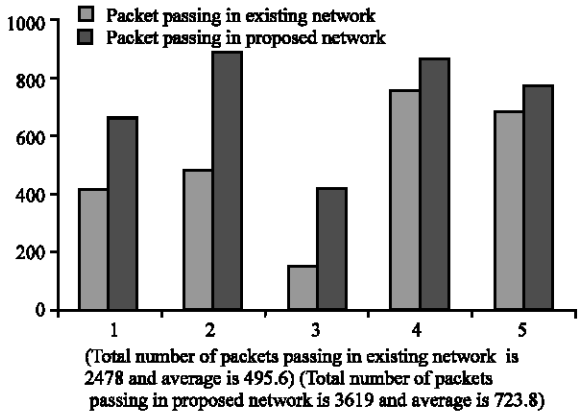

Fig. 8: Proposed network performs better than existing network

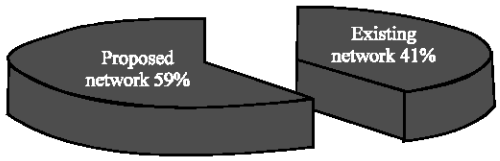

Fig. 9: Percentages of packet passing in existing network and in proposed network

file would be routed by the switch rather than having to go through an external router.

- VLANs support IEEE 802.1Q tagging, which allows the virtual Ethernet adapters to belong different VLANs on the switch. If a (user IP interface) try to configure a VLAN ID value that is already in used for the specified adapter, the configuration fails with the following errors:

Method Error (/usr/lib/methods/chgvlan): 0514-018 The values specified for the following attributes are not valid: vlan_tag_id VLAN Tag ID.

If a user (IP interface) is currently using the VLAN logical device, any attempt to change the VLAN characteristic (VLAN tag ID or base adapter) fails. A message similar to the following displays.

Method error (/usr/lib/methods/chgvlan): 0514-062 cannot perform the requested function because the specified device is busy (NI-Network Instrumants-Observer, 2007).

CONCLUSION

This study tries to analyze the performance by simulation software depending on the collision domain, packets upload and download and packets passing rate. The values of existing network are taken from the real share bandwidth network and the values of proposed network are taken from the simulation software using the share bandwidth network. RouterOSwinbox software is used to measure the performance of VLANs implementation network. As we have seen, there are significant advances in the field of networks in the form of VLANs, which allow the formation of virtual workgroups, better security, improved performance, simplified administration and reduced costs. The VLANs are formed by the logical segmentation of a network and can be classified into Layer1, 2, 3 and higher layers. Only Layer 1 and 2 are specified in the draft standard 802.1Q. The Tagging and the filtering database allow a switch to determine the source and the destination VLAN for received data. If the VLANs are implemented effectively, the performance will be better than existing network. Also this will scalable for the future growth.

During the measurement of data from the real network and the simulation network, sometime problem occurs in taking data. But this research tries to remove this transmission impairment. So, more study is required to provide the more accurate investigation which will increase the performance of VLANs.

REFERENCES

ANIXTER-Products and Technology Overview, 2007. http://www.anixter.com/AXECOM/US.NSF/ProductsTechnology/Overview.

CISCO Systems-Solutions, 2007. http://www.cisco.com/en/US/netsol/index.html.

David J. Buerger, 1995. Virtual LAN Cost Savings will Stay Virtual until Networking's Next Era, Network World.

IBM Networking, 2007. http://www.networking.ibm.com/index.html.

Zhu, M., M. Molle and B. Brahmam, 2004. Design and Implementation of Application-Based Secure VLAN, 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), pp: 407-408.

NI-Network Instruments-Observer, 2007. http://www.networkinstruments.com/products/observer/index.html.

David, P. and J. Freeman, 1997, The Virtual LAN Technology Report, decisys, http://www.3com.com/nsc/200374.html.

Miura, S., T. Boku, M. Sato, D. Takahashi and T. Okamoto, 2005, Low-cost High-bandwidth Tree Network for PC Clusters based on Tagged-VLAN Technology, 8th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'05), pp: 84-93.

STP Root Guard Enhancement-CISCO, 2007. http://www.cisco.com/warp/public/473/74.html.

Otsuka, T., M. Koibuchi, T. Kudoh and H. Amano, 2006, Switch-Tagged VLAN Routing Methodology for PC Clusters with Ethernet, Int. Conf. Parallel Processing (ICPP'06), pp: 479-486.

Alawieh T.S.B. and H.T. Mouftah, 2005. Inter-VLAN VPNs over a High Performance Optical Testbed, First International Conference on Testbeds and Research Infrastructures for the Development of Networks and COMmunities (TRIDENTCOM'05), pp: 221-229.

Vanessa Antoine, 2005. Router Security Configuration Guide, Version 1.1c, http://www.nsa.gov/snac/routers/C4-040R-02.pdf.