Spring 2-1-2002

Implementation of Virtual Local Area Network

Yuheng Zhao
Dakota State University

Implementation of Virtual Local Area Networks

By: Yuheng Zhao

A Project submitted in partial fulfillment of the

requirements for the Master of Science in Information Systems

Dakota State University

2002

MSIS

PROJECT APPROVAL FORM

Student Name: Yuheng Zhao

Expected Graduation Date: December 2002

Master's Project Title: Implementation of Virtual Local Area Networks

Date Project Plan Approved: August 15, 2001

Date Project Coordinator Notified and Grade Submitted: _____

Approvals/Signatures:

Student: Yuheng Zhao Date: 02/04/2003

Faculty supervisor: Date: 2/17/2003

Committee member: Date: 02/04/2003

Committee member: Date: 2/4/2003

Copies to:
Original Attached to Written Report
Copies to: Advisor, Graduate Coordinator, and Student

Table of Contents

Abstract

The goal of the project was to implement Virtual Local Area Networks in Missouri Valley College. This as part of my internship helped me gain an insight into the underlying network architecture existing there and implement VLANs to separate the student network from the security accessed faculty/administration network. Another objective was to study the Wireless Network in Dakota State University and come up with a proposal to implement Virtual Local Area Networks in Dakota State University.

Introduction

Virtual LAN has rapidly become one of the major new areas in the internetworking industry. Virtual LAN (VLAN) is a logical grouping of devices or users. It refers to the ability of switches and routers to configure logical topologies on top of the physical network infrastructure, allowing any arbitrary collection of LAN segments within a network to be combined into an autonomous user group, appearing as a single LAN.

A typical LAN is configured according to the physical infrastructure it is connecting. Users are grouped based on their location in relation to the hub they are plugged in and how the cable is run to the wiring closet. 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) are an alternative solution to using routers to contain broadcast traffic. VLANs offer significant benefits in terms of efficient use of bandwidth, flexibility, performance, and security.

Benefits of VLAN

1) Performance and Broadcast Control

Generally network traffic consists of a high percentage of broadcasts and multicasts. Sending traffic to unnecessary destinations degrades the performance of the network. VLANs 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 [Passmore et al (3Com report)].

Also 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.

2) Formation of Virtual Workgroups

In most organizations, 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. This approach is not as effective as using VLANs.

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

3) Simplified Administration

Seventy percent of network costs are a result of adds, moves, and changes of users in the network [Buerger]. 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 [Cisco white paper]. 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 [Passmore et al (3Com report)].

4) Reduced Cost

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

5) Security

Security is provided by VLANs in two ways.

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 [Passmore et al (3Com report)].

Also as VLANs are logical groups that behave like physically separate entities, inter-VLAN communication is achieved through a router. Thus, all the security and filtering functionality that routers traditionally provide can be used.

Project Objective Statement

Implementation of VLAN in Missouri Valley College and a study to implement the same in DSU.

Missouri Valley College Overview

Missouri Valley College, Marshall, MO vision is to incorporate sophisticated technology in terms of its network architecture to employ advanced learning applications and functionality to students, both on campus and off campus. To do this, the college's resources and Internet access were distributed via fiber, gigabit Ethernet and a web-enabled virtual private network (VPN). In addition two virtual local area networks (VLAN) were to be implemented to separate the student network from the security accessed faculty/administration network.

System Description

There are three sets of users- staff, administration, and students. Each of buildings LANs have to be segmented into two virtual local area networks (VLANs). The staff network should contain access to servers that house information about students' grades and attendance. The administration network stores staff salaries and teachers' histories. These two networks are clubbed into a single VLAN. The student network is reserved for student work. A second VLAN is designed for this. Due to the confidential nature of so much of the data, each VLAN must be isolated from the others.

Feasibility Assessment

The feasibility Assessment involves tangible and intangible benefits for Missouri Valley College:

- Separation of the student network from the faculty/administration network would facilitate electronic enrollment and class registration.
- Isolation of the confidential data between the students and the faculty/administration.
- Availability of an existing strong backbone in the form of fiber, gigabit Ethernet will help in the implementation of VLAN.

Schedules, Timelines

The schedules and timelines are shown in the Gantt Chart. Figure 1

Team Configuration

The Team consisted of

- Yuheng Zhao
- Darrick Davis
- Prof. Minhua Wang
- Prof. Terry Dennis
- Prof. William Figg

Project Plan

	PHASE I : Implementation of VLAN at Missouri Valley College
1	• Configure the switches
2	• Implement the VLAN
3	• Troubleshoot and maintenance of network
	Milestone I complete
	PHASE II : Continuous study of VLAN
	PHASE III : Study and research of WLAN issues and solutions at DSU
4	• Study of WLAN issues
5	• Study of WLAN and VLAN in other universities
6	• Preparation of proposal to implement VLAN in DSU
	Milestone II complete
	Project Closure

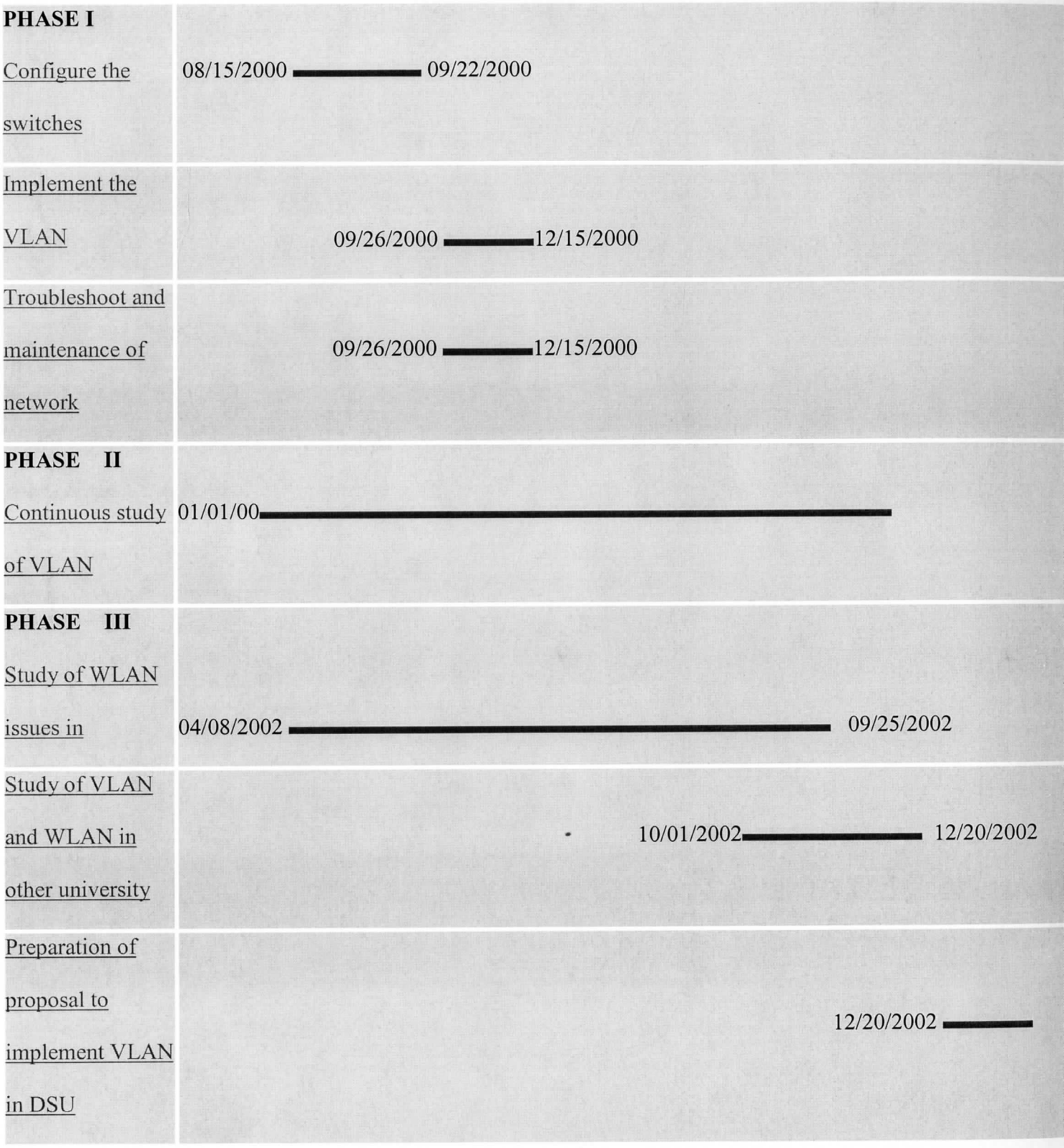


Figure 1: Gantt chart

Analysis and Study of VLAN types

Before considering the implementation of VLAN in Missouri Valley College the types in which VLANs are configured are studied. Then based on this one method is selected.

1) Membership by Port

Port grouping is the most common method of defining VLAN membership, and configuration is straightforward. Membership in a VLAN can be defined based on the ports that belong to the VLAN. For example, in a switch with four ports, ports 2, 3, and 6 belong to VLAN 1 and ports 4, 5 and 7 belongs to VLAN 2 (see Figure 2).

Another implementation is shown using Cisco Catalyst switch. (Figure 3)

PORT	VLAN
2	1
3	1
4	2
5	2
6	1
7	2

Figure 2: Assignment of ports to different VLAN's.

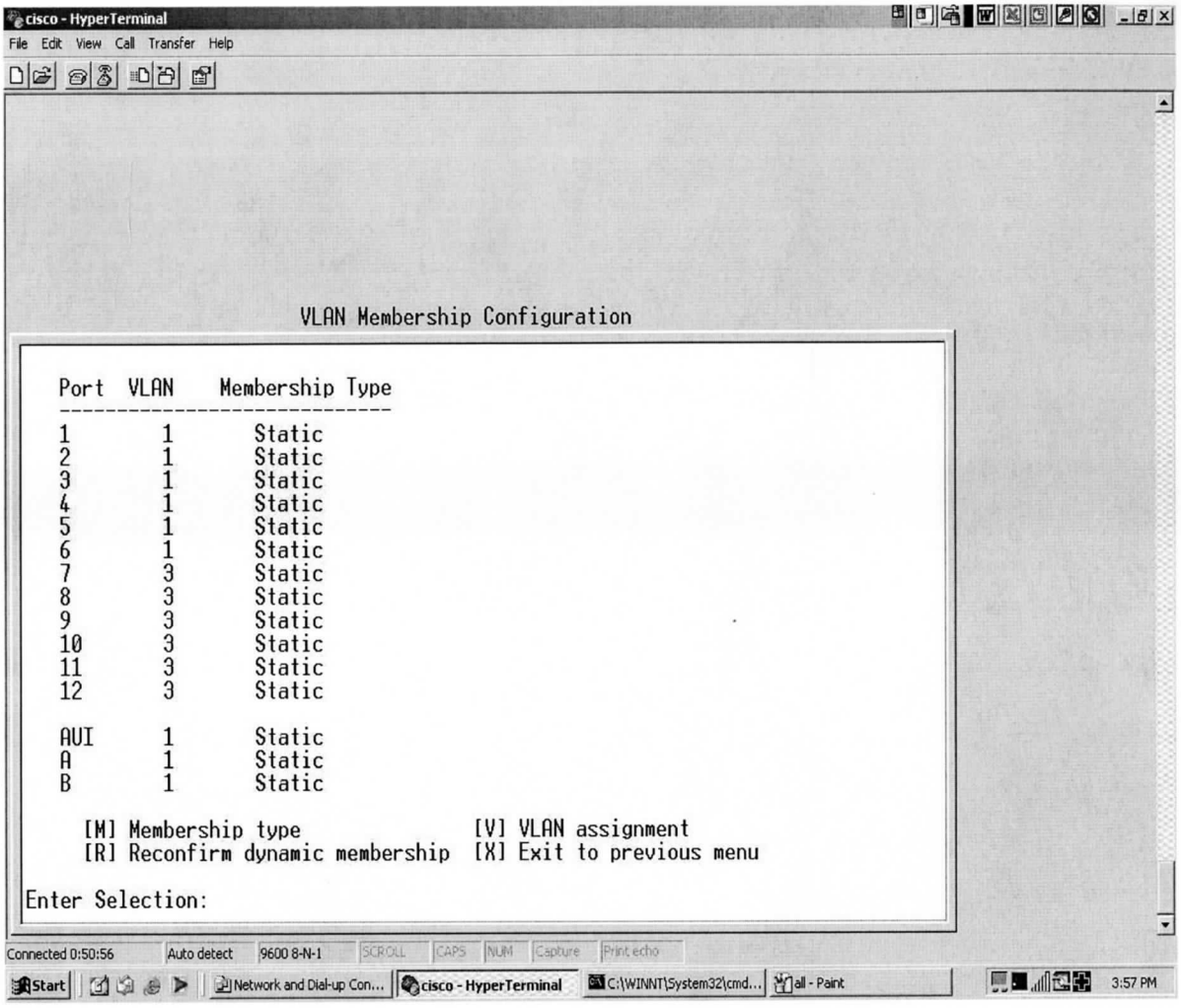


Figure 3: Cisco Implementation

The implementation shown above uses a single switch. However if more devices are to be connected then multiple switches can be used. For example, ports 1 and 2 of switch 1 and ports 4, 5, 6, and 7 of switch 2 make up VLAN A; while ports 3, 4, 5, 6, 7, and 8 of switch 1 combined with ports 1, 2, 3, and 8 of switch 2 make up VLAN B.

The main disadvantage of this method is that it does not allow for user mobility. If a user moves to a different location away from the assigned bridge, the network manager must reconfigure the VLAN. Also defining VLANs purely by port group does not allow multiple VLANs to include the same physical segment (or switch port).

2) Membership by MAC Address

Here, membership in a VLAN is based on the MAC address of the workstation. The switch tracks the MAC addresses which belong to each VLAN (see *Figure* 4). Since MAC addresses form a part of the workstation's network interface card, when a workstation is moved, no reconfiguration is needed to allow the workstation to remain in the same VLAN.

The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is not an easy task. Also, in environments where laptops are used, the MAC address is associated with the docking station and not with the laptop. Consequently, when a laptop is moved to a different docking station, its VLAN membership must be reconfigured.

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

Figure 4: Assignment of MAC addresses to different VLAN's.

3) Membership by Protocol Type

VLANs based on layer 3 information take into account protocol type (if multiple protocols are supported).

VLAN membership is based on the protocol type field.

VLANs defined at layer 3 are particularly effective in dealing with TCP/IP, but less effective with protocols such as IPX(TM) , DECnet® , or AppleTalk® , which do not involve manual configuration at the desktop. Furthermore, layer 3-defined VLANs have particular difficulty in dealing with "unroutable" protocols such as NetBIOS. End-stations running unroutable protocols cannot be differentiated and thus cannot be defined as part of a network-layer VLAN.

4) Membership by IP Subnet Address

Membership is based on the Layer 3 header. The network IP subnet address can be used to classify VLAN membership (see *Figure 6*).

Although VLAN membership is based on Layer 3 information, this has nothing to do with network routing and should not be confused with router functions. In this method, IP addresses are used only as a mapping to determine membership in VLAN's. No other processing of IP addresses is done.

In Layer 3 VLAN's, users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses

Protocol	VLAN
IP	1
IPX	2

Figure 5: Assignment of protocols to different VLAN's.

IP Subnet	VLAN
23.2.24	1
26.21.35	2

Figure 6: Assignment of IP subnet addresses to different VLAN's.

Combination VLAN Definitions

Due to the trade-offs between various types of VLANs, many vendors are planning to include multiple methods of VLAN definition. Such a flexible definition of VLAN membership enables network managers to configure their VLANs to best suit their particular network environment. For example, by using a combination of methods, an organization that utilizes both IP and NetBIOS protocols could define IP VLANs corresponding to preexisting IP subnets (convenient for smooth migration), and then define VLANs for NetBIOS end-stations by dividing them by groups of MAC-layer addresses.

Another important distinction between VLAN implementations is the method used to indicate membership when a packet travels between switches. Two methods exist — implicit and explicit.

Implicit

VLAN membership is indicated by the MAC address. In this case, all switches that support a particular VLAN must share a table of member MAC addresses.

Explicit

A tag is added to the packet to indicate VLAN membership. Cisco ISL and the IEEE 802.1q VLAN specifications both use this method.

To summarize, when a packet enters its local switch, the determination of its VLAN membership can be port-based, MAC-based, protocol-based or IP subnet based. When the packet travels to other switches, the determination of VLAN membership for that packet can be either implicit (using the MAC address) or explicit (using a tag that was added by the first switch). Port-based, protocol-based and IP subnet based VLANs use

explicit tagging as their preferred indication method. MAC-based VLANs are almost always implicit.

The bottom line is that the IEEE 802.1q specification is going to support port-based membership and explicit tagging, so these will be the default VLAN model in the future.

Implementation

For the implementation of the VLAN in Missouri Valley College Lucent's Cajun Switches are chosen over the other vendors. The reasons include scalability, ease of configuration and cost effectiveness.

The CajunView Suite is a comprehensive collection of SNMP based applications that simplifies the complex task of enterprise switched network management. It allows network managers to configure, monitor and control the Lucent Cajun Campus family of products using a single, integrated suite of applications.

CajunView delivers comprehensive Layer 2 and Layer 3 management including a routing manager for Layer 3 management for IP Routing Protocol Configuration, Access Control and Redundancy of a routing element within the network.

The CajunView Suite provides standards-based management across a variety of operating systems for the following campus devices from a single management station:

- **Cajun P330/R**
- **Cajun P550**
- **Cajun P880**

To maximize ease of use, CajunView includes Web-based interfaces for monitoring and configuring devices. This gives network managers the flexibility to manage the network

from any remote site across the Internet. The network manager can use any Internet browser to remotely manage, configure, and view statistics for managed devices.

End-to-end VLAN management

Virtual LANs are used to control broadcast traffic, improve performance and increase security in switched networks. One of the main obstacles to VLAN implementation is the administrative burden it places on the network manager. The initial VLAN design requires detailed knowledge of all network connections. Then, the network manager must maintain VLAN configurations as the network changes and grows.

CajunView provides a very easy-to use, graphical application for VLAN management that allows a network manager to configure and monitor VLAN usage, maintain and assign VLAN numbering and naming across all campus VLANs. Moreover, it enables a network manager to follow additions and changes in the network.

In addition, the application validates VLAN name and tag values and number of VLANS in order to improve VLAN maintenance tasks.

Web-Based Management

Today network management is done usually from a central management station that is located in a control center. Frequently there is a need to access the management data from a number of locations in the network. Webbased management enables the user to access network management data from any station on the network by simply using a Web browser. Web-based management can be very useful for technicians that work anywhere on the network and need access to the management station or device. It may help managers to gather network statistics via their PCs. It gives network managers the flexibility and freedom to manage the network

without being tied to the central management station.

In situations where "heavy-duty" management capabilities are not required and you wouldn't like to make large investment in network management software, Web-based management may be a perfect tool.

With Cajun 333T and 334T Gigabit Ethernet switches, which handle all IP routing, the switch ports are configured to determine which workstations and workgroups can talk to which VLANs. VLANs divide the network into logical workgroups, mainly faculty, student and university administration. VLAN tagging technology is used, which allows a switch port or server to be configured to support multiple VLANs Gigabit Ethernet VLANs create IP-based workgroups based on physical connections. These workgroups are invisible to one another even though they run on the same physical network. VLAN tagging lets workgroups share peripherals and servers. If a student is assigned only to the student computer laboratory on VLAN #10, for instance, he or she can't stray from the confines of that lab network. Even if a rogue student somehow captured the Ethernet switch's IP address and password, he or she still couldn't reach the switch itself or a VLAN of which the student wasn't a member, such as a faculty VLAN.

Network allocations

Notes about the VLAN configuration

- *VLAN* VLAN ID number - used to *Tag* the ports
- *Name* Name/user of VLAN
- *IP Range* Main IP range for workstations
- *Internal* IP range for devices that do not need external access, I.E. printers.

VLAN/IP allocation

VLAN	User	IP Range	Internal IP
1	Faculty	129.78.16/24	172.16.16/24
2	Student	129.78.20/24 129.78.21.0/25	172.16.20/24
3	Administration	IP range reallocated	N/A

Figure 7- VLAN/IP allocation

IP addresses given in CIDR notation. 129.78.16/24 means addresses from 129.78.16.0 to 129.78.16.255 (24 bits Network number, 8 bits workstation).

VLAN implementations in other campuses

This section discusses the implementation of VLAN in Bowdoin University in Brunswick, Maine. The method of implementation and the issues faced by the institution is explained.

Bowdoin University:

Bowdoin University has implemented Virtual Local Area Network using Cabletron switches. Bowdoin has implemented a very flexible "flat" (i.e. no subnets) network structure and use VLANs to isolate or segregate users and hosts where necessary. This is unlike other campuses, which define a subnet structure (size and number of separate subnets determined by a subnet mask for the campus) and then segment the campus network.

The advantages for Bowdoin University using this type of implementation are:

- Flexibility: There is no need to determine a subnet structure or physically co-locate servers and devices to group them.
- Mobility: Users can keep a single IP address and use it anywhere on campus),
- Ease of management: Administration can be done centrally without needing to touch the user's desktop.

Disadvantages:

- The downside is that the implementation is largely vendor (Cabletron) specific and not "standard," and it works best in a flat (unrouted) network. Users and/or

applications that expect a standard subnetted/routed environment need to know how to work within the VLAN environment. Flat networks are also subject to increased broadcast traffic, although Cabletron's VLAN (SecureFast) provides for broadcast containment. Where traditional networks solve these problems with segmentation, VLAN networks solve them in software.

Western Iowa Tech Community College

Western Iowa Tech Community College has implemented VLANs in the form of zones in the college. Each zone is a VLAN in itself. In addition to these zones there are a number of classrooms which have a WLAN. Each classroom has an access point and the laptops have a wireless Ethernet card to enable them to be connected to the network. The classrooms of the future constitute more of these zones. The VLANs are configured for each department and the methodology used in port and MAC address based VLANs. The future plans include configuring a VLAN over the WLANs that exist now.

Dakota State University

WLAN and VLAN

This section briefly explains the concept of WLAN (Wireless LAN). I have taken the example of Dakota State University to illustrate the benefits and the challenges and issues posed by WLAN and the possibility and advantages of implementing VLAN in Dakota State University along with the existing WLAN.

WLAN

WLAN provides the ability for devices to connect to a Local Area Network without any wired connectivity. This allows for devices to gain access to network resources in areas where running physical wires is not possible, (such in open areas), multiple access (as in conference rooms) and permits the ability to roam from one area to another without loosing network connectivity. Wireless connectivity methods have grown over the years from vendor proprietary low speed operations (less than 2Mbps) to IEEE 802.11 networking standards (up to 11Mbps with 22Mbps being released later this year for multiple access, 56MBs for point-to-point). In the most basic form, WLAN is an ordinary LAN protocol that is modulated on carrier waves. IEEE 802.11 is an extension to the existing IEEE 802.3 Ethernet standards.

WLAN utilizes an Access Points (AP), otherwise known as a Wireless Bridge, to provide connectivity between the wireless devices and the wired network. These AP's allow for access ranges of up to 400 feet for 11Mbps and 1500 feet for 1Mbps connectivity. These distances and speed are implementation specific, and affected by power output and obstacles. WLANs are similar to a repeated Ethernet environment where each packet is broadcast to all other WLAN nodes.

However WLAN does pose some challenges and security issues. The following section describes these issues and explains how VLAN can help resolve those.

Challenges include

- IP number allocation to mobile devices and coordination of wireless network deployment.
- Security concerns in WLAN

IP number allocation to mobile devices and coordination of wireless network deployment

IP number allocation is complicated by the mobile nature of wireless users. IP numbers at Dakota State University are mostly bound to a physical location.

In most standard routed network configurations, you would not be able to unplug your computer, walk to another building on campus, plug it in, and expect the IP number to work. You would be on a different part of the network and each part only supports a certain specific list of IP numbers (a subnet).

To resolve this issue for "mobile" computers requesting IP numbers from DHCP servers, Dakota State University can leverage the installed campus routers ability to create a campus wide "virtual" network (VLAN) and forge a single dedicated network and broadcast domain for projected wireless usage, thus allowing IP numbers to work regardless of the router hardware they ultimately pass through.

Security concerns in WLAN

Traditionally WLANs do not provide much security against unauthorized access. Users may freely purchase an 802.11b Wireless network card, install it in their machine, and by utilizing DHCP services, gain access to the local network via a WLAN. Also users do not necessarily need to be physically located within a building served by the WLAN as the distances covered by the WLAN are large.

Some of the methods that can be used to provide security to a WLAN are:

- MAC address filtering
- Vendor specific authentication
- SSID/Network ID

- Wired Equivalent Privacy (WEP)

MAC Address filtering

This technology uses a hand coded list of MAC addresses of the client WLAN interface cards that are allowed to associate with an Access point.

Strengths:

- Useful in small installations where there are few access points and centrally administrated clients.

Weaknesses:

- Scalability problem: for the MAC address list for allowed clients must be installed in every Access Point the client is allowed to associate to.
- Care must be taken to update all the lists if a client interface card is replaced.
- vulnerable to attackers who either steal WLAN interface cards that are allowed to access the WLAN, or by assuming the MAC address of an allowed interface card

Vendor specific authentication

In this technology user names and passwords are coded into the access points. A custom software client is installed on the client devices. The software prompts the user to enter his user name and password before allowing connectivity to the WLAN.

Strengths:

- More security than MAC addressing scheme

Weaknesses:

- All the client machines need to have the client software installed
- Prone to security attacks like sniffing, hacking

SSID/ Network ID

This technology incorporates a seven digit alphanumeric identifier called a SSID/Network ID which is hard coded into the AP and the client devices.

This ID is transmitted by the WLAN client during AP association. It is then authenticated and if correct the AP allows association.

Strengths:

- a large-scale security mechanism

Weaknesses:

- The SSID is transmitted in clear text. SSIDs are vulnerable to an attacker utilizing a Wireless packet sniffer, due to the clear text nature.
- To assign a new SSID to all the AP's and WLAN clients must be manually initiated.

Wired Equivalent Privacy (WEP)

WEP utilizes either 40bit or 128bit encryption algorithms, via shared secret keys. Four different keys (shared secret keys) are defined, but only one key is active at any given time, and these keys are typically stored in encrypted fashion on the AP and WLAN client.

Weaknesses:

- Encrypted WLANs, cannot connect to an non-Encrypted WLAN, such as a home implementation

- WEP is vulnerable to replay attacks and reverse engineering of the WEP keys utilized

Utilizing VLANs

By creating a separate VLAN (Virtual LAN) strategy for the WLANs, one can deliver and contain the WLAN clients without infesting the wired network. A separate VLAN for the WLAN clients will ensure all network broadcasts (ARP, IP broadcast) will remain only on the WLAN. VLANs also offer the ability to expand a WLAN to multiple physical locations. This greatly improves the roaming ability of mobile users. Normally, when a WLAN client associates from AP to AP, a brief network outage is experienced on the roaming WLAN client. This is due to the WLAN client associating with a new AP and establishing a new IP address (if DHCP is utilized). In a static IP environment, users would have to manually change their client IP address to a permitted IP address services by the new AP. By retaining the AP's on the same VLAN and IP subnet, the network outage is brief, for the client will reuse the cached DHCP address, or will continue to use the configured IP address.

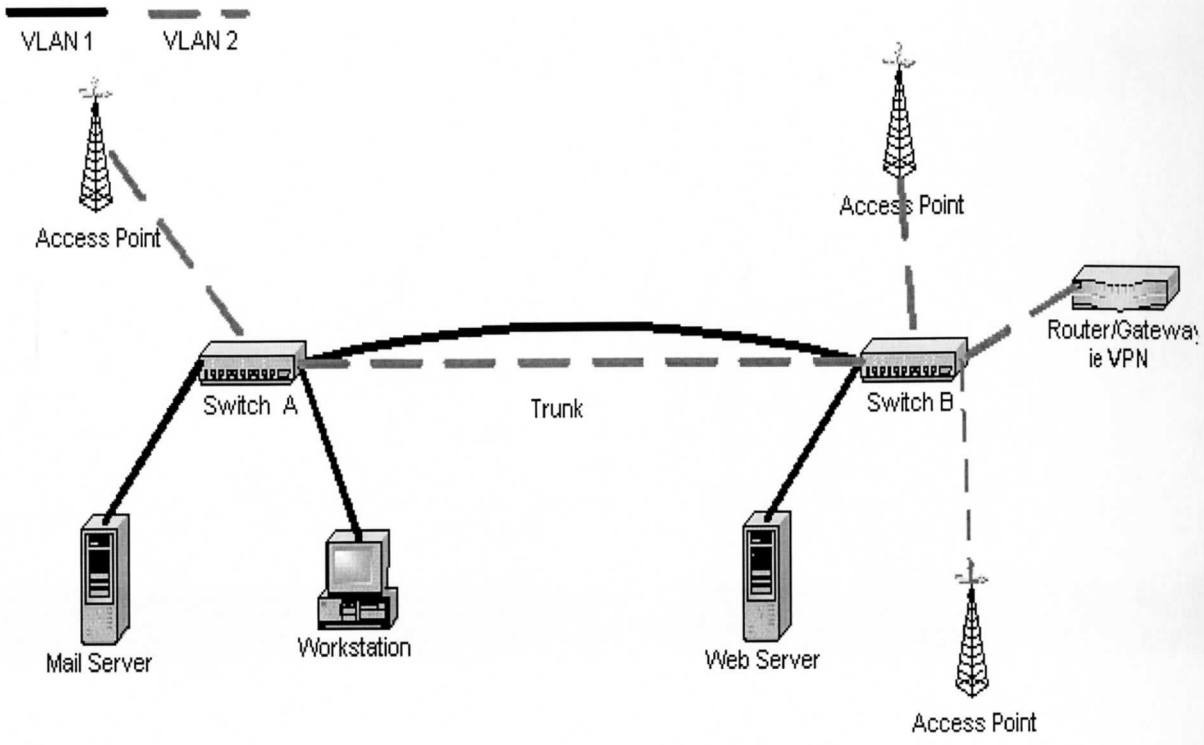


Figure8- Utilizing VLANs

SWOT ANALYSIS of the implementation of VLAN over the WLAN in DSU.

Strengths

The strengths can be summarized in the form of skilled staff, with sound experience and a good budget to back up.

- Skilled staff, responsive to change: DSU's Computing Services and the Network department have been updating the network of DSU to cater to the challenges of increasing bandwidth, mobility among users and security.

DSU's computing services has been constantly upgrading the network since its inception. The latest and the best in network technology has been used to provide the best network access to the students, staff and the faculty.

- Good relationship with other administrative budget centres

There has never been a compromise on the budget regarding network implementation hence getting a budget allocated for VLAN will not be an issue.

- Sound experience in financial control, project management, acquiring and managing resources, bid writing. This has been proven by the implementation of the WLAN in DSU in a short span of time.

The people responsible in the Computing services have strong project management experience and the number of project undertaken have shown that the projects have been under financial and schedule control.

- Good team working at senior management level

Weaknesses

Weaknesses are mainly in the form of new technology and lack of expertise.

- Size and scale make reacting quickly to change/initiatives difficult

To scale the WLAN and simultaneously implement the VLAN will be difficult. This factor needs to be considered while implementing both simultaneously.

- New technology.
- In some areas expertise is concentrated in a few key staff.

VLAN has not been implemented before. Hence this will be a key issue. The expertise is also not spread over all the resources. The technology has to be learnt first before implementation.

Opportunities

The opportunities exist in the form of skilled manpower and external funding.

- Availability of/access to external funding for special projects

The funding options need not be from just with the university. Other resources can be looked into.

- Availability of Substantial external and University capital funding to upgrade campus network..
- Availability of skilled manpower in terms of students and Computing services personnel.

This is very important as the Center of Excellence can provide skilled manpower in the form of students and these students can supplement the already existing skilled personnel of the computing services.

Threats

- Threats are external to the university. They could be in the form of other universities implementing WLAN and VLAN before Dakota State University.
- The devices being of different vendors can make the interoperability difficult.

The compatibility between the different vendors and the different standards has to be looked into. Scalability is another threat as using the present switches might pose a problem is they are not VLAN compatible.

Conclusions and recommendations

The implementation of VLAN at Missouri Valley College has had the following benefits.

- A reduction in cost has been noticed by the implementation of VLAN. This is due to the fact that expensive routers have been eliminated.
- Also the handling and moving or changing workstations has been avoided.
- The administration of the network has been considerably easier
- Security has improved, as the two networks have been isolated.

There are some drawbacks faced by Missouri Valley College:

- As the number of users grow it will be tedious to update one by one the VLAN membership in that group.
- The physical location of some devices is a concern as although some devices such as a printer are configured virtually it is uncomfortable if it is farther away from the user. In some situations the VLANs posed a problem. Consider the situation where one student of the workgroup is on the fourth floor of Sigma Nu House , and the faculty 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 was the implementation of centralized server farms at Missouri Valley College, which are essentially collections of servers and major resources for operating a network at a central location.

Centralized server farms caused problems when setting up the VLAN for faculty as servers could not be placed on the other VLAN. In such a case, the server would be

placed on a single VLAN and the other VLAN's trying to access the server would have to go through a router reducing performance.

- The technology of VLAN is still in development. Standards are still being set. The IEEE 802.1Q, the standardized VLAN setting that manufacturers/vendors must comply so that their products will be interoperable with other VLAN vendor products is still being finalized. Furthermore, the IEEE 802.1Q standard applies only to Layer 1 and Layer 2 VLANs only. Protocol type-based VLANs and higher layer VLANs are not covered in it. It will be hard for proprietary VLANs implemented using the latter type to be interoperable with other vendor products.

The implementation of VLAN in DSU can be considered as a future option as the number of students and users grow in DSU.

It can complement the WLAN technology already implemented in DSU to secure the network further. Several things are to be noted however in regarding the implementation of VLAN over the WLAN.

- Firstly the access points need to be configured on a single VLAN. This would be a wireless VLAN. The students would have complete roaming access due to this.
- Secondly the faculty and administration network should be on a wired VLAN. This would enable security and isolation from the other network.
- To scale this network in the future the single wireless VLAN can be broken down into several VLANs. But roaming capabilities would be restricted if the student goes from one network to another.

Bibliography

Suba Varadarajan, Virtual Local Area Networks, Ohio State University

Jeyasubramanian. V*LAN* http://www.geocities.com/CapeCanaveral/7215/vlan.html, retrieved last 25 February 2000.

UCDAVIS Network 21 Consultants. *VLAN*, http://net21.ucdavis.edu/newvlan.htm, retrieved last 20 February 2000.] IEEE/ISO/IEC, "Virtual Bridged Local Area Networks," *ISO Publication* , July 1998. Draft Standard: IEEE Standard for Local and Metropolitian Area Networks, P802.1Q/D11.

ATMF, "LAN Emulation over ATM Specification, Version 1.0," *The ATM-Forum: Approved Technical Specification*, 1995.

J. L. Sobrinho and A. Krishnakumar, "EQuB - Ethernet Quality of Service Using Black Burst," *Local Computer Network Conference* 1998.

Appendix – A VLAN Protocols

IEEE is the standards body doing the most active work in VLAN standardization. The IEEE 802.1 Internetworking Subcommittee is the specific group in charge of this technology area. In March 1996 the subcommittee finished initial phase of investigation for developing VLAN standards [1]. The IEEE work as well as other VLAN related standards are introduced briefly below.

IEEE 802.1D

IEEE 802.1D is more formally known as the *MAC Bridges Traffic Class Expediting and Dynamic Multicast Filtering Protocol* [1]. It is the IEEE MAC layer spanning tree algorithm. The spanning tree algorithm guarantees loop-free delivery of MAC frames, even in the presence of alternate paths that present the potential of routing loops. This is extremely important to VLAN switching. Fortunately, it was also important to Ethernet bridge based networks years earlier also. The protocol was already completely defined and widely implemented long before VLANs existed.

IEEE 802.1Q

The crown jewel that resulted from the march 1996 IEEE 802.1 Subcommittee meetings was the 802.1Q frame tagging standard. The 802.1Q standard defines how the following functions are to be performed in VLANs [1]:Positions the functions of virtual bridged LANs (VLANs) within an architectural
description of the MAC layer.

- Specifies the operation of the functions that provide frame relay in the VLAN Bridge.
- Defines the structure, encoding, and interpretation of the VLAN control information carried in MAC frames in a VLAN.
- Specifies the rules that govern the insertion and removal of VLAN control information in MAC frames.
- Establishes the requirements for, and specifies the means of, automatic configuration of VLAN topology information.
- Defines the management functionality that may be provided in a VLAN bridge in order to facilitate administrative control over VLAN operation.
- Specifies requirements to be satisfied by equipment claiming to conform to this standard.

There are two MAC tagged frame structures defined in the standard, one for Ethernet and the other for Token Ring/FDDI. The Ethernet "tag" consists of a two octet Tag Protocol Identifier (TPID) and a two octet Tag Control Identifier (TCI). The Token Ring/FDDI "tag" has an eight octet TPID and the same two octet TCI. The TPID identifies the frame as a tagged frame. The TCI delivers user priority information as well as the actual VLAN Identifier (VID).

Inter-Switch Link (ISL)

CISCO switches exchange VLAN membership information using the ISL protocol. ISL uses an extremely cost-effective low-latency method of packet identification and transmission in Fast-Ethernet environments. ISL uses an efficient 10-bit addressing technique [6] (compared to IEEE 802.1Q's 32 bit addressing). Additionally ISL is

supported by the CISCO Internetworking Operating System (IOS) used in CISCO (and other) routers. This provides VLAN interoperability between switches connected through routers.

IEEE 802.10

IEEE 802.10 protocol was designed as a tagging format for adding security to LANs at layer 2. The protocol is not widely used. CISCO introduced the idea to use the 802.10 tagging format to transmit VLAN tagging information. The introduction of 802.1Q and ISL now replace much of the functionality the 802.10 protocol was to be used for. The one major function CISCO still uses this for is to communicate VLAN information across FDDI links. Neither 802.1Q nor ISL are defined for FDDI frame types.

LAN Emulation (LANE)

ATM LAN Emulation (LANE) designed to allow existing Ethernet based devices/protocols to run over ATM backbone networks as if they were on the same LAN [4]. This is accomplished by introducing two new types of devices into the network: LANE Servers (LESs) and LANE Clients (LECs). A LEC is software that resides either on the Ethernet switch or a stand-alone device. A LES is software that resides either on the ATM switch or a stand-alone device. The LESs and LECs serve as MAC to ATM address translators. After the address translation is done, the LECs handle the conversion of Ethernet frames to and from ATM cells.

Within this kind of mixed technology environment VLANs can still exist. The primary limitation is that with basic LANE implementations, all ATM connected machines that interface to the Ethernet world through a given interface must belong to the same VLAN. This is due to LANE implementation issues. This limitation can be avoided in more

robust LANE implementations that allow multiple LECs to be instantiated within the same physical switch or device. This improvement comes at the cost of additional configuration and management. Note that there is no limitation on VLAN usage by Ethernet connected hosts. If ATM is used only as the backbone of the network, and there are no ATM connected hosts, LANE introduces no limitations.

APPENDIX – B Screenshots of VLAN configuration

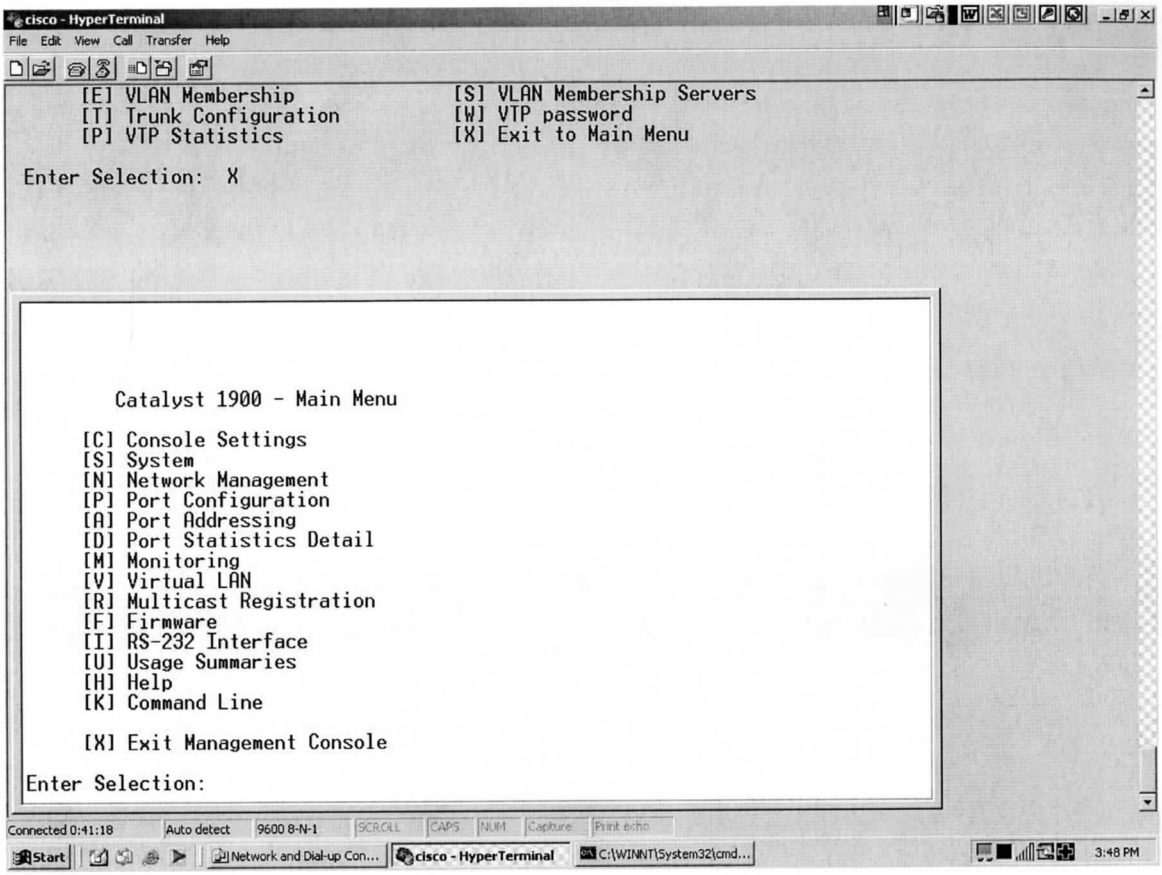


Figure B.1 Main menu screen

The user enters option [V] for VLANs. The next screen Figure B.2 shows the switch's VLAN options menu.

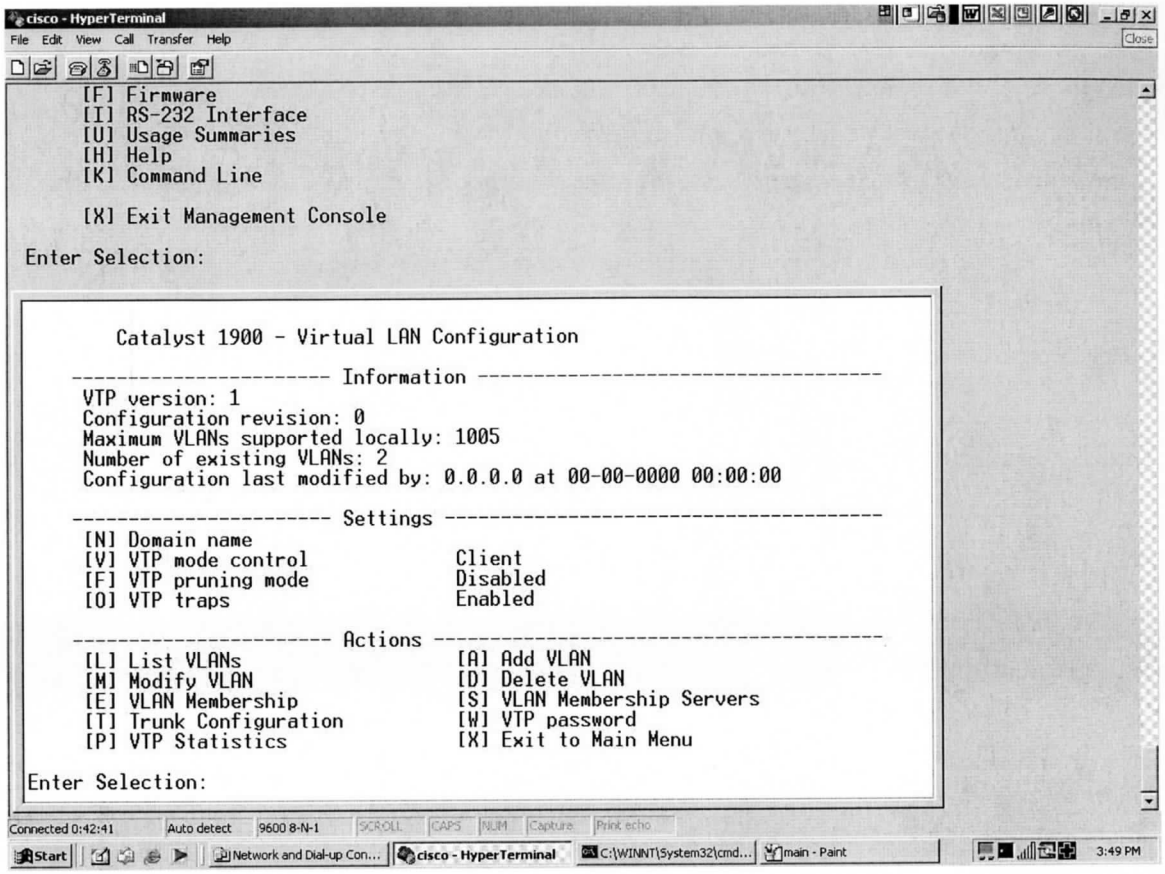


Figure B.2 Options screen

The user can list, modify, add or delete a VLAN or configure the trunk. The next screen Figure B.3 shows the screen after the user has selected option [A].

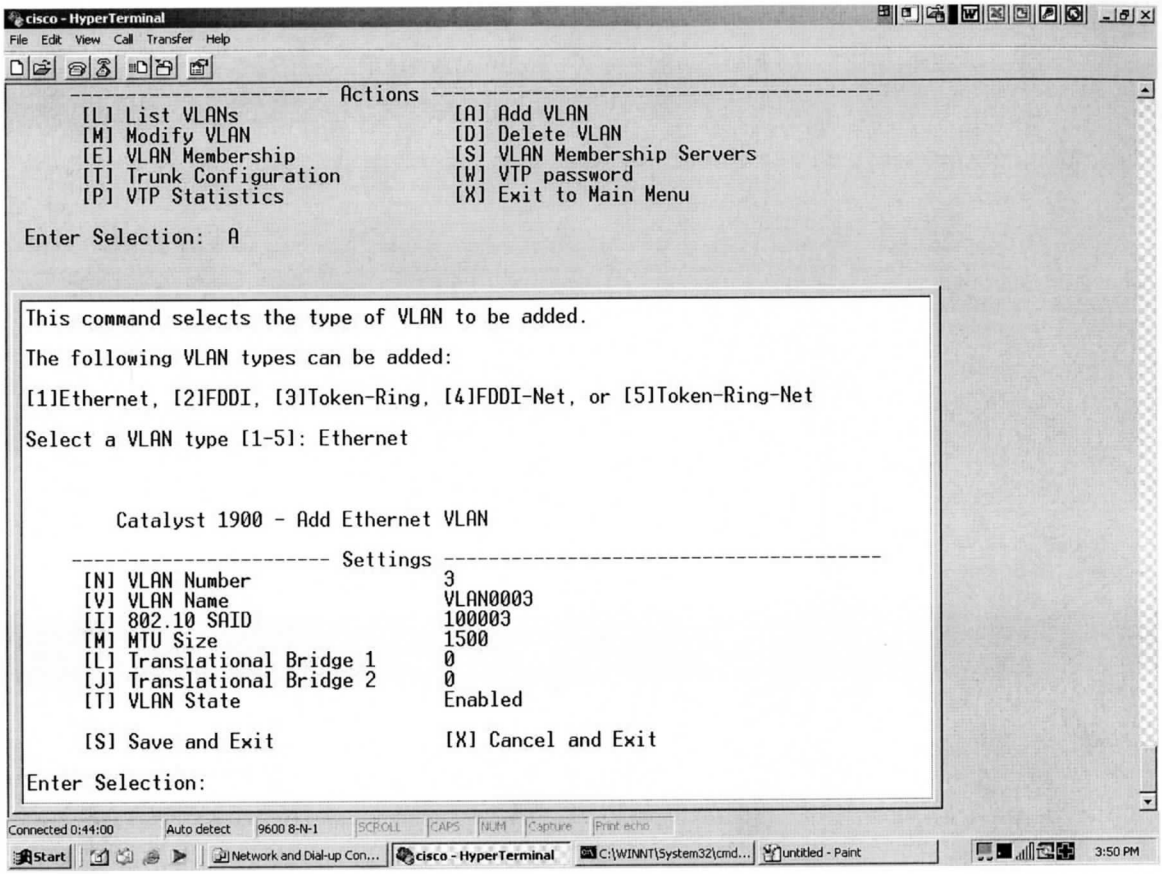


Figure B.3 Adding a VLAN

After the user has selected [A] the default VLAN name will be displayed. Here it is VLAN 3 as VLAN 1 and 2 have already been assigned. The user can then change the default name from VLAN0003 to Student.

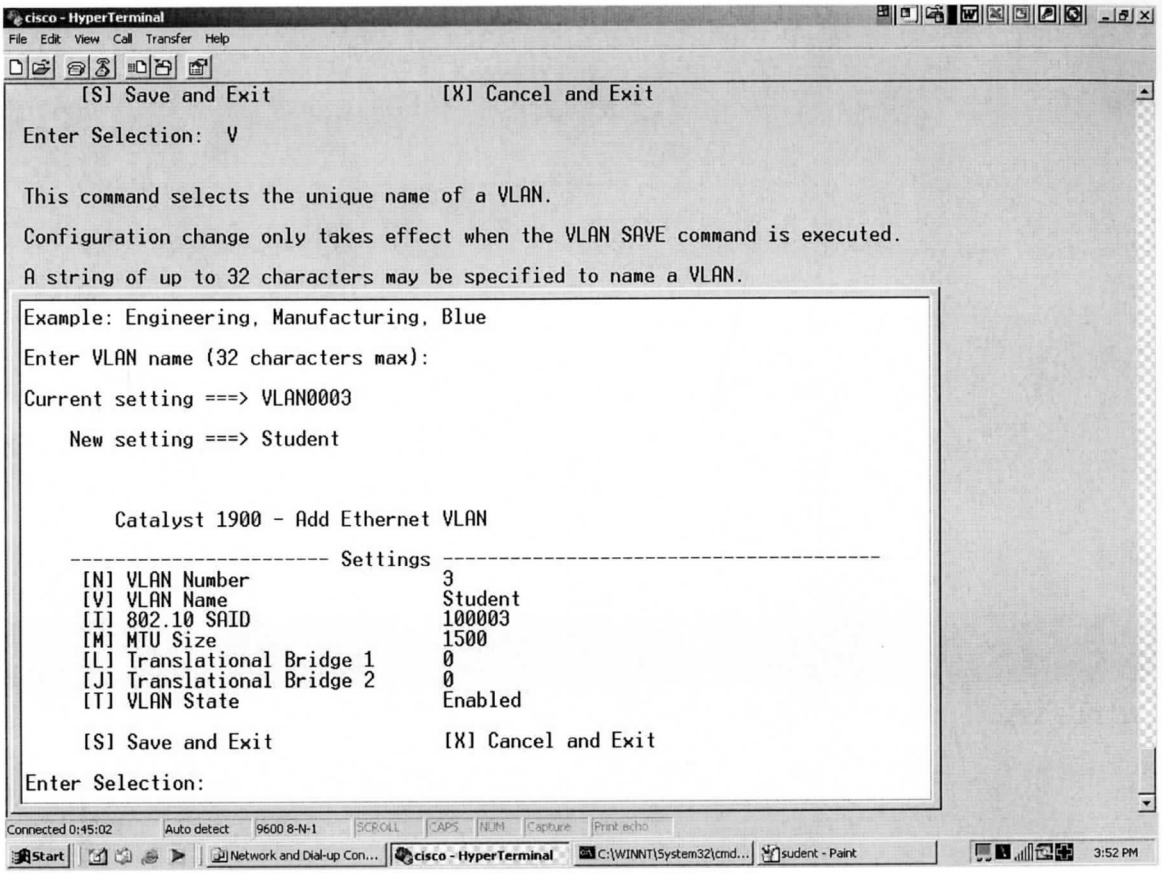


Figure B.4 Changing the name of VLAN

The next screen Figure B.5 then shows the various ports to which the user can assign VLAN student. Here we have assigned ports 7-12 for student VLAN.

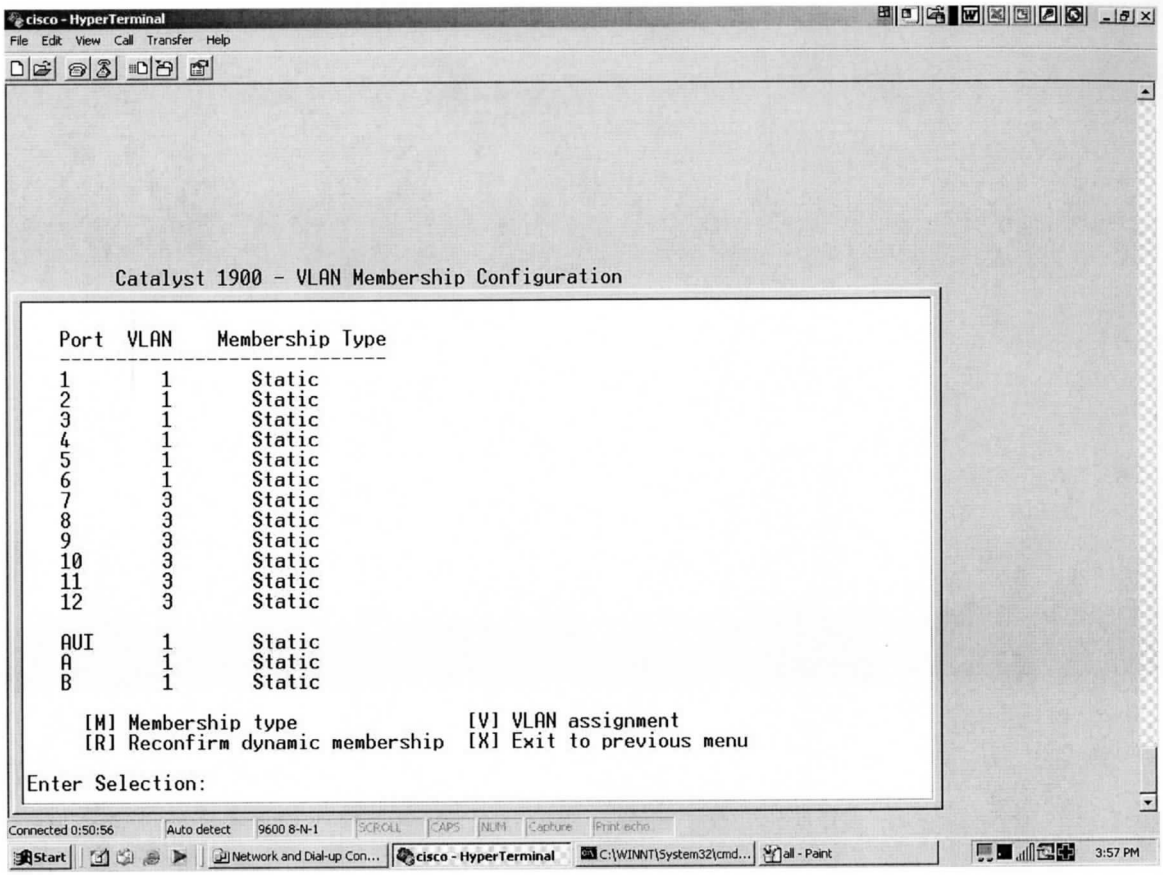


Figure B.4 Port assignment to student VLAN

The next option is to exit to previous menu so that the user can either add another VLAN or add trunking information.

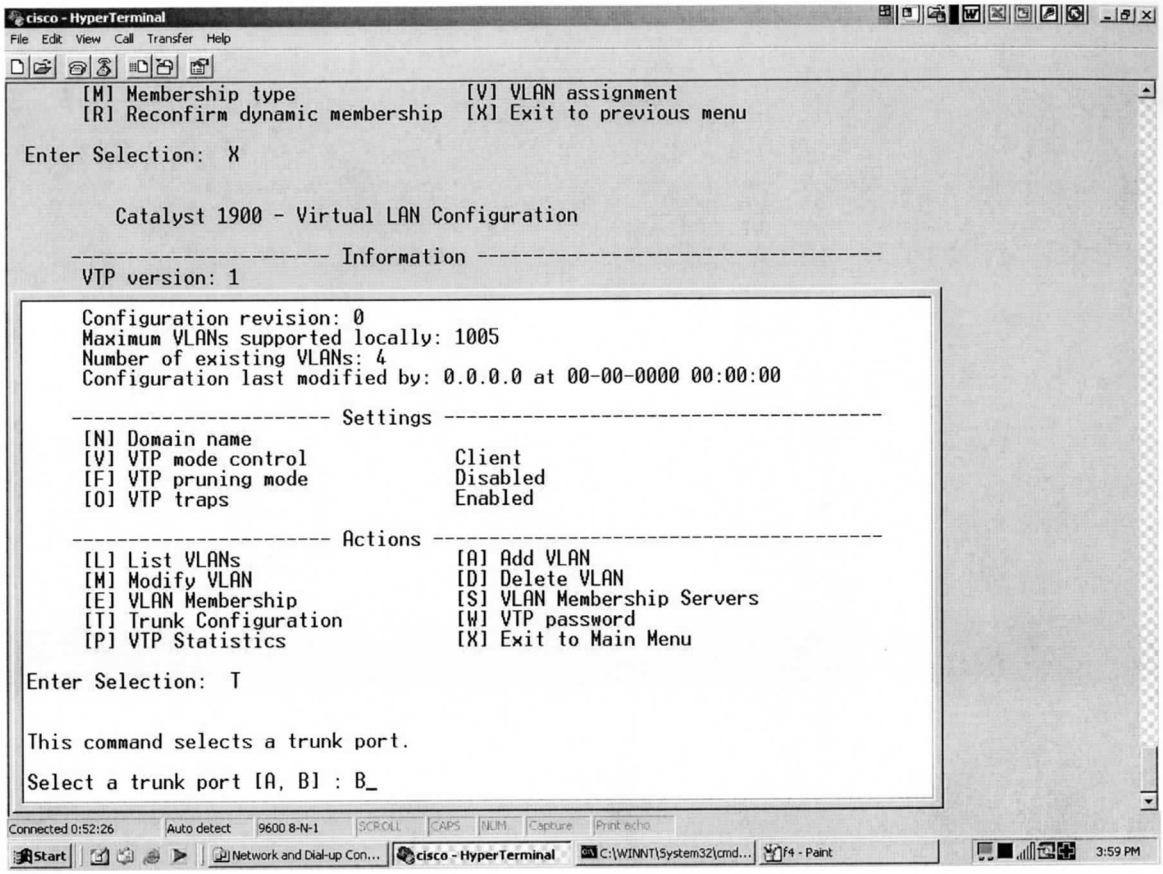


Figure B.5 Trunking configuration

Here the user selects option [T] for configuring the trunk. There are two ports A and B of the router to which the user can trunk the switch. Here we select port B.

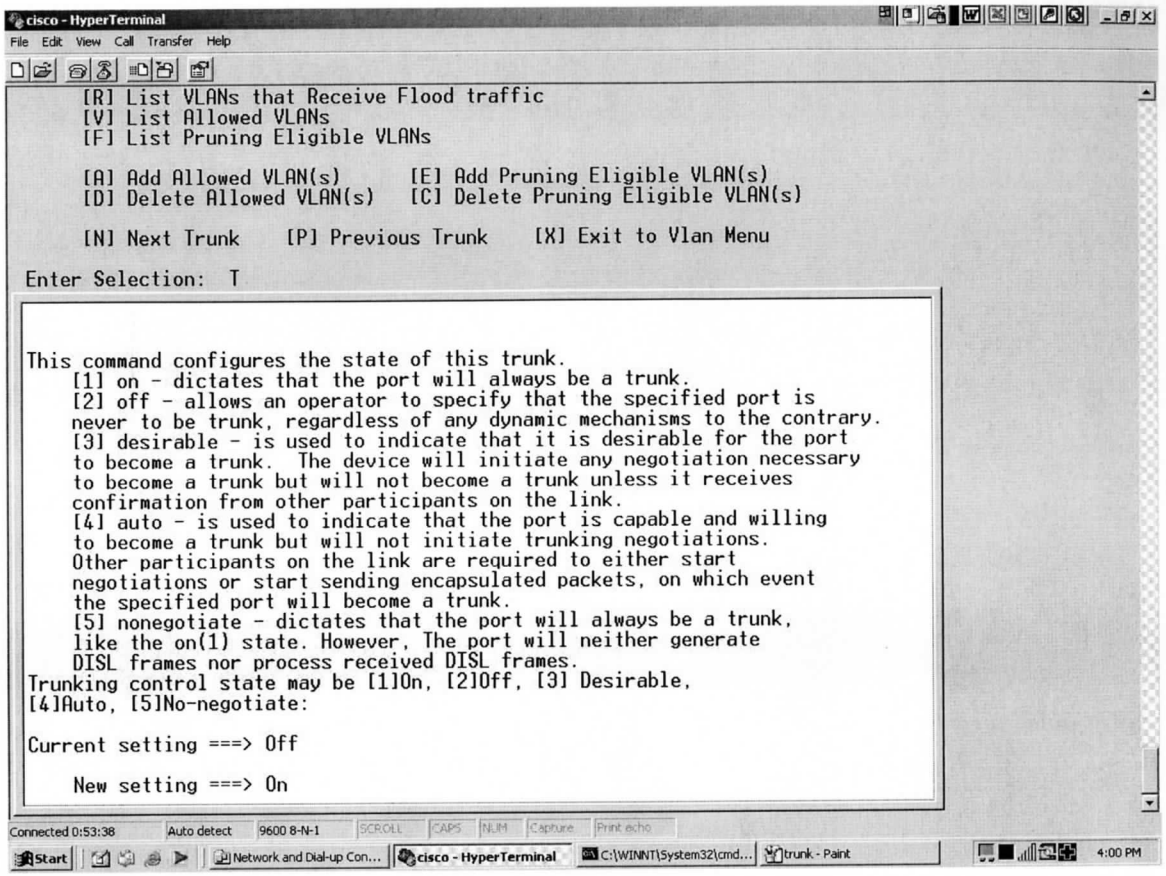


Figure B.6 State of the trunk

Here the user can set the state of B to be ON.

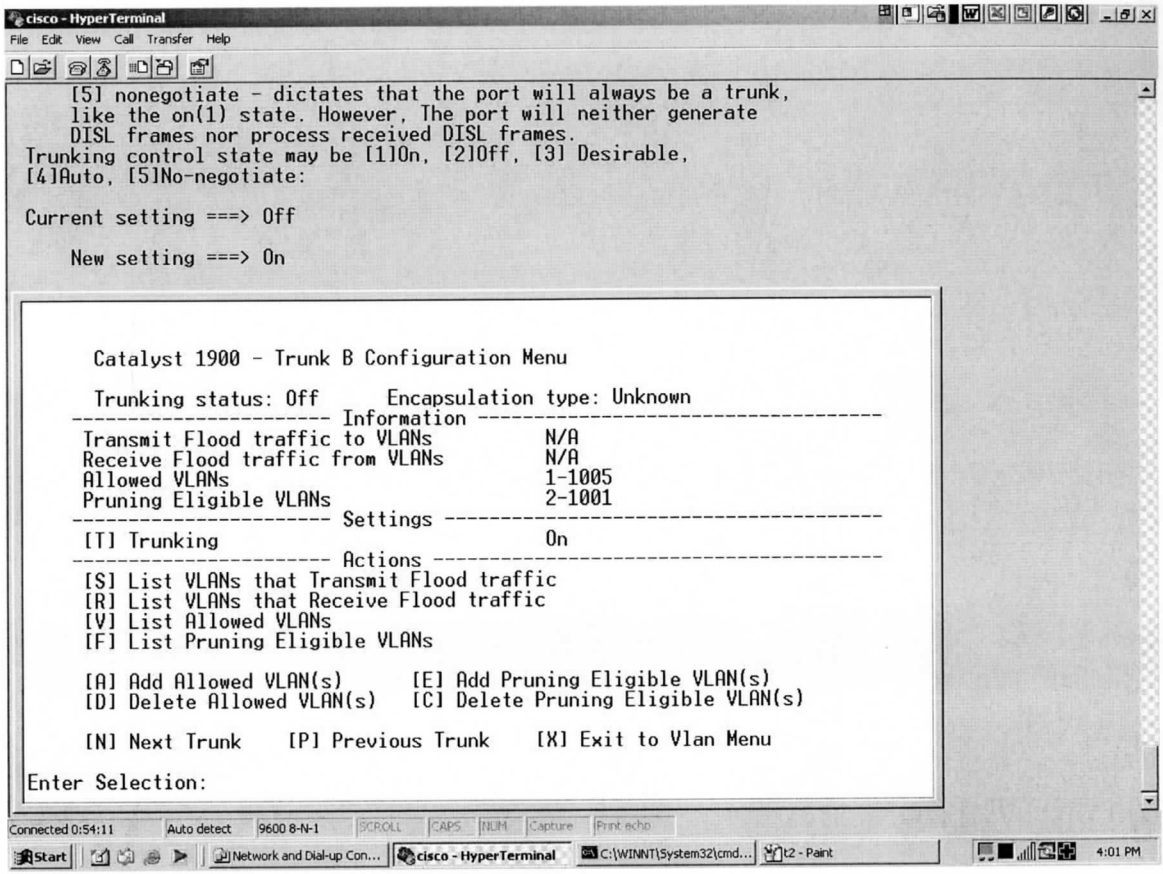


Figure B.7 Trunk status

After the trunking has been done the user can exit back to the previous menu by pressing [X].

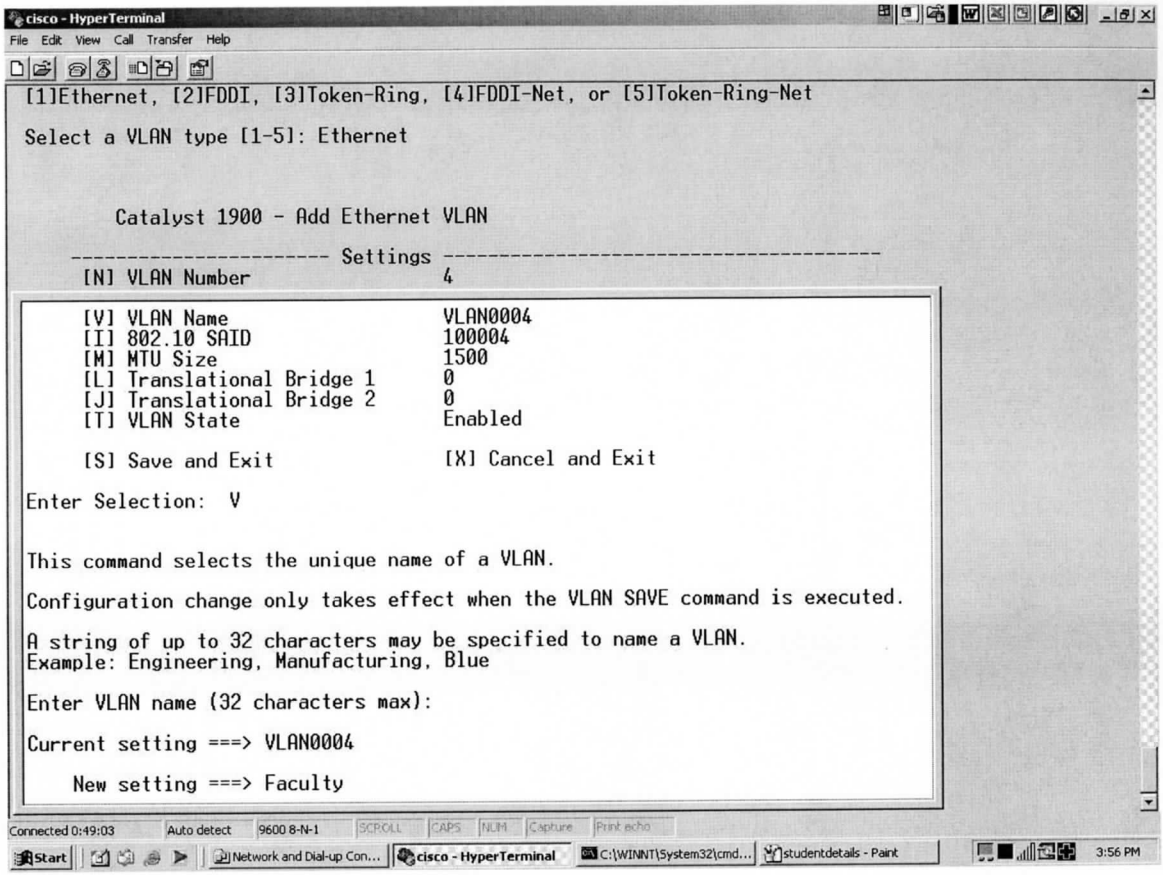


Figure B.8 Faculty VLAN

Here the user can select [V] again for entering the information about Faculty VLAN.

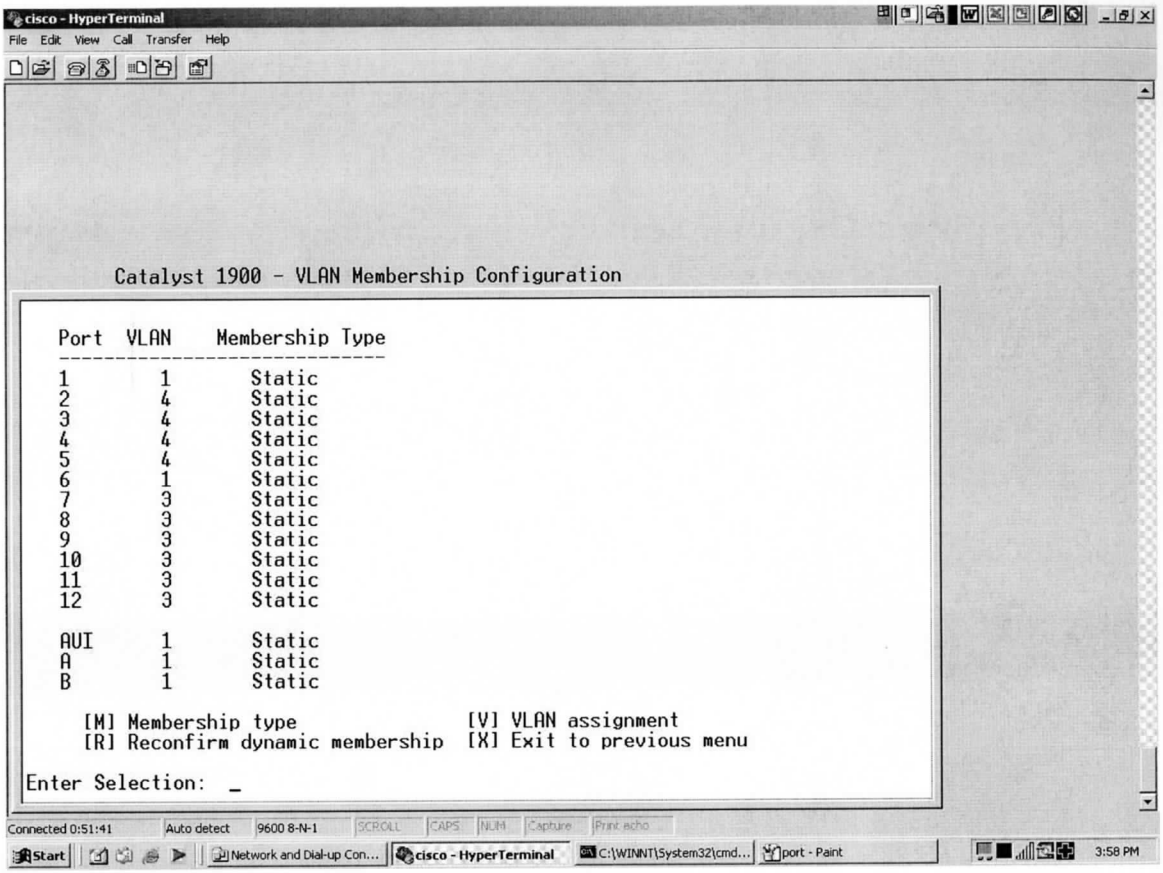


Figure B.9 Faculty ports

Ports 2-5 are selected for Faculty VLAN.

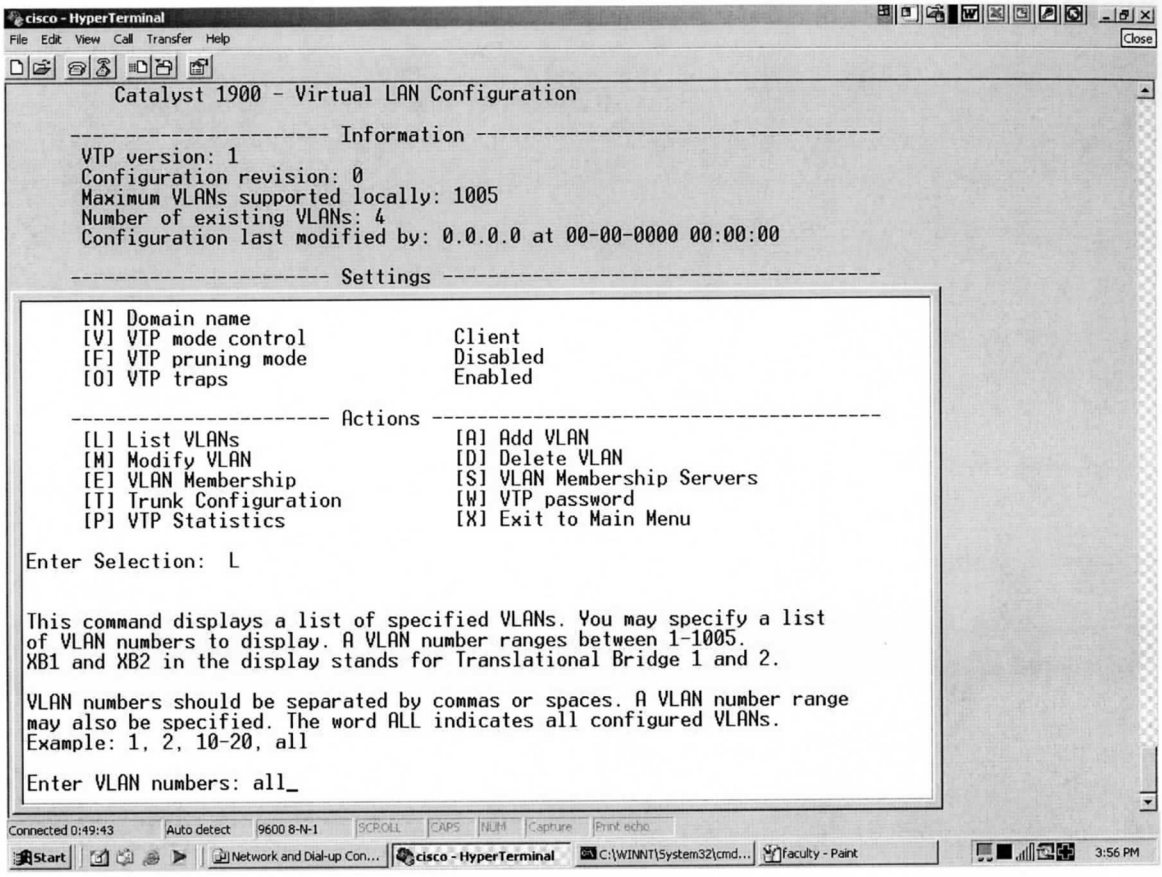


Figure B.10 List VLANs

Here the user can select option [L] to list the VLANs.

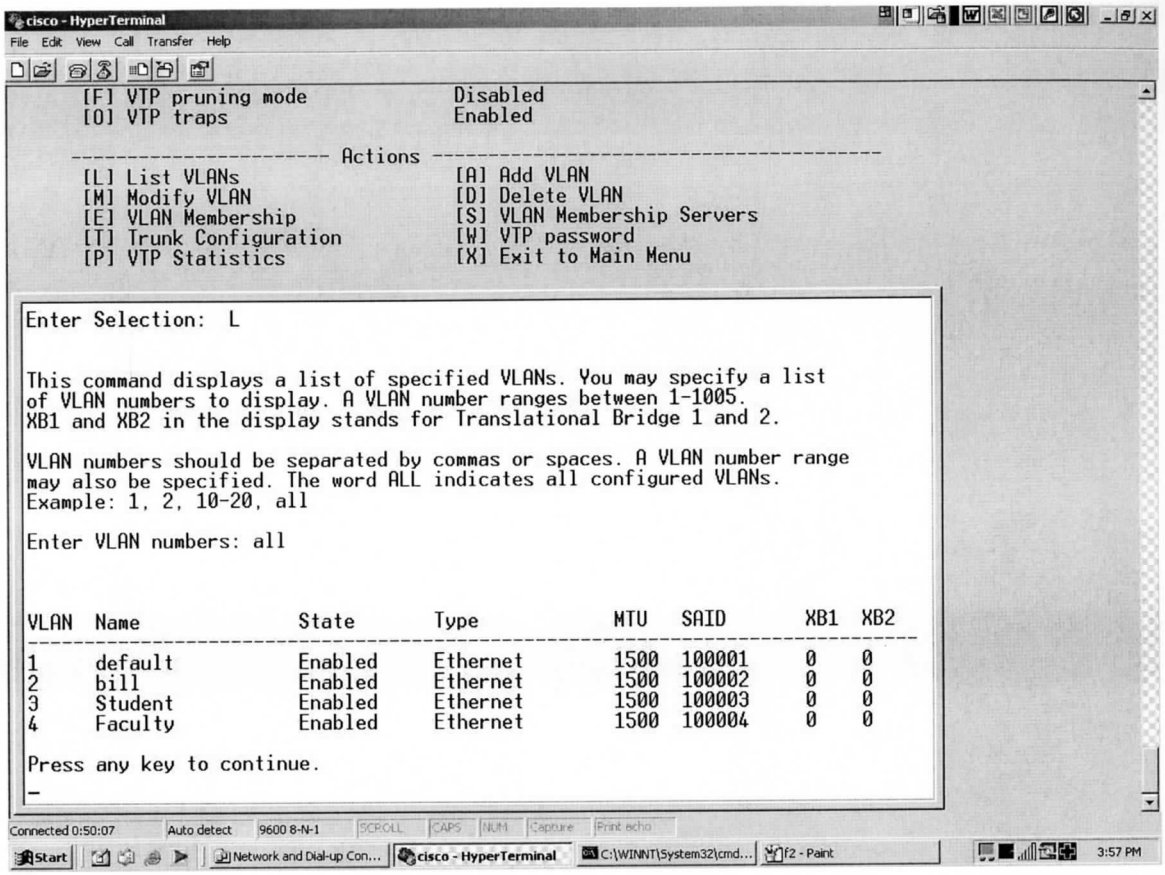
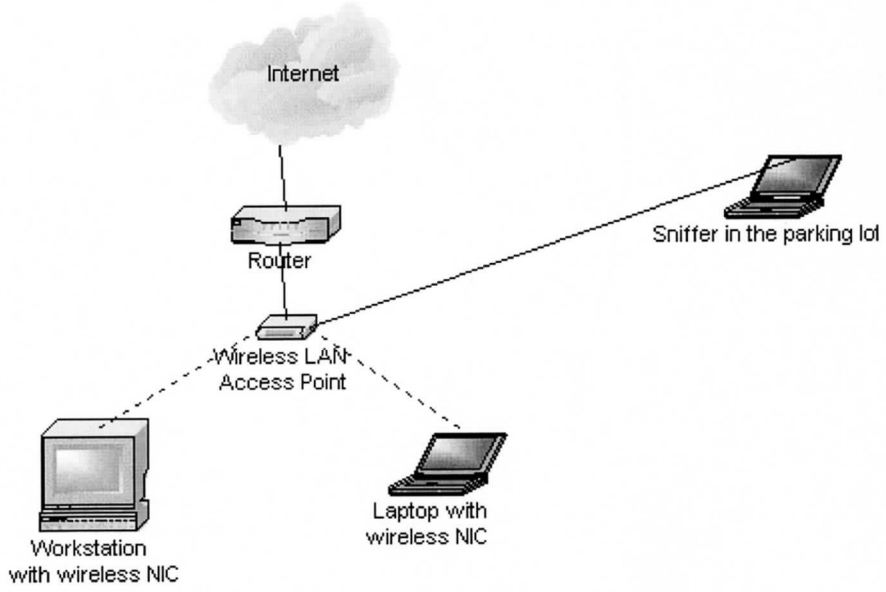
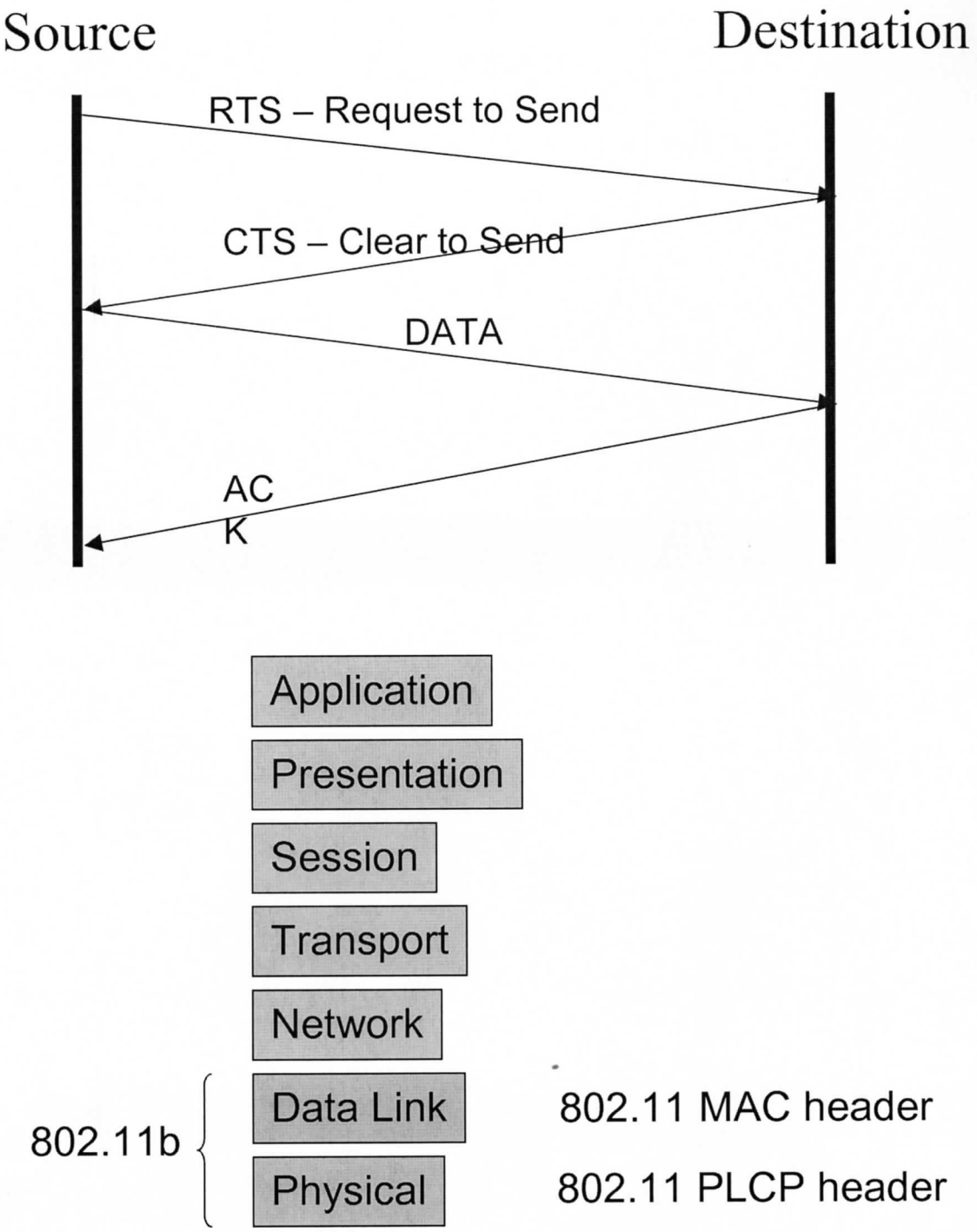
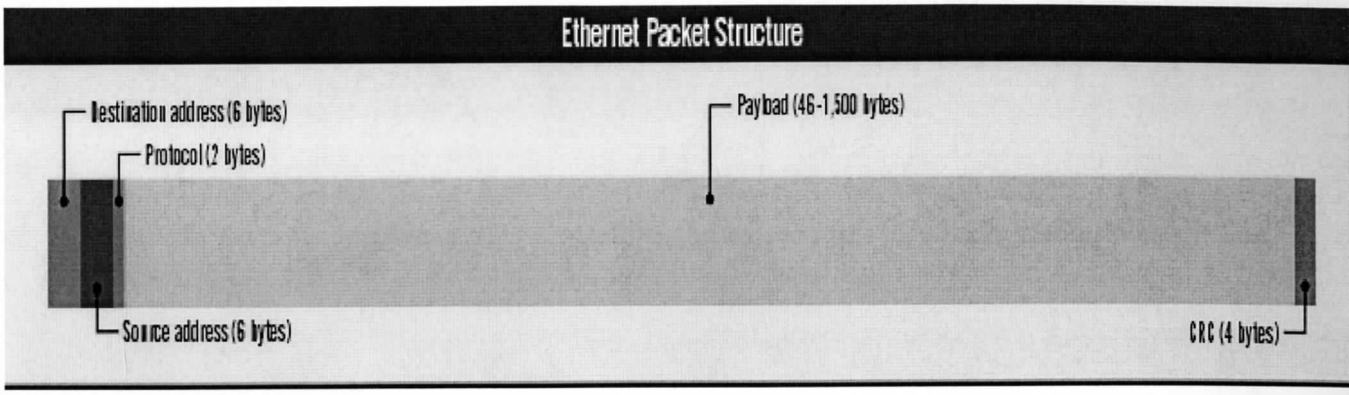


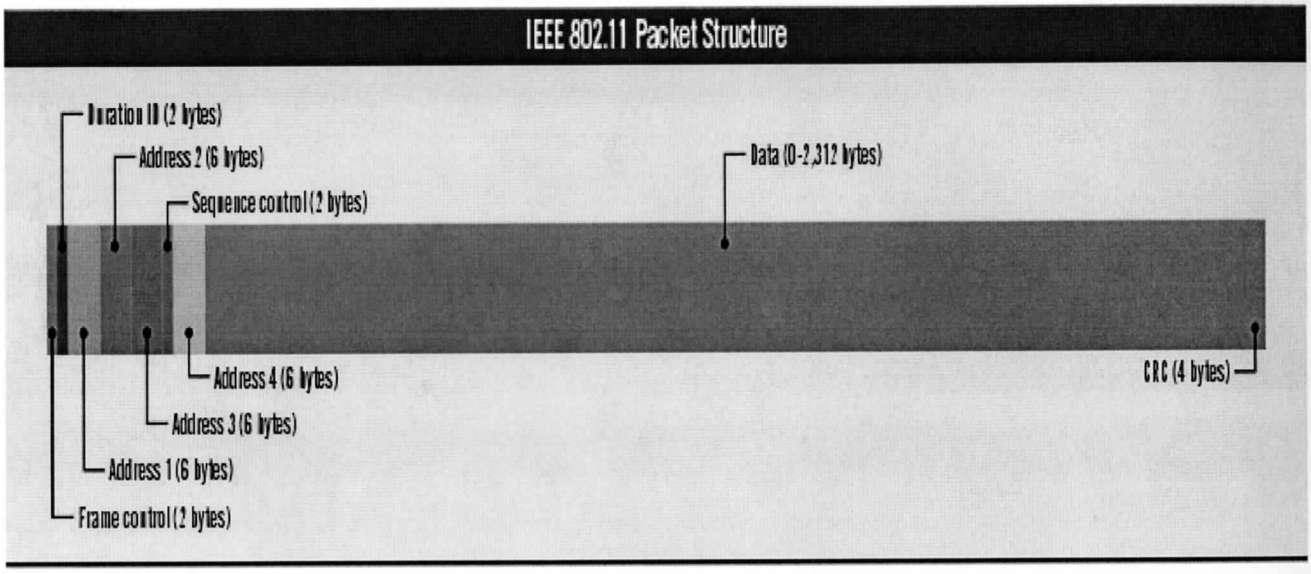
Figure B.11 All VLANs

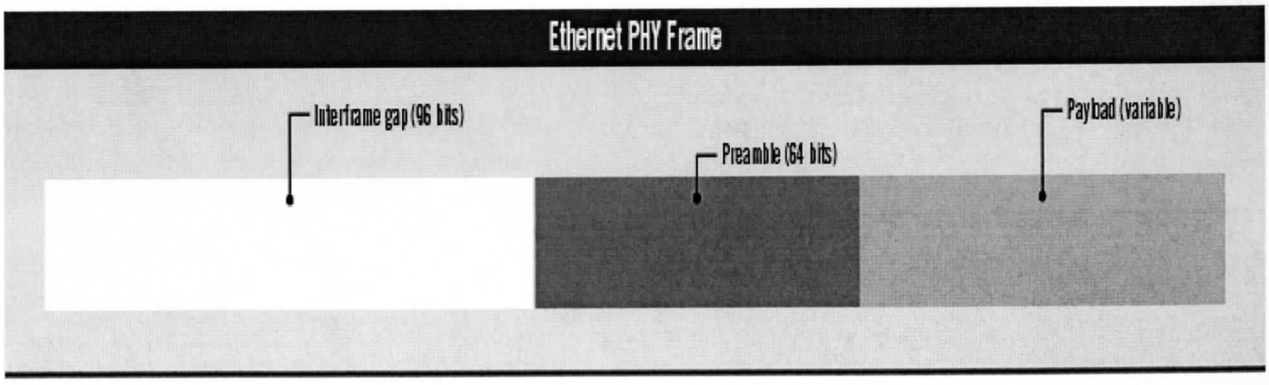
This screenshot shows the four VLANs.

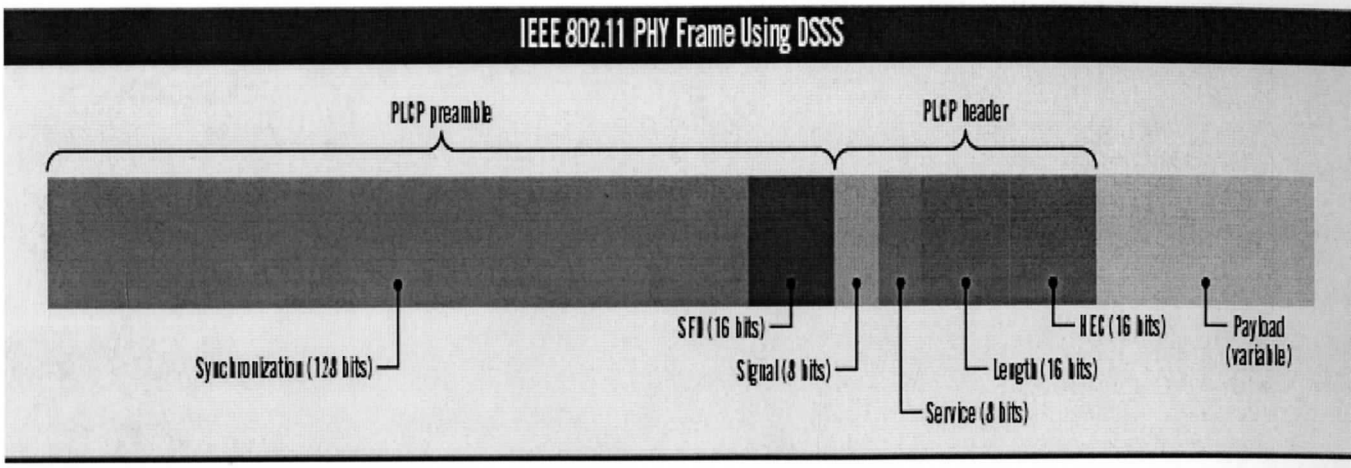

Internet
Router
Sniffer in the parking lot
Wireless LAN
Access Point
Workstation
with wireless NIC
Laptop with
wireless NIC

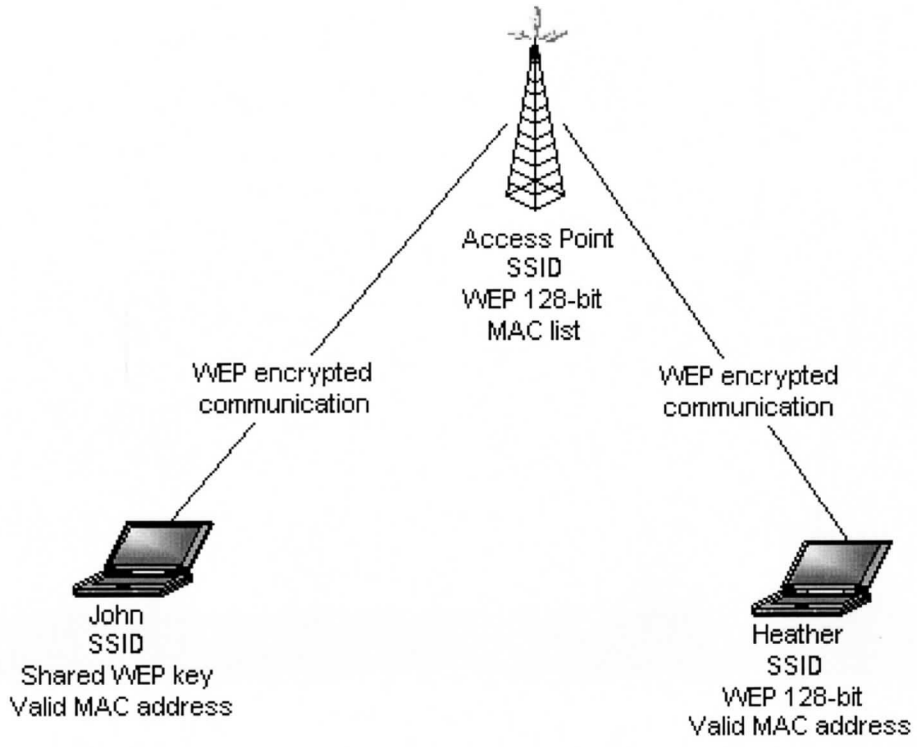

Source
Destination
RTS – Request to Send
CTS – Clear to Send
DATA
AC
K
Application
Presentation
Session
Transport
Network
802.11b
Data Link
Physical
802.11 MAC header
802.11 PLCP header

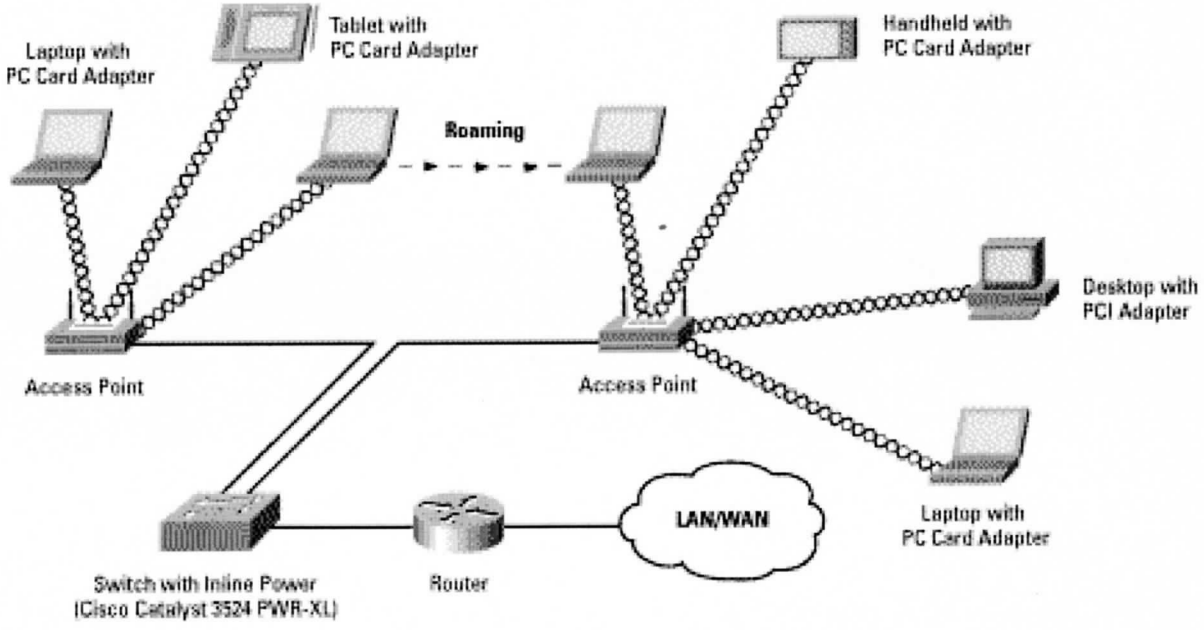

Ethernet Packet Structure
Destination address (6 bytes)
Protocol (2 bytes)
Payload (46-1,500 bytes)
Source address (6 bytes)
CRC (4 bytes)

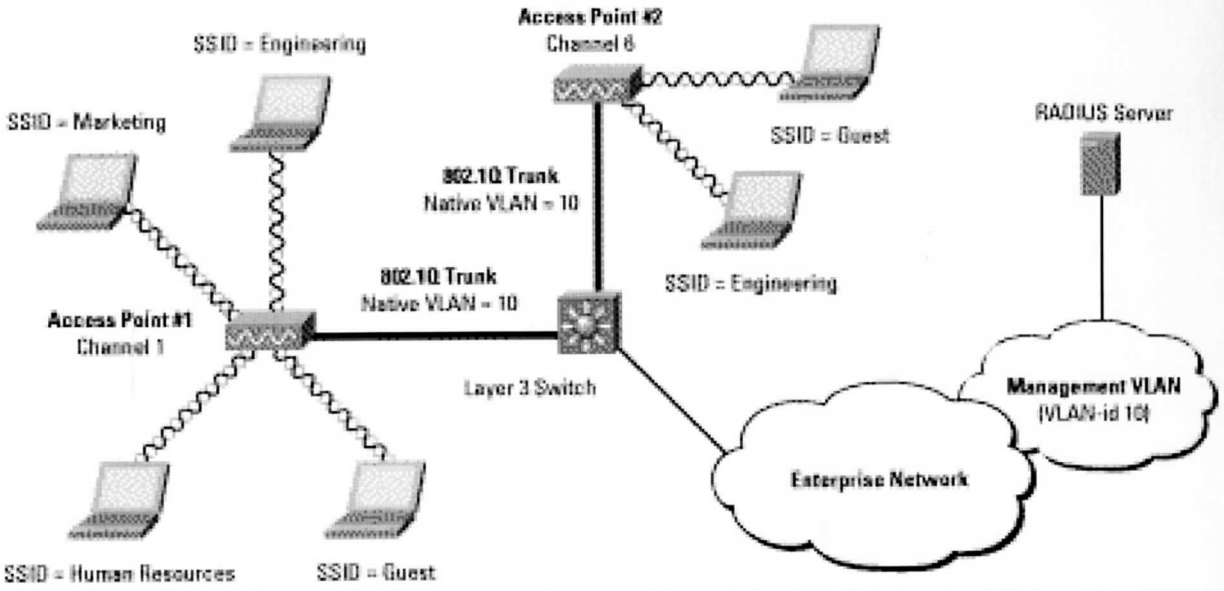

IEEE 802.11 Packet Structure
Duration ID (2 bytes)
Address 2 (6 bytes)
Sequence control (2 bytes)
Data (0-2,312 bytes)
Address 4 (6 bytes)
CRC (4 bytes)
Address 3 (6 bytes)
Address 1 (6 bytes)
Frame control (2 bytes)

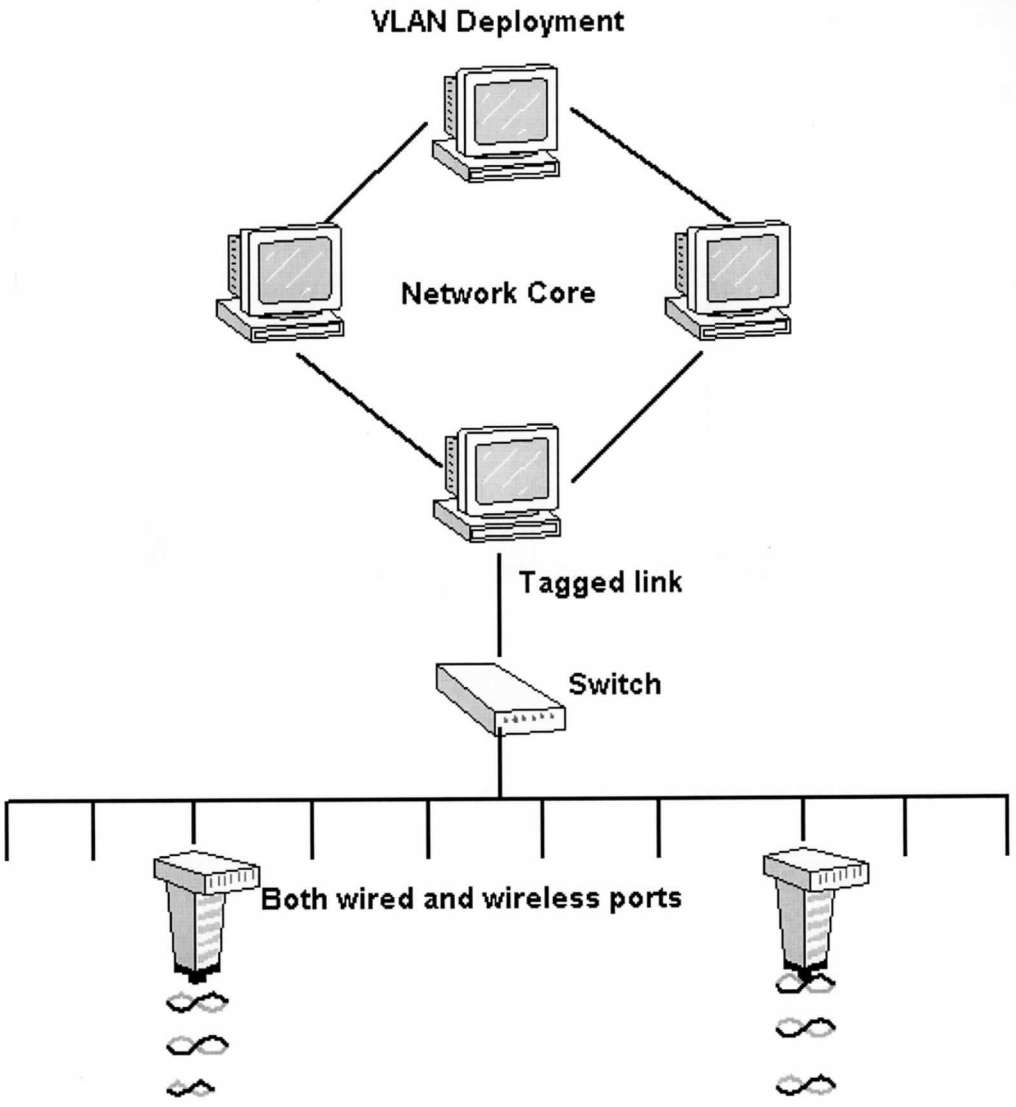

Ethernet PHY Frame
Interframe gap (96 bits)
Preamble (64 bits)
Payload (variable)


IEEE 802.11 PHY Frame Using DSSS
PLCP preamble
PLCP header
Synchronization (128 bits)
SFD (16 bits)
Signal (8 bits)
Service (8 bits)
Length (16 bits)
HEC (16 bits)
Payload (variable)


Access Point
SSID
WEP 128-bit
MAC list
WEP encrypted
communication
WEP encrypted
communication
John
SSID
Shared WEP key
Valid MAC address
Heather
SSID
WEP 128-bit
Valid MAC address


Laptop with
PC Card Adapter
Tablet with
PC Card Adapter
Handheld with
PC Card Adapter
Roaming
Desktop with
PCI Adapter
Access Point
Access Point
LAN/WAN
Laptop with
PC Card Adapter
Switch with Inline Power
(Cisco Catalyst 3524 PWR-XL)
Router


Access Point #2
Channel 6
SSID = Engineering
SSID = Marketing
SSID = Guest
RADIUS Server
802.1Q Trunk
Native VLAN = 10
802.1Q Trunk
Native VLAN = 10
SSID = Engineering
Access Point #1
Channel 1
Layer 3 Switch
Management VLAN
(VLAN-id 10)
Enterprise Network
SSID = Human Resources
SSID = Guest


VLAN Deployment
Network Core
Tagged link
Switch
Both wired and wireless ports

Missouri Valley College campus Backbone Network Description

There are 20 buildings both academic and residential buildings.

Academic buildings

Baity Hall

Collins Science Center

Ferguson Center

Mabee Memorial Chapel

Murrell Memorial Library

Morrison Fine Arts Center

Burns Multi-Purpose Center

Stadium Stands

Residential buildings

McDonald Hall

Young Hall

Sigma Nu House

Tau Kappa Epsilon

Alpha Sigma Phi House

Moreland Hall

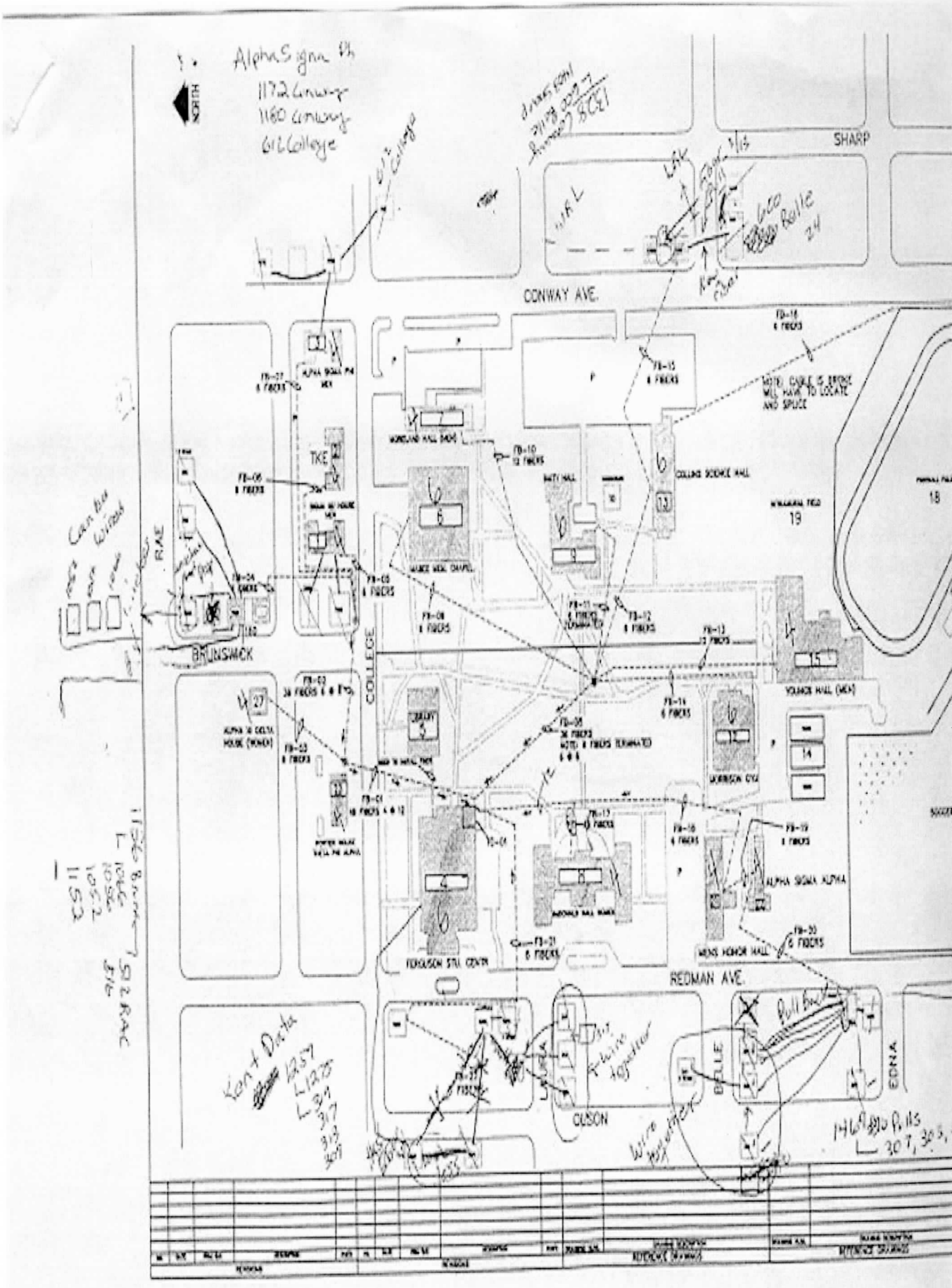
Newhard House

Men's Honor Hall

Alpha Sigma Alpha Sigma

Porter Hall

Saline Hall


NORTH
CONWAY AVE.
SHARP
COLLEGE
BRUNSWICK
REDMAN AVE.
OLSON
BELLE
EDNA
TKE
FERGUSON STU CENTER
ALPHA SIGMA ALPHA

Notes about the layout

- Campus buildings are connected to one of the core locations via multimode fiber, typically at 100M/bit full duplex.
- The main server center is housed in the Ferguson Center.
- Fifty concurrent dial-in server capability with an 800/888 access is present.This system allows remote access for commuter students and after hour access by faculty and staff.
- Operating system are Microsoft 2000 server and any UNIX variant.

TCP/IP addresses are allocated to all campus connected devices and delivered via DHCP backed by a home grown web registration application with a SQL database backend. With Cajun 333T and 334T Gigabit Ethernet switches, which handle all IP routing, the switch ports are configured to determine which workstations and workgroups can talk to which VLANs. VLANs divide the network into logical workgroups, mainly faculty, student and university administration. VLAN tagging technology is used, which allows a switch port or server to be configured to support multiple VLANs Gigabit Ethernet VLANs create IP-based workgroups based on physical connections. These workgroups are invisible to one another even though they run on the same physical network. VLAN tagging lets workgroups share peripherals and servers.

If a student is assigned only to the student computer laboratory on VLAN #10, for instance, he or she can't stray from the confines of that lab network. Even if a rogue

student somehow captured the Ethernet switch's IP address and password, he or she still couldn't reach the switch itself or a VLAN of which the student wasn't a member, such as a faculty VLAN.

VLAN establishment and configuration using Cajun View

Console into the switch by attaching the workstation serial port to the switch console port with a rollover cable

View / Configure the IP address and subnet mask for the switch

Assign an IP address and subnet mask to the switch. Be sure to use an IP address and subnet mask that are compatible with the network or subnet the switch is currently on. If the switch is connected to Router Lab-A, Interface E1 as shown in the standard lab setup diagram, then assign a compatible IP address and subnet mask to the switch.

IP Address: 192.5.5.2 Subnet Mask: 255.255.255.0

] List VLAN's Enter VLAN numbers: [M] Modifiy VLAN Select a VLAN [1-1005]: [E] VLAN Membership Catalyst 1900 - VLAN Membership

Connect the workstation to the switch with a straight-through CAT5 Ethernet cable using port 12 on the switch. Verify that the workstation has IP address, Subnet Mask and Default Gateway settings that are compatible with the switch and router. Telnet to the switch from the workstation DOS prompt

telnet 192.5.5.2

To connect a PC terminal or VT-100 terminal to the Cajun P330

1. If you are using a PC, initiate a VT-100 terminal emulation session using an application such as Windows® HyperTerminal.

2. Press Enter.

- The Welcome to Cajun P330 menu is displayed.

3. Type the User name root when prompted and press Enter.

4. Type the default password root when prompted and press Enter.

- The Cajun_P330-N(super)# prompt appears
- N is the number of the switch in the stack.

Assigning the Stack IP Address

- Commands are shown as follows: set interface inband;

parameters which you need to enter are shown in <> as follows: <*vlan*>

1. Type set interface inband <*vlan*> <*ip_address*> <*netmask*>

replacing <*vlan*>, <*ip_address*> and <*netmask*> with the VLAN, IP address and net mask of the stack and press Enter.

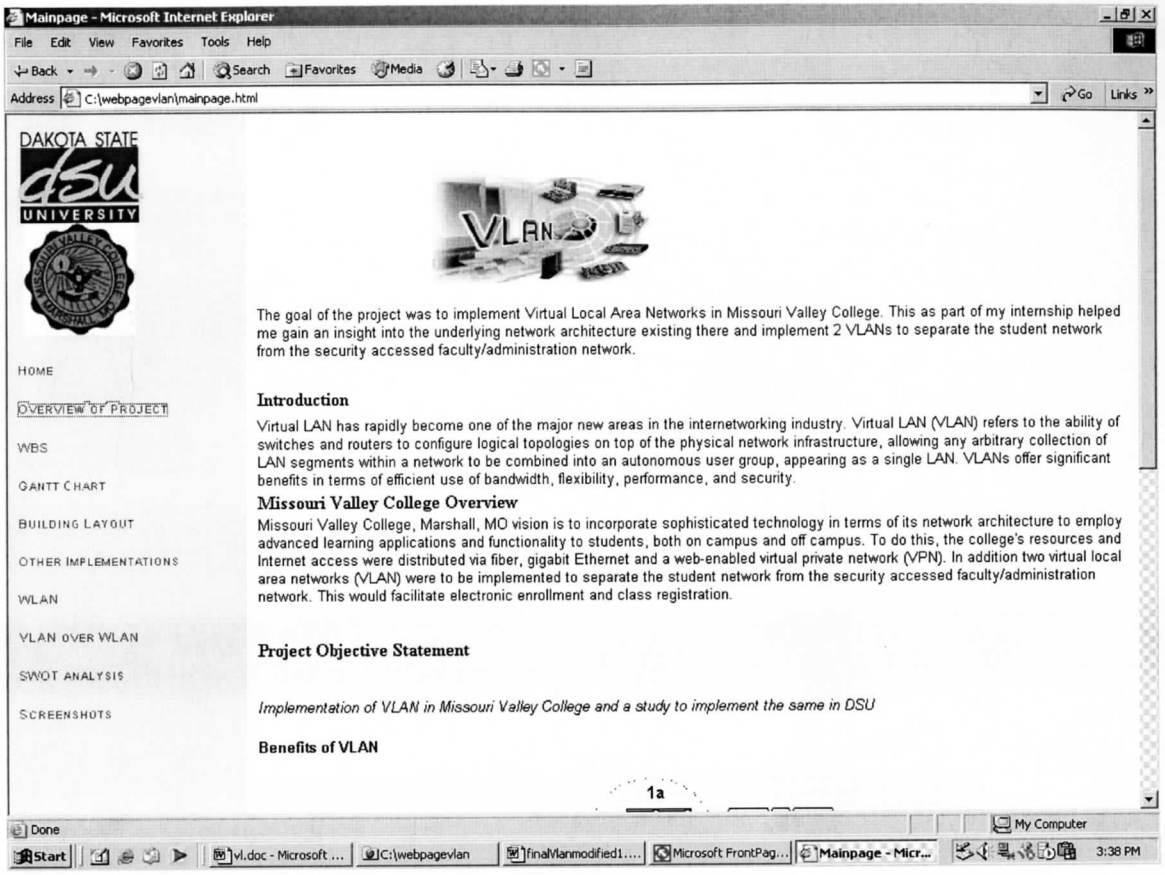
2. Type reset and press Enter to reset the stack.

3. After the Reset, perform login again as described above.

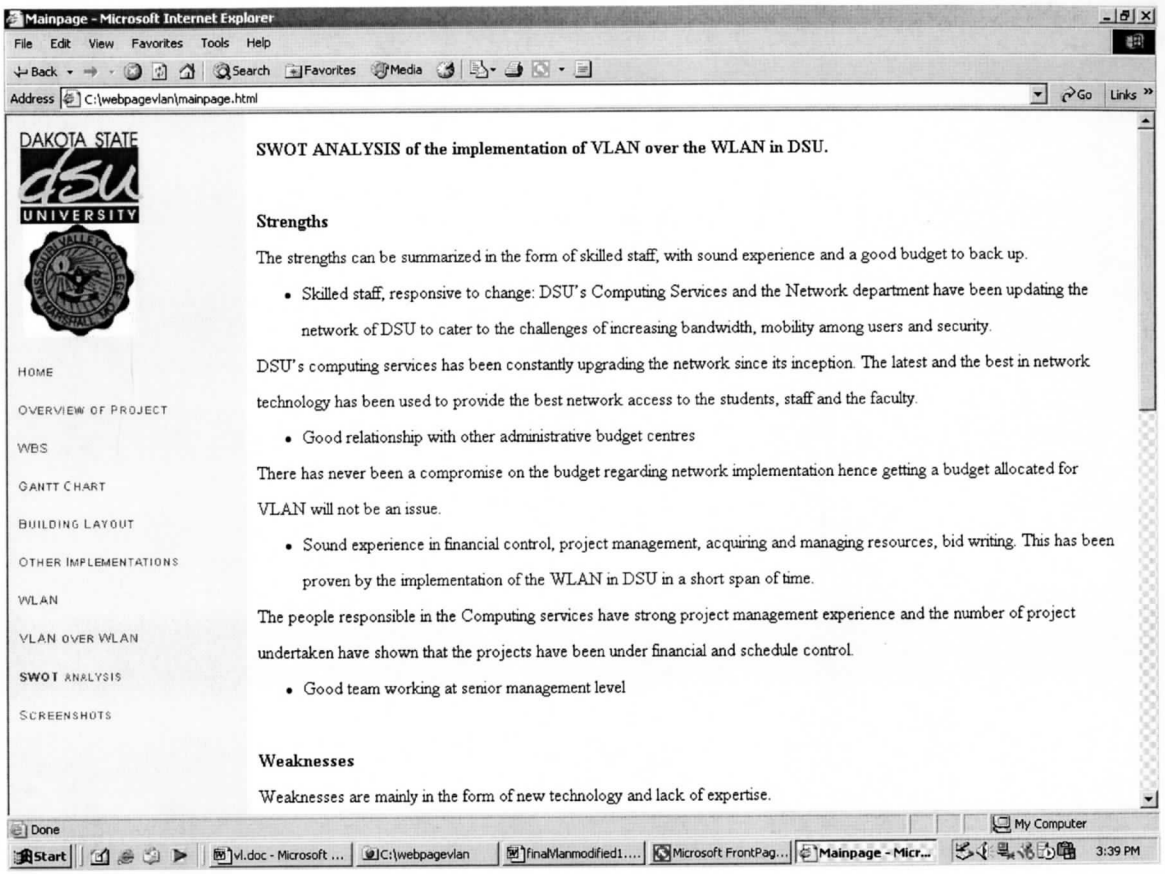
- The Cajun_P330-N(super)# prompt appears.

4. Type set ip route <*destination*> <*gateway*>, replacing <*destination*> and <*gateway*> with the destination and gateway IP addresses.

5. Press Enter to save the destination and gateway IP addresses.



Screenshot of the website


Mainpage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\webpagevlan\mainpage.html
Go Links
DAKOTA STATE
dsu
UNIVERSITY
HOME
OVERVIEW OF PROJECT
WBS
GANTT CHART
BUILDING LAYOUT
OTHER IMPLEMENTATIONS
WLAN
VLAN OVER WLAN
SWOT ANALYSIS
SCREENSHOTS
SWOT ANALYSIS of the implementation of VLAN over the WLAN in DSU.
Strengths
The strengths can be summarized in the form of skilled staff, with sound experience and a good budget to back up.
• Skilled staff, responsive to change: DSU's Computing Services and the Network department have been updating the network of DSU to cater to the challenges of increasing bandwidth, mobility among users and security.
DSU's computing services has been constantly upgrading the network since its inception. The latest and the best in network technology has been used to provide the best network access to the students, staff and the faculty.
• Good relationship with other administrative budget centres
There has never been a compromise on the budget regarding network implementation hence getting a budget allocated for VLAN will not be an issue.
• Sound experience in financial control, project management, acquiring and managing resources, bid writing. This has been proven by the implementation of the WLAN in DSU in a short span of time.
The people responsible in the Computing services have strong project management experience and the number of project undertaken have shown that the projects have been under financial and schedule control.
• Good team working at senior management level
Weaknesses
Weaknesses are mainly in the form of new technology and lack of expertise.
Done
My Computer
Start
vl.doc - Microsoft ...
C:\webpagevlan
finalManmodified1....
Microsoft FrontPag...
Mainpage - Micr...
3:39 PM