NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

Local Area Network Switches Techniques and Security Management

Graduation Project
COM 400

Student : MOH'D RIFAT ALKHAIRY(990972)

Supervisor:Mr. Halil Adahan

Nicosia – 2003

Acknowledgement

This work would have not been possible without the active cooperation, patience and encouragement of my Tutor Dr. Halil Adahan who not only guided me successfully in my research work but also provided me a great environment that made my work smooth and bearable, in addition he helped me with valuable comments and knowledge that improved the quality of my thesis.

My praise for Dr. Halil can not be expressed in one page.

Overall my study years were tough but nice at the same time. I would like to thank my parents, friends, and my beautiful girlfriend for always supporting me in all my joys and disappointments of graduate experience. I will always be grateful to them for their blessings on my graduate degree.

In addition I am grateful to all my educational staff who gave me their efforts and knowledge whenever I landed in problems.

ABSTRACT

This reports gives solid coverage and explanation of the structure of LAN design considerations and how to gain the knowledge to design, implement and maintain a network so that it will meet the needs for today's networks and for future technologies. Great for the networking novice.

In addition to explain the technology and principles of VLANs and Gigabit Ethernet and explores implications for its application and operation in LANs. Tells how to identify appropriate application environments for this technology and how to integrate it with other technologies such as OSI, choose products and features, and set realistic expectations about performance. Of interest to anyone involved with LAN technologies, such as network planners and administrators, application developers, technical salespeople, and students in advanced courses on LAN.

On the other hand the rapid increase in Internet connections has caused a dramatic rise in the technological and administrative difficulties experienced by LAN and WAN users and managers as they try to meet the demand for intercompatibility between advanced systems. This report talks about these challenges by covering the latest technological advancements, including LAN security, system software,application software,viruses ,data security and layer's systems. Provides extensive information on wiring systems, devices and management, covering both copper and fiber cabling for all types of LAN topologies, including Ethernet, Fast Ethernet, Token-Ring,

TABLE OF CONTENTS

CHAPTER ONE

Local Area Networks

1.1 Introduction

Computer networks interconnect sets of autonomous computers, providing the means by which data can be dispatched from one computer for delivery to one or more of the other machines on the network. Exchange of information paves the way for resource sharing. Application programs and data sets stored on file servers can be made available to users of other network-attached computers; likewise, hardware devices, ranging from laser printers to back-up systems to communications gateways, can process data from other network machines.

By definition, LANs connect computers situated within a relatively small geographical area, such as a building or campus. Given a small site, topological constraints can be imposed to allow computers to be interconnected by a shared communication medium over which data is broadcast so that every computer which is connected to that medium receives the data. Each packet contains the address(es) of the destination computer(s). Computers check the destination address and ignore packets intended for other computers. If a shared medium is to carry all of the network traffic, it must be relatively high speed. Since LANs are small and normally owned by a single institution, the cost and legal constraints which force most long-haul networks to use the public telephone carriers do not apply. Institutions are able to install their own LANs, and normally choose to do so using transmission media which are both high speed and highly reliable. This means that LAN protocols can be simpler than wide area network (WAN) protocols since there is less need to maximise performance and minimise errors. On the other hand, it is no good trying to "scale-up" LAN technology beyond its intended topological limits; global communication would be impossible if every networked computer in the world had to be sent every data packet. Because of the inherent differences between them, careful planning is needed to ensure that WANs, such as JANET (the UK's Joint Academic NETwork), and LANs can be interconnected.

1.2 What Is a LAN?

A LAN is a high-speed data network(meduim allows a high bit transmission rate) that covers a relatively small geographic area(ex within a building). It typically connectspersonal computers, workstations, printers, servers, and other devices, LANs are connected by permanent cables that allow rapid data transfer. A LAN will generally comprise several personal computers, shared peripheral devices such as printers and scanners, and a central file server with high capacity disk storage. A network server stores data and programs that can be used and shared by any computer linked to the LAN (subject to users having access rights), Most LANs, as mentioned above. Node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data.

1.3 How does LAN Operate?

A LAN requires special operating system software to allow the various devices connected to the LAN to communicate with each other.As Lan follows the rule of server-client networkes,the server must have the power to operate strongly within the network.This strongness and effictevness of the server lies in the precense of a strong operating system ex:-windows NT ,windows 2000 may be also used.

Local area network (LAN) could use any topology for connection ,bus topology is useto connect the pc's together ,and the information and data are stored in the file system(FS) , these file servers contain the software necessary to implement a wide area networks(WAN) through connections of LAN'S together ,taking into attention that any cooruptions in the FS may cause a troubleshoot(problems) in connecting LAN'S.

1.4 What is a LAN Network Operating System?

Unlike operating systems, such as DOS and Windows95, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

1.4.1 Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems.

Figure1.1 : Peer-to-Peer Network

1.4.1.1 Advantages of a Peer-to-Peer Network:

Less initial expense - No need for a dedicated server.

Setup - An operating system (such as Windows 95) already in place may only need to be reconfigured for peer-to-peer operations.

1.4.1.2 Disadvantages of a Peer-to-Peer Network:

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network.

1.4.2 Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers . The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware and Windows NT Server are examples of client/server network operating systems.

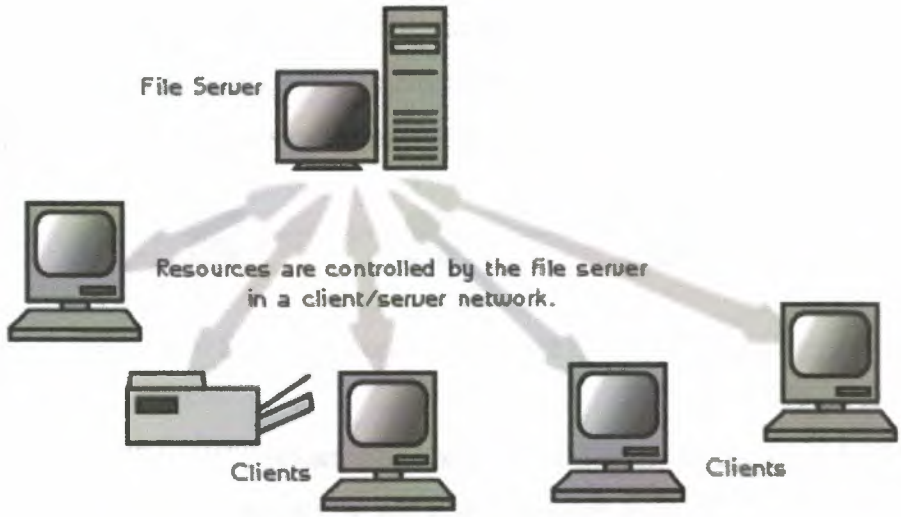

Figure 1.2: Client/Server Network

1.4.2.1 Advantages of a Client/Server Network:

1. Centralized - Resources and data security are controlled through the server.
2. Scalability - Any or all elements can be replaced individually as needs increase.
3. Flexibility - New technology can be easily integrated into system.
4. Interoperability-All components (client/network/server) work together.
5. Accessibility - Server can be accessed remotely and across multiple platforms.

1.4.2.2 Disadvantages of a Client/Server Network:

1. Expense - Requires initial investment in dedicated server.
2. Maintenance - Large networks will require a staff to ensure efficient operation.
3. Dependence - When server goes down, operations will cease across the network.

1.5 LAN Topologies and Media

The physical layout of the LAN is called Network Topology. Common LAN topologies are Ring, Bus, Tree, and Star.LAN topologies define the manner in which network devices are organized,and their architecture in which they are implemented in real life. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

1.5.1 Bus Topology

A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks--- , including 100BaseT---, implement a bus topology, which is illustrated in Figure 1.3

Figure1.3: Some networks implement a local bus topology.

With the Bus topology, all workstations are connect directly to the main backbone that carries the data. Traffic generated by any computer will travel across the backbone and be received by all workstations. This works well in a small network of 2-5 computers, but as the number of computers increases so will the network traffic and this can greatly decrease the performance and available bandwidth of your network.

1.5.1.1 Advantages of Bus Topology

1. Easy to connect a computer or peripheral to a linear bus.
2. Requires less cable length than a star topology.

1.5.1.2 Disadvantages of a Bus Topology

1. Entire network shuts down if there is a break in the main cable.
2. Terminators are required at both ends of the backbone cable.
3. Difficult to identify the problem if the entire network shuts down.
4. Not meant to be used as a stand-alone solution in a large building.

1.5.2 Star Topology

A star topology is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology, which is illustrated in Figure(1.4) .

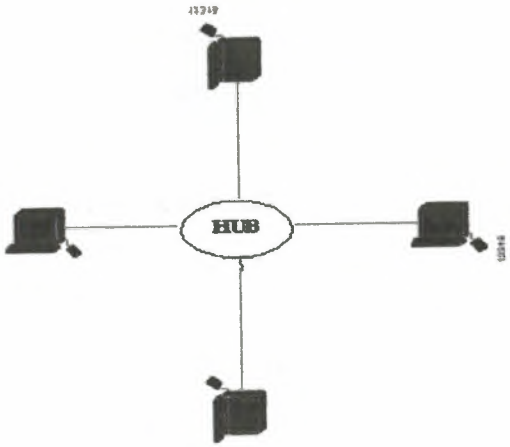

Figure1.4 : star LANS

All stations are attached by cable to a central point, usually a wiring hub or other device operating in a similar function. In the star topology, the information or data is sent through cables as signals to the central hub,which gives the access ability to all worstations connected to the hub.

Several different cable types can be used for this point-to-point link, such as shielded twisted-pair (STP), unshielded twisted-pair (UTP), and fiber-optic cabling. Wireless media can also be used for communications links.

1.5.2.1 Advantages of a Star Topology

1. Easy to install and wire.
2. No disruptions to the network then connecting or removing devices.
3. Easy to detect faults and to remove parts.
4. no cable segment is a single point of failureimpacting the entire network.

1.5.2.2 Disadvantages of a Star Topology

1. Requires more cable length than a linear topology.
2. If the hub or concentrator fails, nodes attached are disabled.
3. More expensive than linear bus topologies because of the cost of the concentrators

Mentioning the last advantage of the star topology is that no cable segment is a single point of failure impacting the entire network. This allows for better management of the LAN. If one of the cables develops a problem, only that LAN-attached station is affected; all other stations remain operational.

1.5.3 Ring Topology

A ring topology is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology. Figure depicts a logical ring topology,in ring topology one of the pc's connected on the network transmittes a signal, this signal circles through the closed loop and is then copied by the intended destination network node. The signal is then absorbed by the original station that transmitted the signal.

Figure 1.5 : Some networks implement a logical ring topology.

Token Ring (IEEE 802.5) best represents a ring topology. Although the physical cabling is considered to be a star topology, Token Ring is a ring in logical topology, as

demonstrated by the following figures. Although physical topology is a physical layer attribute, the media access method used at the data link layer determines the logical topology. Token Ring defines a logical ring and contention, as Ethernet defines a logical bus. Even when attached to a hub, when one Ethernet device transmits, everyone hears the transmission, just as though on a bus.

1.5.4 Tree Topology

A tree topology is a LAN structure that is identical to the bus topology, except that branches with multiple nodes are possible in this case. Figure 1.6 illustrates a logical tree topology. The protocols used with star configurations are usually Ethernet or LocalTalk. Token Ring uses a similar topology, called the star-wired ring.

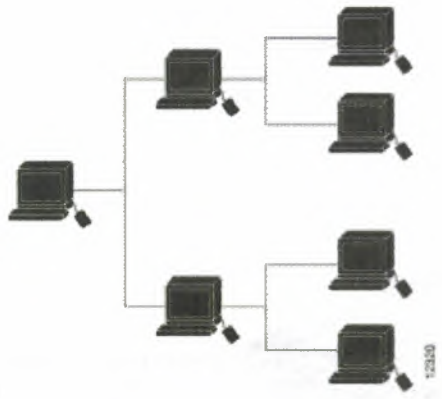

Figure1.6 : A logical tree topology can contain multiple nodes.

1.5.4.1 Advantages of a Tree Topology

1. Point-to-point wiring for individual segments.
2. Supported by several hardware and software vendors.

1.5.4.2 Disadvantages of a Tree Topology

1. Overall length of each segment is limited by the type of cabling used.
2. If the backbone line breaks, the entire segment goes down.
3. More difficult to configure and wire than other topologies

1.6 LAN Cabling

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

1.6.1 Twisted Pair

1.6.1.1 Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for small networks (See Fig. 1.7).

Figure1.7 : Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Categories of Unshielded Twisted Pair

Type	Use
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

1.6.1.2 Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 1.8). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Figure1.8 : unshielded twisted pair connector

1.6.1.3 Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

1.6.2 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig.1.9). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

Figure1.9 : Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial. Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks, especially linear bus networks. Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 1.10). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

Figure1.10: connector for coaxial cabling

1.6.3 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 1.11). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

Figure1.11 : Fiber optic cable

Facts about fiber optic cables:

- Outer insulating jacket is made of Teflon or PVC.
- Kevlar fiber helps to strengthen the cable and prevent breakage.
- A plastic coating is used to cushion the fiber center.
- Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

1.7 Devices Connected to LAN

1.7.1 Hubs

A hub is a physical layer device that connects multiple user stations, each via a edicated cable. The purpose of a hub is to regenerate and retime network signals. This is done at the bit level to a large number of hosts (e.g. 4, 8, or even 24) using a process known as concentration. You will notice that this definition is very similar to the repeater's, which is why a hub is also known as a multi-port repeater. The difference is the number of cables that connect to the device. Two reasons for using hubs are to create a central connection point for the wiring media, and increase the reliability of the network. The reliability of the network is increased by allowing any single cable to fail without disrupting the entire network. This differs from the bus topology where having one cable fail will disrupt the entire network. Hubs are considered Layer 1 devices because they only regenerate the signal and broadcast it out all of their ports (network connections). A hub is used in as ethernet conjunction with 10BaseT and 100BaseT cables. The cables run from the network's computers to ports on the hub. Using a hub makes it easier to move or add computers, find and fix cable problems, and remove computers temporarily from the network (if they need to be upgraded, for instance).

There are different classifications of hubs in networking. The first classification is active or passive hubs. Most modern hubs are active; they take energy from a power supply to regenerate network signals. Some hubs are called passive devices because they merely split the signal for multiple users, like using a "Y" cord on a CD player to use more than one set of headphones. Passive hubs do not regenerate bits, so they do not extend a cable's length, they only allow two or more hosts to connect to the same cable segment.

Another classification of hubs is intelligent or managed(dump). This classification is explained below:

1.7.2 Repeaters

A repeater is a physical layer device used to interconnect the media segments of an extended network.

A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment. These actions prevent signal deterioration caused by long cable lengths and large numbers of connected devices. Repeaters are incapable of performing complex filtering and other traffic processing.

In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified.

The total number of repeaters and network segments that can be connected is limited due to timing and other issues.

1.7.3 Bridging

This section focuses on transparent bridges, which can also be referred to as learning or Ethernet bridges. Bridges have a physical layer (Layer 1), but are said to operate at the data link layer (Layer 2) of the OSI model. Bridges forward data frames based on the destination MAC address. Bridges also forward frames based on frame header information. Bridges create multiple collision domains and are generally deployed to provide more useable bandwidth. Bridges don't stop broadcast traffic; they forward broadcast traffic out every port of each bridge device. Each port on a bridge has a separate bandwidth (collision) domain, but all ports are on the same broadcast domain.

Bridges were also deployed in complex environments, which is where broadcast storms became such a problem.

Routers were added to the complex bridged environments to control broadcasts. Later, VLANs were devised when switches were deployed in enterprise environments and brought back the old problem of broadcast storms.

Note that Bridges, like repeaters, do not modify traffic. Unlike repeaters, bridges can originate traffic in the form of spanning tree bridge protocol data units (BPDUs).

Bridges maintain a MAC address table, sometimes referred to as a content addressable memory (CAM) or bridging table, which maintains the following information:

- MAC addresses
- Port assignment

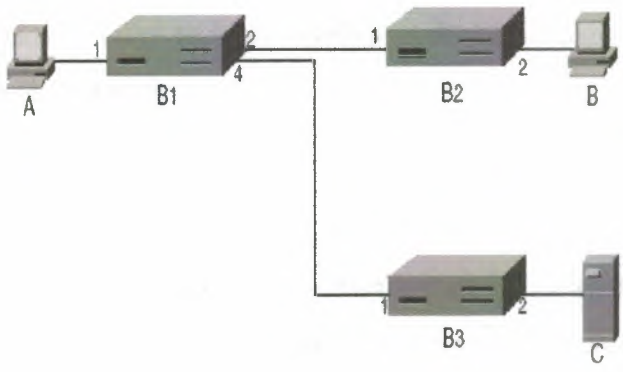

Figure 1.12 :Simple Bridge Network

The original all-ports broadcast of A's first frame to B ensures that B3 knows how to send to frames to A. An attempt by C to communicate with B results in B3 broadcasting the frame on all ports (except number 2), so the frame reaches B1 on port 4. While B1 forwards this frame to B2, it also learns what to do with frames destined for C.

1.7.4 Routers

A router is a Layer 3 device. Working at Layer 3 allows the router to make decisions based on groups of network addresses (Classes) as opposed to individual Layer 2 MAC addresses. Routers can also connect different Layer 2 technologies, such as Ethernet, Token-ring, and FDDI. However, because of their ability to route packets based on

Layer 3 information, routers have become the backbone of the Internet, running the IP protocol.

The purpose of a router is to examine incoming packets (Layer 3 data), choose the best path for them through the network, and then switch them to the proper outgoing port. Routers are the most important traffic-regulating devices on large networks. They enable virtually any type of computer to communicate with any other computer anywhere in the world! While performing these basic functions, routers can also execute many other tasks that are covered in later chapters.

In networking, there are two addressing schemes: one uses the MAC address, a data link (Layer 2) address; the other uses an address located at the network layer (Layer 3) of the OSI model. An example of a Layer 3 address is an IP address. A router is a type of internetworking device that passes data packets between networks, based on Layer 3 addresses. A router has the ability to make intelligent decisions regarding the best path for delivery of data on the network.

1.8 LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast.In each type of transmission, a single packet is sent to one or more nodes.

The three classification of local area network transmission methods,are explained below,showing how data is transfered from one machine into another.

1.8.1 Unicasting

With unicast transmissions, a single packet is sent from the source to a destination on a network. The source-node addresses the packet by using the network address of the destination node. The packet is then forwarded to the destination network and the network passes the packet to its final destination. Figure 1.13 is an example of a unicast network.

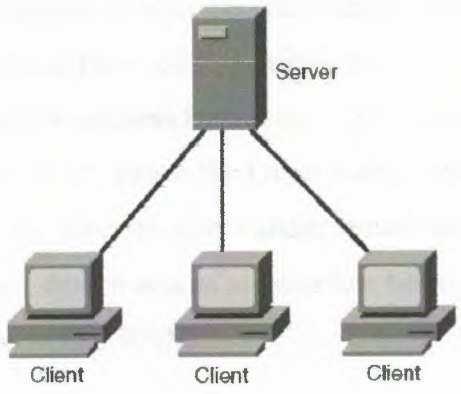

Figure1.13: Unicast Network

1.8.2 Multicasting

With a multicast transmission, a single data packet is copied and forwarded to a specific subset of nodes on the network. The source node addresses the packet by using a multicast address. For example, the TCP/IP suite uses 224.0.0.0 to 239.255.255.255. The packet is then sent to the network, which makes copies of the packet and sends a copy to each segment with a node that is part of the multicast address. Figure 1.14 is an example of a multicast network.

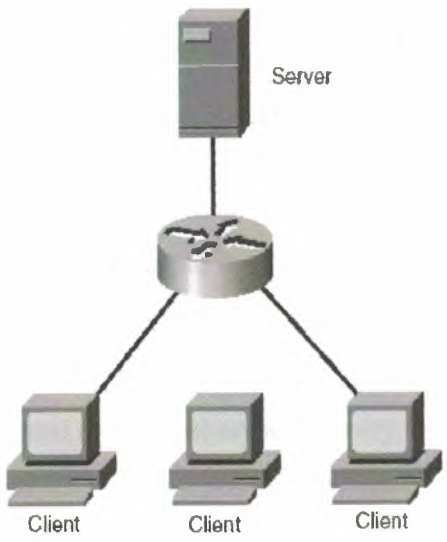

Fig 1.14 : Multicasted Network

1.8.3 Broadcasting

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address.Broadcasts are found in LAN environments. Broadcasts do not traverse a WAN unless the Layer 3 edge-routing device is configured with a helper address (or the like) to direct these broadcasts to a specified network address. This Layer 3 routing device acts as an interface between the local-area network (LAN) and the wide-area network (WAN).

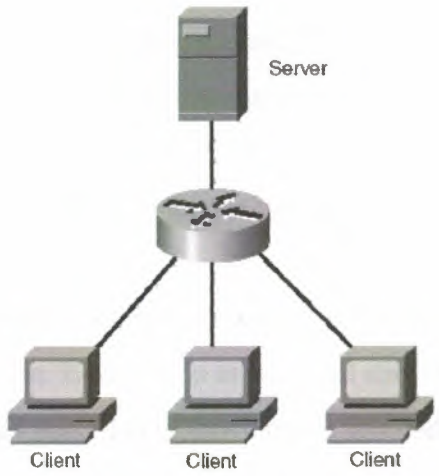

Figure 1.15 : Broadcated Transmission

1.9 Some Advantages and Disadvantages of LAN

Some of the advantages and disadvantages of LAN networks are listed below:

1. Shared access to devices and;
2. **Speed**. Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, then carrying or sending the disks from one computer to another. This method of transferring files (referred to as sneaker-net) is very time-consuming.
3. **Cost**. Networkable versions of many popular software programs are available at considerable savings when compared to buying individually licensed copies. Besides monetary savings, sharing a program on a network allows for easier upgrading of the program. The changes have to be done only once, on the file server, instead of on all the individual workstations.

4. **Security.** Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.
5. **Centralized Software Management.** One of the greatest benefits of installing a network at a school is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.
6. **Resource Sharing.** Sharing resources is another area in which a network exceeds stand-alone computers. Most schools cannot afford enough laser printers, fax machines, modems, scanners, and CD-ROM players for each computer. However, if these or similar peripherals are added to a network, they can be shared by many users.
7. **Electronic Mail.** The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids in personal and professional communication for all school personnel, and it facilitates the dissemination of general information to the entire school staff. Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school. If the LAN is connected to the Internet, students can communicate with others throughout the world.
8. **Flexible Access.** School networks allow students to access their files from computers throughout the school. Students can begin an assignment in their classroom, save part of it on a public access area of the network, then go to the media center after school to finish their work. Students can also work cooperatively through the network.
9. **Workgroup Computing.** Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.
10. **Shared access to devices and applications.**

1.10 Disadvantages of LAN

1. **Expensive to Install.** Although a network will generally save money over time, the initial costs of lan installation can be prohibitive. Cables, network cards, and software are expensive, and the installation may require the services of a technician.
2. **Requires Administrative** Time. Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.
3. **File Server May Fail.** Although a file server is no more susceptible to failure than any other computer, when the files server "goes down," the entire network may come to a halt. When this happens, the entire school may lose access to necessary programs and files.
4. **Cables May Break.** The Topologies present information about the various configurations of cables. Some of the configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can stop the entire network.

1.11 Other Implemented Data Networks

1.11.1 Metropolitan Area Network

A Metropolitan Area Network (MAN) covers larger geographic areas, such as cities or school districts. By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries.

One example of a MAN is the MIND Network located in Pasco County, Florida. It connects all of Pasco's media centers to a centralized mainframe at the district office by using dedicated phone lines, coaxial cabling, and wireless communications providers.

1.11.2 Wide Area Network

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network.

Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of minutes, without paying enormous phone bills. A WAN is complicated. It uses multiplexers to connect local and metropolitan networks to global communications

networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN or a MAN.

CHAPTER TWO

2.1 Chapter Goals

1. Understand the relationship of LAN switching to legacy internetworking devices such as bridges and routers.
2. Understand the advantages of VLANs.
3. Know the difference between access and trunk links.
4. 4-Know the purpose of a trunk protocol.
5. Understand Layer 3 switching concepts.
6. Describe the guidlines and distance limitatios of fast ethernet .
7. Distinguish between cut and store and forward lan switches .

2.2 History

The earliest LAN switches were developed in 1990. They were Layer 2 devices (bridges) dedicated to solving desktop bandwidth issues. Recent LAN switches evolved to multilayer devices capable of handling protocol issues involved in high-bandwidth applications that historically have been solved by routers. Today, LAN switches are used to replace hubs in the wiring closet because user applications demand greater bandwidth.

2.3 LAN Switching and VLANs

A LAN switch is a device that provides much higher port density at a lower cost than traditional bridges. For this reason, LAN switches can accommodate network designs featuring fewer users per segment, thereby increasing the average available bandwidth per user. This chapter provides a summary of general LAN switch operation and maps LAN switching to the OSI reference model.

The trend toward fewer users per segment is known as microsegmentation. Micro-segmentation allows the creation of private or dedicated segments , One user per segment. Each user receives instant access to the full bandwidth and does not have to contend for available bandwidth with other users. As a result, collisions (a normal phenomenon in shared-medium networks employing hubs) do not occur, as long as the equipment operates in full-duplex mode. A LAN switch forwards frames based on

either the frame's Layer 2 address (Layer 2 LAN switch) or, in some cases, the frame's Layer 3 address (multilayer LAN switch). A LAN switch is also called a frame switch because it forwards Layer 2 frames, whereas an ATM switch forwards cells.

Figure 2.1 :illustrates a LAN switch providing dedicated bandwidth to devices and illustrates the relationship of Layer 2 LAN switching to the OSI data link layer.

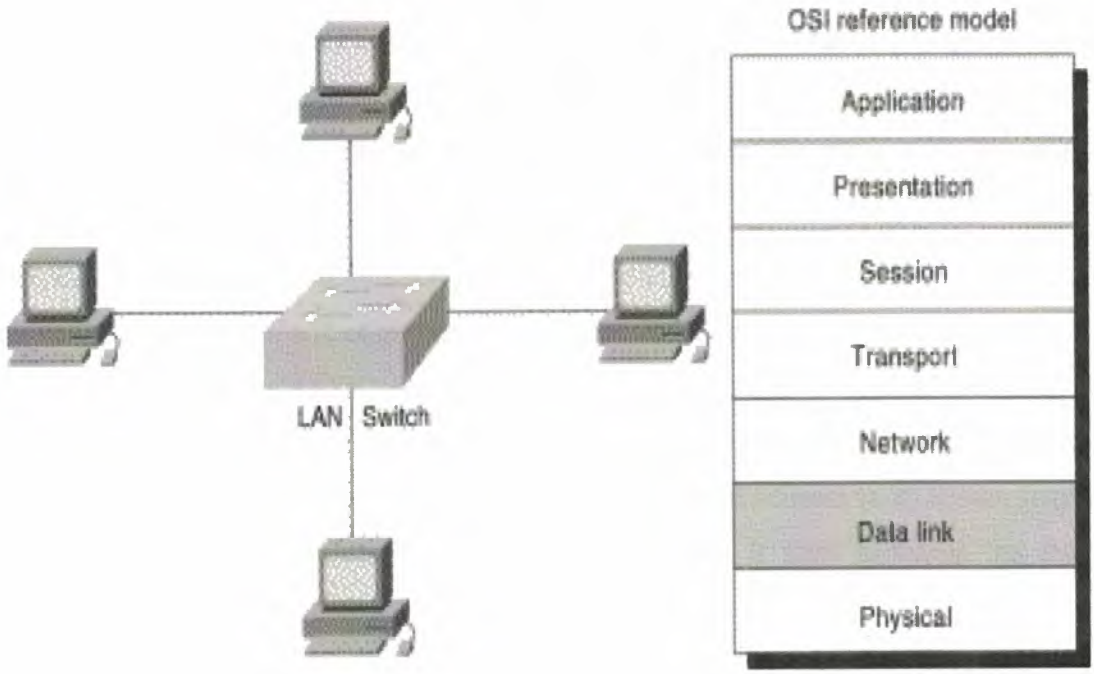

Figure 2.1: A LAN Switch Is a Data Link Layer Device

2.4 LAN Switch Operation

LAN switches are similar to transparent bridges in functions such as learning the topology, forwarding, and filtering. These switches also support several new and unique features, such as dedicated communication between devices through full-duplex operations, multiple simultaneous conversations, and media-rate adaption.

Full-duplex communication between network devices increases file-transfer throughput. Multiple simultaneous conversations can occur by forwarding, or switching, several packets at the same time, thereby increasing network capacity by the number of conversations supported. Full-duplex communication effectively doubles the throughput, while with media-rate adaption, the LAN switch can translate between 10 and 100 Mbps, allowing bandwidth to be allocated as needed.

Deploying LAN switches requires no change to existing hubs, network interface cards (NICs), or cabling.

2.5 LAN Switching Forwarding

LAN switches can be characterized by the forwarding method that they support. In the store-and-forward switching method, error checking is performed and erroneous frames are discarded. With the cut-through switching method, latency is reduced by eliminating error checking.

With the store-and-forward switching method, the LAN switch copies the entire frame into its onboard buffers and computes the cyclic redundancy check (CRC). The frame is discarded if it contains a CRC error or if it is a runt (less than 64 bytes, including the CRC) or a giant (more than 1518 bytes, including the CRC). If the frame does not contain any errors, the LAN switch looks up the destination address in its forwarding, or switching, table and determines the outgoing interface. It then forwards the frame toward its destination.

With the cut-through switching method, the LAN switch copies only the destination address (the first 6 bytes following the preamble) into its onboard buffers. It then looks up the destination address in its switching table, determines the outgoing interface, and forwards the frame toward its destination. A cut-through switch provides reduced latency because it begins to forward the frame as soon as it reads the destination address and determines the outgoing interface.

Some switches can be configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached, when they automatically change to store-and-forward mode. When the error rate falls below the threshold, the port automatically changes back to store-and-forward mode.

LAN switches must use store-and-forward techniques to support multilayer switching. The switch must receive the entire frame before it performs any protocol-layer operations. For this reason, advanced switches that perform Layer 3 switching are store-and-forward devices.

2.6 LAN Switching Bandwidth

LAN switches also can be characterized according to the proportion of bandwidth allocated to each port. Symmetric switching provides evenly distributed bandwidth to each port, while asymmetric switching provides unlike, or unequal, bandwidth between some ports.

An asymmetric LAN switch provides switched connections between ports of unlike bandwidths, such as a combination of 10BaseT and 100BaseT. This type of switching is also called 10/100 switching. Asymmetric switching is optimized for client/server traffic flows in which multiple clients simultaneously communicate with a server, requiring more bandwidth dedicated to the server port to prevent a bottleneck at that port.

A symmetric switch provides switched connections between ports with the same bandwidth, such as all 10BaseT or all 100BaseT. Symmetric switching is optimized for a reasonably distributed traffic load, such as in a peer-to-peer desktop environment.

A network manager must evaluate the needed amount of bandwidth for connections between devices to accommodate the data flow of network-based applications when deciding to select an asymmetric or symmetric switch

2.7 LAN Switch and the OSI Model

LAN switches can be categorized according to the OSI layer at which they filter and forward, or switch, frames. These categories are: Layer 2, Layer 2 with Layer 3 features, or multilayer.

A Layer 2 LAN switch is operationally similar to a multiport bridge but has a much higher capacity and supports many new features, such as full-duplex operation. A Layer 2 LAN switch performs switching and filtering based on the OSI data link layer (Layer 2) MAC address. As with bridges, it is completely transparent to network protocols and user applications.

A Layer 2 LAN switch with Layer 3 features can make switching decisions based on more information than just the Layer 2 MAC address. Such a switch might incorporate some Layer 3 traffic-control features, such as broadcast and multicast traffic management, security through access lists, and IP fragmentation.

A multilayer switch makes switching and filtering decisions based on OSI data link layer (Layer 2) and OSI network layer (Layer 3) addresses. This type of switch dynamically decides whether to switch (Layer 2) or route (Layer 3) incoming traffic. A multilayer LAN switch switches within a workgroup and routes between different workgroups.

Layer 3 switching allows data flows to bypass routers. The first frame passes through the router as normal to ensure that all security policies are observed. The switches watch the way that the router treats the frame and then replicate the process for subsequent frames. For example, if a series of FTP frames flows from a 10.0.0.1 to 192.168.1.1, the frames normally pass through a router. Multilayer switching observes how the router changes the Layer 2 and Layer 3 headers and imitates the router for the rest of the frames. This reduces the load on the router and the latency through the network.

2.8 Benefits of Network Segmentation With Switches

LAN switching will significantly improve network performance without impacting the addressing structure within the network. Switching is defined as the ability to forward packets on the fly through a cross point matrix, a high speed bus, or shared memory arrangement. As a packet enters the switch, either the source and destination addresses or just the destination address is examined. This examination determines the switching action to be taken for the packet. Since the address fields are only fields examined, there is minimal delay, and the packet is switched to the destination address segment (port) before it is received in its entirt.

LAN switches were originally introduced as layer 2 devices operating in the same manner as a bridge in that a LAN switch is specifically designed to address LAN performance problems such as bandwidth shortages and network bottlenecks. A switch segments a LAN collision domain into smaller collision domains thus reducing or eliminating station contention for media access. Switched Ethernet is based on standard Ethernet that provides a Full-Duplex Ethernet connection to each node directly

connected to one of its switched ports. If an Ethernet switched port is connected to a hub, all the devices connected to that hub will share a half-duplex connection.

A LAN switch also includes the addition of VLAN (Virtual Local Area Network) technology. VLAN technology allows a switched network to be logically divided into several broadcast domains or sub-networks. Layer 3 switching technology then allows these subnets to be routed together faster than traditional routing procedures. LAN switches also use the data link layer information to create a direct a point to point path across the switch or across several switches between the source and destination. Use of the MAC layer information for transmitting packets enables a LAN switch to be protocol enables a LAN switch to be protocol Independent.

A Switch is able to create VLANs by grouping ports together into logical groups that effectively create Broadcast domains instead of collision domains. Within each collision domain frames can be moved at wire speed between ports in the same VLAN. This means that each VLAN will be its own sub-network. For the VLANs to communicate together a Layer-3 device such as a router is required. The device may be an external router with connections to each VLAN or a special router that can understand the VLANs and route directly using the using the already provided VLAN information within the switch. The extra item of information is called TAGGING.

Inside a Switch, as a frame enters the switch it is tagged with the VLAN that the port belongs to so the switch can determine what to do with the frame and how to control it. A Layer-3 switch can read and route the tagged frames very fast from VLAN to VLAN with lower overhead and less latency than a standard router. Routers that have the ability to route between VLANs support standards for VLAN interfacing including the ISL and 802.1Q trunking standards.

2.9 Describe the Guidelines and Distance Limitations of Fast Ethernet

Rules specify the maximum transmission path length between two 100BaseT data terminal equipment (DTE) devices. A DTE is an end station, bridge, switch, router, or similar equipment at the end of a link. A Fast Ethernet repeater cannot be a DTE device. The identifier "100Base-X" refers collectively to the 100Base-TX and 100Base-FX standards described in the following sections. Both 100Base-TX and 100Base-FX share a common signaling specification, called "4B/5B", that originated with the ANSI

X3T9.5 standard for Fiber Distributed Data Interface (FDDI). An existing signaling specification was adopted to help speed 100Base-X products to market.

2.10 Distinguish Between Cut-Through and Store-and-Forward LAN Switching

Packet latency and error detection for forwarding through the switch depends on the configured switching mode. Faster modes trade off error checking for low forwarding latency. Switch throughput is not affected by the choice of switching modes, as throughput is determined at wire speed. There are three operational modes to handle packet (frame) switching:

2.10.1 Store and Forward

In the store and forward mode, the switch receives the complete packet before forwarding takes place. After re-calculating and verifying the CRC at the end of each frame, the destination and source addresses are read and the packet is forwarded. Of course the frame is discarded if it contains a CRC error, is a runt (less than 64 bytes including the CRC) or a giant (more than 1518 bytes including the CRC). Latency increases in proportion to packet size when this switching technique is used due to the time to receive and check the entire frame.

2.10.2 Cut Through

With the cut through mode, the switch does not wait for the packet to be completely received nor does it check the CRC. It waits only for the header to be received in order to determine the destination address. Depending on the network transport protocol being used (connectionless or connection oriented), there is a significant decrease in latency from input port to output port. Latency in cut through switching remains constant regardless of packet size because this switching mode starts to forward the packet as soon as the switch reads the source and destination addresses (some switches read only the destination address). Cisco implements this method on their lower end workgroup switches like the 1900.

2.10.3 Fragment-Free

A modified form of cut through switching. In the Fragment-Free switching mode, the switch waits for the collision window (64 bytes) to pass before forwarding. If a packet has an error or better explained, a collision, it almost always occurs within the first 64 bytes. Fragment-Free mode provides better error checking than the Cut through mode with practically no increase in latency.

2.10.4 Hybrid

Other switches employ hybrids that include the automatic changing of the above switching modes based on a determination of performance and frame reliability.

2.11 The Operation of The Spanning-Tree Protocol and its Benefits

Ethernet bridges and switches implement the IEEE 802. 1d Spanning Tree Protocol(STP) specification to prevent loops in a network.The Spanning Tree Protocol establishes a root node and constructs a network topology with one path for reaching any node.The resulting tree structure, originating from the Root-Bridge,spans connectivity to all LAN segments. Packets are then forwarded to and from interfaces included in the spanning tree. Packets received from interfaces not in the spanning tree are dropped. Packets should never be forwarded onto interfaces that are not part of the spanning tree. Network devices exchange messages with each other to detect bridging loops and then stop the loops by blocking selected interfaces. The protocol also ensures that the redundant paths are utilized to construct a new tree in case of a failed device and maintains connectivity with other downstream nodes.

A Spanning Tree Enabled bridge or switch will both send out bridge protocol data units (BPDUs) and listen to BPDUs of other bridges. The BPDU configuration contains enough information so that all bridges can perform the following:

Select a single bridge that will act as the "root" of the spanning tree;

1. Calculate the distance, of the shortest path from itself to the root bridge
2. For each LAN segment, designate one of the bridges as the closest one to the root. That bridge will handle all communication from that LAN to the root bridge and will be known as the "designated bridge."
3. Let each bridge choose one of its interfaces as its root interface, which gives the best path to the root bridge

4. Allow each bridge to mark the root interface and any other inter faces on it that have been elected as designated bridges for the LAN to which it is connected as being included in the spanning tree
5. This setup improved the operation of a LAN built with multiple bridges, because the topology could automatically recover from link failures. However, all those interfaces blocked by spanning tree do waste a lot of potential bandwidth that could be used to carry traffic on the network

2.12 VLANs

A VLAN is defined as a broadcast domain within a switched network. Broadcast domains describe the extent that a network propagates a broadcast frame generated by a station. Some switches may be configured to support a single or multiple VLANs. Whenever a switch supports multiple VLANs, broadcasts within one VLAN never appear in another VLAN. Switch ports configured as a member of one VLAN belong to a different broadcast domain, as compared to switch ports configured as members of a different VLAN.

Creating VLANs enables administrators to build broadcast domains with fewer users in each broadcast domain. This increases the bandwidth available to users because fewer users will contend for the bandwidth.Routers also maintain broadcast domain isolation by blocking broadcast frames. Therefore, traffic can pass from one VLAN to another only through a router.Normally, each subnet belongs to a different VLAN. Therefore, a network with many subnets will probably have many VLANs. Switches and VLANs enable a network administrator to assign users to broadcast domains based upon the user's job need. This provides a high level of deployment flexibility for a network administrator.

2.12.1 Advantages of VLANs :

1. Segmentation of broadcast domains to create more bandwidth
2. Additional security by isolating users with bridge technologies
3. Deployment flexibility based upon job function rather than physical placement
4. Switch Port Modes

Switch ports run in either access or trunk mode. In access mode, the interface belongs to one and only one VLAN. Normally a switch port in access mode attaches to an end user device or a server. The frames transmitted on an access link look like any other Ethernet frame.

Trunks, on the other hand, multiplex traffic for multiple VLANs over the same physical link. Trunk links usually interconnect switches, as shown in Figure 2.2. However, they may also attach end devices such as servers that have special adapter cards that participate in the multiplexing protocol.

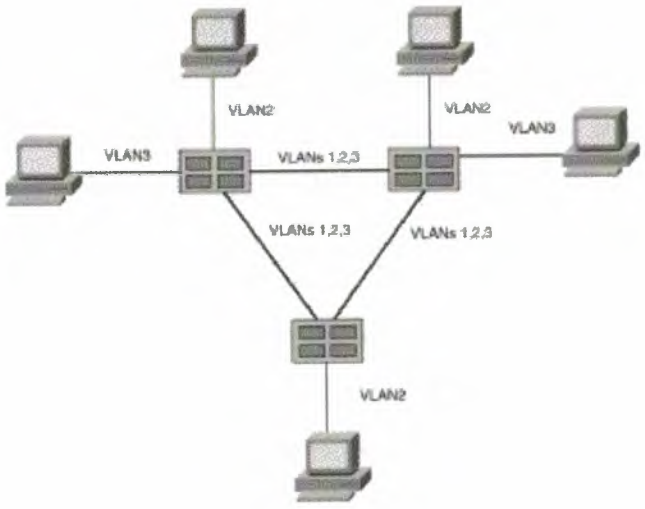

Figure 2.2: Switches Interconnected with Trunk Links

Note that some of the devices attach to their switch using access links, while the connections between the switches utilize trunk links.

To multiplex VLAN traffic, special protocols exist that encapsulate or tag (mark) the frames so that the receiving device knows to which VLAN the frame belongs. Trunk protocols are either proprietary or based upon IEEE 802.1Q. For example, a proprietary trunk protocol may be like Cisco's proprietary Inter-Switch Link (ISL), which enables Cisco devices to multiplex VLANs in a manner optimized for Cisco components. Or, an intervendor solution may be implemented, such as 802.1Q, which enables products from more than one vendor to multiplex VLANs on a trunk link.

Without trunk links, multiple access links must be installed to support multiple VLANs between switches. This is not cost-effective and does not scale well, so trunks are preferable for interconnecting switches in most cases.

2.12.2 The Benefits of Virtual LANs

A Switch is able to create VLANs by grouping ports together into logical groups that effectively create Broadcast domains instead of collision domains. Within each collision domain frames can be moved at wire speed between ports in the same VLAN. This means that each VLAN will be its own sub-network. For the VLANs to communicate together a Layer-3 device such as a router is required. The device may be an external router with connections to each VLAN or a special router that can understand the VLANs and route directly using the already provided VLAN information within the switch. The extra item of information is called TAGGING.

VLAN implementation is most often done in the switch software and assist greatly in network administrative functions such as moves, additions, or changes in the network. With VLANs there is no need to ever move equipment to accommodate users with similar logical function who are located in several physical locations.

Cisco's VLAN implementation associates a switch interface or group of interfaces with a particular VLAN. Some manufacturers also allow the association of MAC addresses to VLAN's however for traffic control and security thatr is not typically the best implementation as Cisco's concept is the most practical.

VLANs can also be extended throughout all network switching hardware allowing the VLAN information to be moved throughout the network for easy LAN administration using VLAN trunking protocols such as Cisco's ISL or IEEE 802.1Q. Some switches offer routing interfaces which allow the assignment of network addresses to each VLAN for Layer 3 routing purposes.

2.13 Describing the Function of MAC Address

MAC addresses identify network devices in LANs that implement the IEEE MAC addresses of the data link layer. Like many data link addresses, MAC addresses are unique for each LAN interface. MAC addresses are 48 bits in length and are displayed

as 12 hexadecimal digits. The first 6 hexadecimal digits identify the manufacturer or vendor. The last 6 hexadecimal digits comprise the interface serial number, or another value administered by the specific vendor. MAC addresses sometimes are called *burned* in addresses because they are "burned" into read only memory or ROM and are then copied into RAM when the interface card initializes.

Since MAC addresses are required for communications, they must also be determined for various uses.

1. Address Resolution Protocol (ARP) maps network addresses to MAC addresses.Address resolution is the process of mapping network addresses to the Media Access Control (MAC) addresses.
2. Hello protocol enables network devices to learn the MAC addresses of other network devices
3. The Hello protocol is a network layer protocol that enables network devices to identify one another and indicate that they are still functional. When a new end system powers up, for example, it broadcasts Hello messages onto the network. Network devices can learn the MAC addresses of other devices by examining Hello protocol packets.
4. MAC addresses are either embedded in the network layer address or are generated by an algorithm.Some protocols like IPX use predictable MAC addresses. These MAC addresses are predictable because the network layer either embeds the MAC address in the network layer address or uses an algorithm to determine the MAC address.

2.14 The Features and Benefits of Gigabit Ethernet

In networking operating systems, protocols, or applications. The Gigabit Ethernet specification delivers a good improvement, offering data tr traditional Ethernet. Gigabit Ethernet delivers this capacity for bandwidth-starved servers and the backbone infrastructures of corporate and educational communication ansfer of 1 gigabit per second (that's 1 billion bits per second)--100 times that of networks. The IEEE ratified the standard in record time; the move was hastened by the cooperation of the consortium of vendors that make up the Gigabit Ethernet Alliance IEEE 802.3z is a logical step forward from 10-Mbps and 100-Mbps Ethernet. It requires no change

2.15 Token Ring

2.15.1 The features and benefits of Token Ring

Devices on a Token Ring network get access to the media through token passing. Token and data pass to each station on the ring, as follows:

1. The devices pass the token around the ring until one of them needs to transmit data.
2. The device that wants to transmit takes the token and replaces it with a frame.
3. Each device passes the frame to the next device, until the frame reaches its destination.
4. As the frame passes to the intended recipient, the recipient sets certain bits in the frame to indicate that it received the frame.
5. The original sender of the frame strips the frame data off the ring and issues a new token.

2.15.2 Describe the guidelines and distance limitations of Token Ring

Token Ring is a 4-Mb/s or 16-Mb/s token-passing, baseband LAN that operates in a ring topology. Token Ring conforms to the IEEE 802.5 standard. A Token Ring LAN uses shielded or unshielded twisted-pair cable.

The Token Ring/802.5 interface is IEEE 802.5-compatible with IEEE 802.2 Type 1 (connectionless) and Type 2 (connection-oriented) support. You can configure the interface to operate at 4 or 16 Mb/s to respond to different network requirements. The interface supports IBM Type 1 and Type 3 cabling. Stations on a Token Ring network attach to the network using a multistation access unit (MAU). Although the Token Ring is logically a ring, it is physically a star, with devices radiating from each MAU.

MAUs connect a limited number of devices, typically two, four, or eight. You can extend the Token Ring by connecting the Ring Out (RO) port of one MAU to the Ring In (RI) port of the next. You must complete the ring by connecting all RI and RO ports

2.16 IEEE Standards.

The IEEE ("eye-triple-E"), The Institute of Electrical and Electronics Engineers, Inc.,helps advance global prosperity by promoting the engineering process of creating,

developing, integrating, sharing, and applying knowledge about electrical and information technologies and sciences for the benefit of humanity and the profession.

2.17 ANSI Stanards

The American National Standards Institute (ANSI) has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for more than 80 years. Founded in 1918 by five engineering societies and three government agencies, the Institute remains a private, nonprofit membership organization supported by a diverse constituency of private and public sector organizations.

Throughout its history, the ANSI Federation has maintained as its primary goal the enhancement of global competitiveness of U.S. business and the American quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and promoting their integrity. The Institute represents the interests of its nearly 1,000 company, organization, government agency, institutional and international members through its office in New York City, and its headquarter in Washington, D.C.

ANSI does not itself develop American National Standards (ANSs); rather it facilitates development by establishing consensus among qualified groups. The Institute ensures that its guiding principles, consensus, and are followed by the more than 175 distinct entities currently accredited under one of the Federation's three methods of accreditation (organization, committee or canvass). In 1999 alone the number of American National Standards increased by nearly 5.5% to a new total of 14,650 approved ANS. ANSI-accredited developers are committed to supporting the development of national and, in many cases international standards, addressing the critical trends of technological innovation, marketplace globalization and regulatory reform.

2.18 Introduction to LANs Security

"Security" is a concept to manage an ensemble of interacting LAN computers and backup systems, rather than just focusing on one computer. The fact that our data has been immuned from internet attacks depends on no luck. İt depends on carefully crafted infrastructures intertwined by different levels of secured LAN computers, and hardworks from SysAdms, a. k. a. the "Watchdogs". There are several rules of thumb to design such an infrastructure. Don't put all your eggs in one basket: Mail server, Web server, File server, these servers require different levels of security. It's recommended not to put all in one box for the sake of data. In order words, in the concept of security, any service for promoting personal convenience is not of top priority. I know what you have been doing: Activities on the internet are transparent; therefore, "being anonymous" is a joke. Everything can be tracked on the internet. Therefore, checking the system logs may often help to detect abnormal activities. Especially, daemons such as LPRNG (printing), Sendmail (mail), Apache(web), Xinet (internet), NFS (file sharing) and others that have the root privileges to run background jobs are vulnerable targets under attack. Checking their log files on a regular basis is a must. Know your enemy, know yourself: Sometimes, one has to think like a hacker to detect where the weakest link is in a network of computers. More important of all, upgrading software packages that can be related to any security leak should be done as often as possible. We have three levels of secured LAN computers, and each level would not share files with one another. Because low security computers are gateways that can be accessed by any remote host through the secure shell layer, we merely format low security computers if they are attacked. No question's asked. Behind the low security computers are the "high" and "tight" security computers. For the high security computers, they share home directories and printers. Backups are done by users on a regular basis, and users are requested to change their passwords that are different from those on low security ones often. Remote hosts can be included upon, long as their security can be comparable to our "high" level of security. It imples that, if remote machines are webservers or are connected by DHCP, they should not be included in our trusted host list under any circumstances. For "tight" security computers, sophisticated firewalls are installed, and trusted remote hosts are selected exclusively; SysAdm must have root access to the trusted remote hosts for imperative security checks.

2.19 DEFINITIONS AND CONVENTIONS DEFINITIONS

2.19.1 Security

From an IT perspective, security refers mainly to the protection of IT resources against unauthorized or unintended events. Examples of unauthorized events are: intentional interference or damage to programs or data, unauthorized program or data access and any misuse of a computer as defined in the Computer Crimes Ordinance1993, examples of unintended events are: hardware or software faults, power interruptions, and virus infections.

2.19.2 Workstation

In these guidelines, workstation refers to a microcomputer operating either in standalone mode , or in a local area network as a network terminal.

2.19.3 Server

A server in the LAN environment is essentially a high performance microcomputer acting as a central service provider to the network. Examples of such services are: file sharing, data sharing, and gateway access to another computer; hence the names file server, database server, communications server respectively.

2.19.4 Systems Software

Systems software refers to operating systems of microcomputers such as DOS or Windows 95 and that of LAN file servers such as NetWare.

2.19.5 Application Software

Application software refers to the commonly used microcomputer packages such as spreadsheet and word processing software, as well as self-developed application programs running on microcomputers.

2.19.6 Virus

Virus is a subversive computer program that may corrupt or erase computer files and it may change the normal behaviour of the computer. Any of the following symptoms could be a signal of viral activity:

1. The program takes longer than usual to execute.
2. A sudden reduction in available system memory or disk space.
3. A device light is on whilst there should be no activity with that device.

2.20 Guidelines on Microcomputers and LAN Security

2.20.1 Generals

AVACS

The Anti-Virus and Access Control System developed by ITSD for enforcing security on microcomputer systems. Moreover, AVACS provides a customizable menu system to simplify microcomputer operations, a file encryption utility, a report program on system information, and a text-file viewer program.

Conventions

Since IT security is about the protection of resources against unintended or unauthorized events, the guidelines are presented according to following hierarchical format:

Protection Against Unintended Events

1. Access Control
2. General guidelines
3. LAN Environment guidelines

Protection Against Unintended Events

1. Office environment is in general acceptable for the operation of microcomputer equipment. However, for some equipment, there might be special requirements on site preparation and the operating environment. For such cases, advice can be sought from the equipment vendors and ITSD.
2. Sufficient space must be provided for the microcomputer equipment as both operating and access area.
3. Additional space must be allowed to cater for media storage, working area, and future expansion.
4. Microcomputer equipment must not be located near to heat-generating areas or places where fire risk is high. Examples of such places are boiler rooms and canteen kitchens.
5. Smoking and drinking near the microcomputer equipment should be prohibited.
6. Portable fire extinguishers are preferred to be installed at sites with microcomputer equipment.

7. Direct sunlight upon the microcomputer systems should be avoided to prevent possible overheating or reflection from the monitor screens.
8. The operating environment should preferably be with low level of dust and dirt. The accommodation area is expected to be vacuum-cleaned regularly.
9. The microcomputer equipment should not be located in an area where there is high-frequency apparatus, or where there is excessive vibration.
10. The storage for microcomputer related magnetic media (such as tapes and floppy diskettes) should be away from any lightning conductor in the building as far as possible.
11. Provision of plastic covers for microcomputer equipment when they are powered off can, to a certain extent, protect the equipment from water damage.
12. All electrical installations should conform to the relevant standard specifications on electrical installation for Government buildings.
13. Electrical load surges or transient disturbance can cause system failures. Mains supply should not be shared with heavy, intermittent or switched loads.
14. Power sockets are recommended to be installed separately and dedicated to the microcomputer equipment. Appliances that are switched on and off frequently would be better not connected to dedicated power circuits.
15. Installation of hardware and software items to the microcomputer equipment should only be carried out by authorized personnel. LAN Environment
16. If the LAN is to be installed on solid ground, ducts or trunkings (PVC or metal, covered by ramps) should, as far as possible, be used to protect the LAN cables from mechanical damage. Raised floors may be used optionally.
17. LAN cables should not be laid adjacent to mains electrical cables, telephone cables, paging system cables, etc. without suitable trunkings.
18. Uninterruptible power supply (UPS) should be considered for protecting the LAN servers against power surges and for the tidy close-down of the servers in case of prolonged power failure.
19. Connection of equipment to, or disconnection of equipment from, a LAN should only be carried out by authorized personnel.

2.20.2 Systwm Software Security

- Backup copies of the systems software and related configuration files should be taken periodically. Since systems software are the vital parts of any production service, the entire process of backup and restore should be well proven.
- Wherever possible, backup copies of the systems software and related configuration files should be stored at a safe and secure location remote from the primary site, so that it would still be possible to reconstruct the operating environment should a disaster occur at the primary location.

2.20.3 Application Software Security

When two or more applications are to reside in the same microcomputer system, some measures must be devised to guard themselves against unintended interference by one another. For example, when data files are shared, each application should be aware of the possible risk in data corruption.

Similar to systems software, backup copies of the application software and related control files should be taken periodically. The entire process of backup and restore should be well proven. Wherever possible, the backup copies should be stored at a safe and secure location remote from the primary site, so that it would still be possible to reconstruct the operating environment should a disaster occur at the primary location.

2.20.4 LAN Environment

The need for process isolation is again emphasized for applications running in the LAN environment. Sufficient isolation schemes must be implemented to prevent unintended process interference.

It should be noted that in most cases, an existing single-user application on a microcomputer system would not work properly when directly migrated to run in a multi-user LAN environment.

2.20.5 Data Security

1. Backup copies should be maintained for all operational data to enable reconstruction should loss or destruction occur.
2. The backup copies should be taken at regular intervals such that recovery to the most up-to-date state is possible.

3. Procedures for data backup and recovery should be well established . Wherever possible, their effectiveness in real-life situations should be tested thoroughly.
4. Its advisable to store backup copies at a safe and secure location remote from the site of the microcomputer systems. In case of any disaster which damages totally the systems, the data could still be reconstructed on similar microcomputers elsewhere.
5. Multiple generations of backup copies should be maintained. This would provide additional flexibility and resilience to the recovery process.
6. Should software updates, besides backup copies of the data, be necessary to recover an application system, the updates (or backup copies of them) and the data backup should be stored together.
7. All data and documents of Confidential classification or above intended for processing by microcomputer systems should only be stored on removable media (e.g. floppy diskettes, removable hard disks) which can be stored away in a secure place after processing. Confidential data stored on the hard disk of a stand alone computer can be acceptable only if the computer can be stored in a secure place.
8. All media, including magnetic ones, containing classified information must be marked, handled and stored in the same way as their paper equivalent in accordance with Control of Classified Documents of the Security Regulations.
9. All intermediate material and information produced in the course of processing must also be accorded security protection of a degree commensurate with the highest classification of information contained in them.
10. Deletion of data files from microcomputer systems does not imply complete removal of the information. In most cases, the data are only made inaccessible by normal means. Thus it is advisable to either reuse the previously occupied area for storage of information of the same security classification, or reinitialize the area for storing data of a lower security classification.
11. Complete erasure of hard disk information can be accomplished through some common utility packages, a disk formatting function in the AVACS of ITSD, or physical destruction of the concerned disk.
12. All out-dated hardcopy printout or reports with classified grading should be downgraded and/or disposed in accordance with the relevant Security Regulations

13. User data can be stored both in the LAN file server and in the workstations. There are many factors (e.g. backup and recovery set-up, physical security, server capacity) governing where private data should be stored, and the decision may vary from case to case. Advice can be sought from ITSD whenever necessary.

2.21 Virus Consideration

General

1. Illegal copies of software have been regarded as the most common source of viruses. It must be emphasized that in order to minimize the risk of contracting virus and to avoid infringement of copyrights, software products should only be acquired from authorized agents.
2. It is a good practice to check every floppy diskette (especially those of unknown origin) with a virus scanning program before use. However, it should be noted that new viruses are being discovered almost every day, thus a floppy diskette may contain a new virus that cannot be recognized by the scanning program.
3. Public domain software, according to past records, have a relatively higher chance of being virus infected. Use of such software should be avoided.
4. It is a good practice to write-protect all floppy diskettes that are not expected to be written. Also, it is a good practice to remove floppy diskettes from drive slots after use.
5. In a publicly accessed microcomputer or LAN server, a memory-resident anti-virus program should be used for continuous virus monitoring.
6. Programs of doubtful origin should never be used. If there is a doubt about a program in use, it is advisable to restrict its use to a microcomputer without hard disk or, if applicable, that having the hard disk writeprotected through system setup. The concerned microcomputer should also be logged out from the network if it is connected to one. It should also be powered off after use for cleaning any possible virus in memory.
7. Connection to an external network (e.g. Internet) or any Bulletin Board System (BBS) should be controlled. A security scheme (e.g. checking of every downloaded file for virus) should be devised before any such connection is made. In this regard, advice can be provided by TSSC. Moreover, TSSC may be consulted for the background of any external BBS.

8. Any suspected virus case should be reported to the management immediately. The TSSC Helpdesk can provide assistance in investigating suspected virus cases, and in cleaning the virus. Virus cleaning can also be done through anti-virus software in the market.
9. If a machine is suspected to be infected by a virus, all activities on that machine should be stopped immediately. Continued usage of the machine may cause a serious deterioration of the situation.
10. Successfully cleaning a virus from a computer does not necessarily imply that contaminated or deleted files can be recovered or retrieved. The most effective way for recovering corrupted files is to replace them with the original copies. Therefore, sufficient backup copies should be kept to facilitate recovery from a virus attack.
11. If the output data from a microcomputer system are to be processed by another system (regardless of whether a microcomputer, mainframe or midrange system), consideration should be given to ensure that the output data are virus-free so as to prevent direct or indirect contamination of other computer systems.

2.22 Guidelines on Microcomputers and LAN Security Protection Against Unauthorized Access

2.22.1 Access Control

General

1. Only authorized personnel should be allowed access to the microcomputer systems. In case a system is shared by many users, an administrator responsible for controlling access to the system is required.
2. Appropriate measures should be taken against theft at all times as microcomputer equipment and their components are fairly transportable. Some microcomputers, such as the notebook computers, are even designed for portability. If such portable microcomputers are allowed to be on loan for office duties, a suitable controlling scheme (e.g. on aspects such as the items on loan, their physical identification, the responsible officer, loan period) should be in force.

3. All microcomputer systems should require the use of passwords to gain access. Passwords can usually be set at both the hardware level (e.g. keyboard locking) and the software level (e.g. login systems, screen savers). Passwords must be used for access at all levels. The AVACS of ITSD, or equivalent login systems, are recommended to be installed.
4. Passwords should be so chosen that their meaning cannot be easily guessed or deduced. The length of passwords should be long enough (e.g. at least 6 characters) to prevent machine-assisted revelation. Also, they should be changed at least once every 3 months. Passwords of three or four characters are vulnerable to attack unless chosen from a large character set.
5. Users should exercise sufficient caution to prevent the exposure of their passwords at the moment of password input.
6. Hardcopies of passwords for record-keeping or other purposes are not advisable. If it is necessary to maintain such a hardcopy, adequate security measures (e.g. put in a sealed envelope and stored in a safe) accompanied by disclosure procedure should be devised.
7. Some equipment and physical devices that can restrict access to the microcomputer systems may be considered for enhancing security. The following are some examples: cabinets with locks, custom-made housing, diskette drive locks, disabled floppy drive for boot-up, smart cards for user authentication.
8. If a diskette drive is not an operational necessity, as is the case for some workstations in a LAN environment, it can be removed or, "floppyless" workstations can be ordered, so that the risk of direct data retrieval is minimized.
9. A server room with locks is highly recommended for protecting the servers and the LAN equipment from unauthorized access. Moreover, it is advisable to have the servers locked inside cabinets.
10. Remote access, remote control or remote dial-in software are commonly used in the LAN environment. These software packages all offer security features to the users. These security features must be fully studied and used.
11. For all common LAN operating systems, a majority of the server operations can be done at a LAN workstation. Security of a LAN server can therefore be enhanced if, where affordable, the keyboard is locked or disconnected.

12. System security would be enhanced if the trunkings for LAN cables are, where applicable, sealed, locked, or accommodated in areas with high security.

2.22.2 Systems Software Security

General

1. Microcomputer operating system such as DOS provides minimal security features to the users. Users are thus recommended to enhance their workstation security by installing AVACS, or an equivalent security system in addition to DOS.
2. The default settings for systems access should follow the spirit of "implicitly restricted until explicitly granted", as opposed to one of "implicitly granted until explicitly denied."
3. The alarm thresholds for access attempts should be appropriately adjusted to a level low enough to prevent intrusion, whilst high enough to avoid too many false alarms.
4. .For systems access and control purposes, personal accountability should be the prime objective. Each user of the system must, as far as possible, be assigned a unique personal identifier. It is not recommended that two or more persons share the same identifier, even when they possess the same systems access privileges or share common data.
5. Today most LAN installations are using NetWare or LAN Manager as LAN operating systems. These operating systems offer security features in the form of matching user rights with resource locks. Files, directories, and hardware components are examples of the resources. The LAN Administrator should be aware of the security implications associated with the different settings of the resource locks .
6. In planning a LAN configuration, the LAN Administrator should appropriately match the settings of the resource locks with the user rights so as to arrive at a target security level. Samples of the settings can be found in the relevant LAN Administrator's Guidelines published by ITSD.
7. Where applicable, system security can be enhanced by restricting certain non-mobile LAN users to login through pre-defined workstations.
8. Intrinsic in the design of most common LAN operating systems, the user identifier (UserID) with the highest systems privileges is often implicitly

assumed to be the security administrator. In this case the person (usually the LAN Administrator) in possession of the UserID would be responsible for two different roles. The Administrator should be of a rank in the senior cadre among the users of a LAN. He/She should hold a post listed in Appendices I and IV of the Integrity Checking Instructions issued by the Secretary for the Civil Service as per Security Regulation so that clearance for access to classified information would have been made.

9. System access through a UserID with the highest systems privileges should be restricted to only one (or at most two, for mutual backup purpose) senior and responsible officer, as such privileged access has the potential of causing severe damage to the system. Considerations and guidelines for designation of any person who has high system privileges should be similar to those of the LAN Administrator.

10. AVACS, or equivalent microcomputer security system, is recommended to be used in addition to whatever security features offered by the LAN operating system.

2.22.3 Data Security

General

1. Encryption devices or programs should be considered for enhancing the security level of application data. It is advisable that sensitive data to be transferred from one workstation to another in a networked environment be encrypted before transfer. Some software, such as cc:mail, will encrypt mails that are transmitted over the network.
2. Classified data and documents should only be processed by microcomputer systems when nobody other than the authorized operating staff has access to the processing.
3. Storage of data and documents of a nature up to Confidential on the local hard disk of a standalone (i.e. not connected by any means to any network) microcomputer system is acceptable, provided that the system is in a secure place (e.g. in an office suitable for storing Confidential paper documents), since the system itself would be treated as a Confidential document. Guidelines on Microcomputer and LAN Security

4. It is emphasized that potential risks exist in data exposure when different LANs are connected. Sufficient security measures (e.g. data encryption through software or hardware means) should therefore be planned in the network design stage. In this regard, advice should be sought from ITSD.

5. Stipulated rules and advice from Security Branch should be observed when considering the transmission of classified information over the network .

Chapter Three

Designing a Secure Local Area Network

3.1 Introduction

In order to design and build a well-secured network, many factors must be taken in to consideration, such as the topology and placement of hosts within thenetwork, the selection of hardware and software technologies, and the careful configuration of each component. My reserch will be an examination of someofthe issues in designing a secure Local Area Network (LAN) and some of the bestpractices suggested by security experts. I will discuss securing a LAN from the topology which comprises the physical and logical design of the network;securing the routers andswitches which connect segments and hosts to form thenetwork; and, finally, some of the emerging and advanced techniques in networksecurity will be examined.

3.2 Initial Assumptions and Challenges

My goal is to examine some of the security issues commonly found in the small to medium sized LAN set up for a business or other institution, and to identify some of the best practices from the perspective of the network designer. While no two networks are exactly alike, some of the typical challenges faced by the network designer include the following:

1. Securing the network from Internet launched attacks.
2. Securing Internet facing web, DNS and mail servers.
3. internally launched attacks.
4. Securing sensitive and mission critical internal resources such financial.
5. records, customer databases, trade secrets, etc.
6. Building a framework for administrators to securely manage the network.
7. Providing systems for logging and intrusion detection.

Before beginning the design process, a security policy should be put in place, or updated to accurately reflect the goals of the company. Additionally, a realistic assessment of the risks faced, and identification of the resources (manpower, hardware, budget) that are available should be made. Once the organization's security policy and the available resources have been identified the design process can begin

3.3 Topology and Architecture

A critical step in designing networks is defining the network topology. The topology is the physical and logical layout of the network. On the physical side, we will need to provide distribution to the offices or buildings where the users are located. We will need to provide connectivity to the servers which comprise our intranet, to the Internet, and possibly to other company locations or business partners, remote users connecting via telephone lines, etc. The logical topology must be considered as well. It is bound to some degree by the physical topology, but with technologies such as Virtual LANs (VLANs) and Virtual Private Networks (VPNs) there is considerable flexibility in designing the logical topology. In laying out the logical topology we will need to consider our security policy, and decide what our trust model is. Which parts of the network are less trusted, and which are more.Which groups of devices and users should be logically grouped together, and which should be separated?

The basic design illustrates our connection to the Internet with a border router and firewall, and our public extranet servers which are connected to a third interface on the firewall. The firewall is one of four connections to a core router or, if higher performance is required . The remaining connections to our core router are the floor or building switches which provide connectivity to the different departments and our intranet servers. This topology demonstrates how devices with similar functions and security profiles are grouped together ,the public extranet servers, user workstations, and the intranet servers. By creating separate security zones, we will be able to enforce our security policy with the appropriate firewall rules and layer 3 access lists. 1

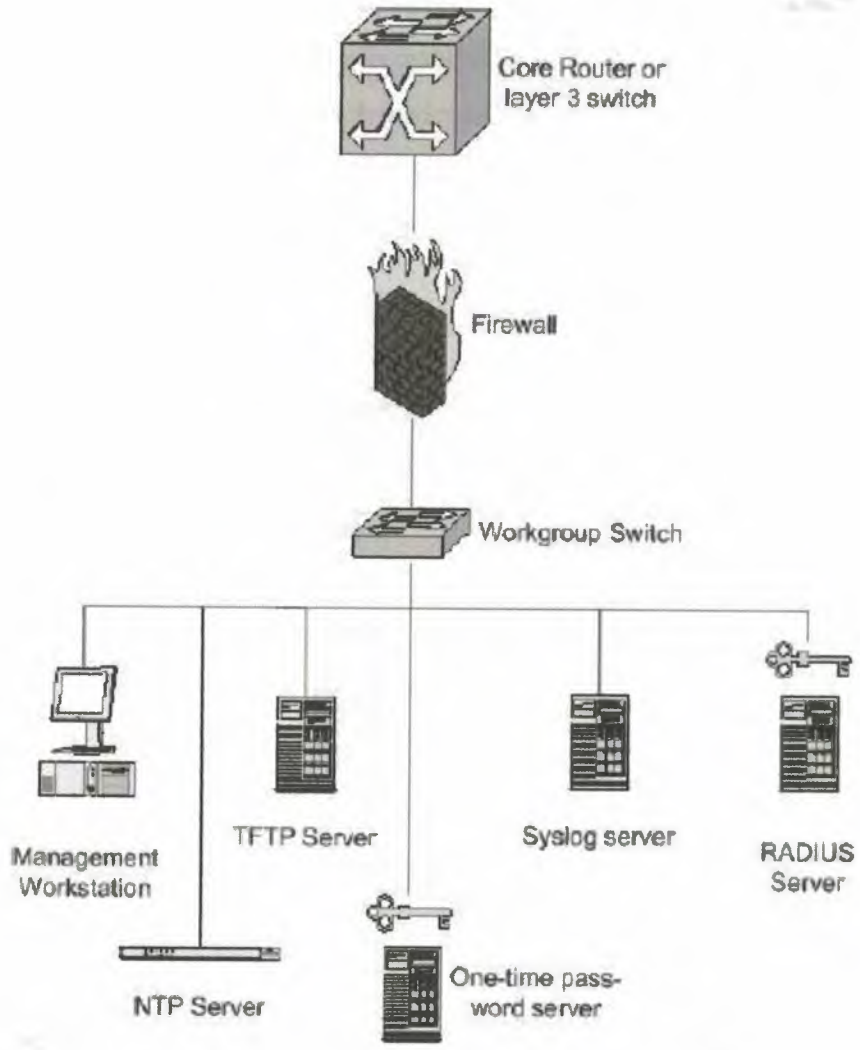

Figure 3.1 Basic Network Design

One element our basic design lacks is the infrastructure for managing our network. We will need one or more management workstations, tftp servers, and one or more syslog servers at a minimum. Other typical servers for the management network are a one-time password (e.g. RSA SecurID or Axent Defender) server, RADIUS server, etc. Because these servers will form the foundation of our network management and security, we will want to create a separate management VLAN which is isolated from the rest of the network by a firewall or access lists. The only traffic that we will allow in to the management network is either from

the managed devices or protected by encryption. A design goal will be to keep management traffic off the production network, to eliminate the possibility that it could be intercepted in transit. Ideally we would configure each device with a physical port on the management VLAN. If this is not possible because of physical or other limitations, management should be encrypted via ssh or IPSEC. Below is a representation of the management network

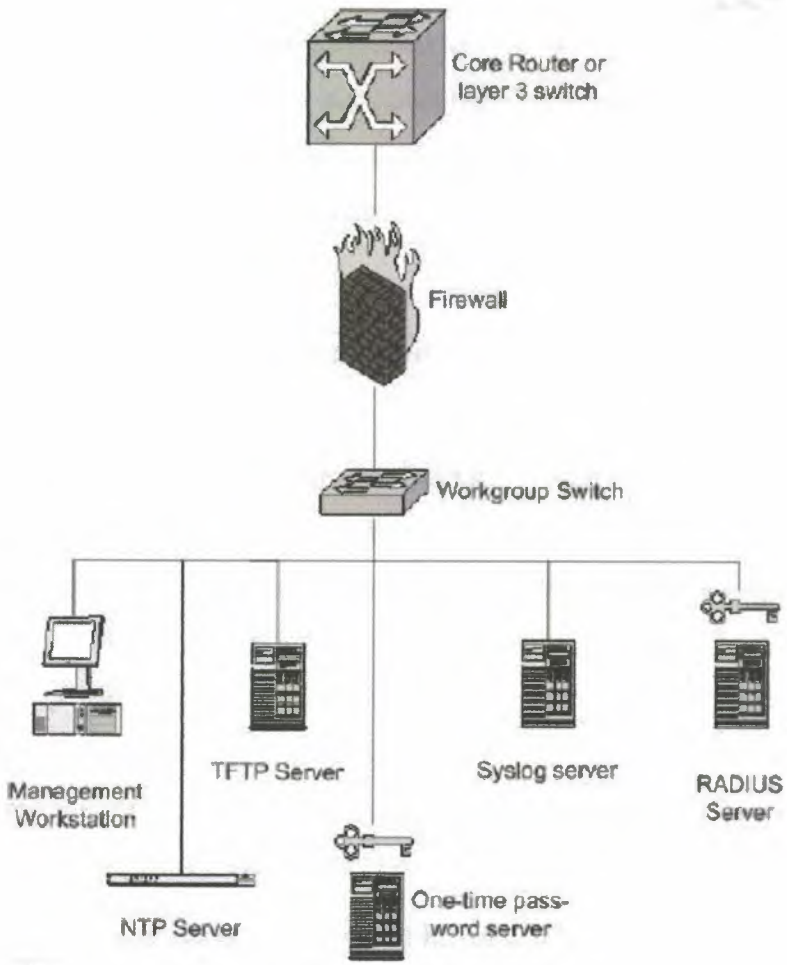

Figure 3.2 Management VLAN

3.4 Securing Routers and Switches

Now that the topology has been defined, let's take a look at building security into our network elements and configurations. Our design calls for segmenting the network into subnets based on function and, possibly, location. By implementing routing at the at the network core, our segments are isolated into individual broadcast domains. This improves performance and also improves security by preventing sniffing or are based attacks between segments.

Within each subnet the hosts are connected to an Ethernet switch. A switch provides high performance by putting each host in its own collision domain, and enhances security by making sniffing and arp based attacks difficult. A hub is a less expensive alternative to a switch for layer 2 connectivity, though it is less desirable both from a performance and a security standpoint.

3.5 Layer Three Design and Access Lists

Our layer 3 design is quite simple, with a central core router connecting the different production and management networks. Because we have mapped out our trust model and security policies, we can use access lists at layer 3 to implement our security policy. For traffic coming into a subnet, we will permit only appropriate incoming packets, based on the policy of that subnet. Similarly, we will filter outbound traffic to eliminate spoofing and minimize any malicious or illegitimate activities. Let's consider some example access lists based on the Cisco IOS command set. Suppose we have a Windows 2000 file server and a web server on our server subnet. How do we configure our access list to permit the necessary traffic and deny everything else

- ! Permit icmp echo to the server subnet (192.168.1.0/24)
- ! for troubleshooting
- access-list 111 permit icmp any 192.168.1.0 0.0.0.255 echo
- access-list 111 permit icmp any 192.168.1.0 0.0.0.255 echo-reply
- ! Permit Windows file sharing protocols to the Windows 2000
- ! server at 192.168.1.200

- access-list 111 permit tcp any host 192.168.1.200 eq 135
- access-list 111 permit tcp any host 192.168.1.200 eq 139
- access-list 111 permit tcp any host 192.168.1.200 eq 445
- access-list 111 permit udp any host 192.168.1.200 eq 137
- access-list 111 permit udp any host 192.168.1.200 eq 138
- access-list 111 permit udp any host 192.168.1.200 eq 445
- ! Permit http access to the web server at 192.168.1.201
- access-list 111 permit tcp any host 192.168.1.201 eq 80
- ! Deny any other traffic
- access-list 111 deny ip any any log

The above commands illustrate the concept of our layer 3 design, and would need to be expanded and modified in a production environment. Let's now consider a workgroup subnet populated with desktops but no servers. Since we don't expect servers to be placed here, inbound tcp traffic is limited:

- ! Permit icmp echo to the workgroup subnet (192.168.2.0/24)
- ! for troubleshooting
- access-list 121 permit icmp any 192.168.2.0 0.0.0.255 echo
- access-list 121 permit icmp any 192.168.2.0 0.0.0.255 echo-reply
- ! Permit established tcp connections only
- access-list 121 permit tcp any 192.168.2.0 0.0.0.255 established
- ! Permit inbound udp traffic to support NetMeeting
- access-list 121 permit udp any 192.168.2.0 0.0.0.255 gt 1023
- ! Deny any other traffic
- access-list 121 deny ip any any log

Finally, we will want to filter traffic leaving each subnet to prevent spoofing. The presence of incorrect source addresses could indicate either a misconfigured machine, or one which was compromised and attempting to launch a DDOS or similar attack. Here's how outbound filters would be defined for the workgroup subnet:

- ! Permit outbound traffic from workgroup subnet
- ! (192.168.2.0/24) with a legitimate source address;
- ! Deny all other traffic
- access-list 122 permit ip 192.168.2.0 0.0.0.255 any
- access-list 122 deny ip any any log

3.5.1 Securing Layer Three

its illestrated that our layer 3 design and access lists are used to implement our security policies. We also want to take steps to ensure that the routers themselves are secured against attacks. There are many excellent templates for hardening Cisco routers against attacks such as the National Security Agency's or Cisco's. 2, 3 I would like to point out a couple key strategies that are relevant to our discussion. Secure management of the routers is enforced by several mechanisms. First is the management VLAN, which ensures that the management traffic does not traverse the production network. Access lists should be configured on the management ports to block illegitimate connections. Out Of Band (OOB) communication, such as via a terminal server, is another excellent means of securing management traffic. We will use strong authentication provided by a one-time password server, such as RSA Security's ACE server. Encrypted communication protocols such as ssh should be used if in band (over the production network) communication is necessary. Logging to the syslog servers located on the management network will meet our auditing requirements. 4, 5 The following excerpt from a Cisco 7500 router configuration file demonstrates some of these concepts:

- ! Configure logging to syslog server (192.168.7.88)
- logging trap debugging
- logging facility local7
- logging 192.168.7.88
- ! Configure aaa authentication to the radius server
- ! on the management VLAN
- aaa new-model
- ! create a local user account in case radius

- ! is unavailable
- user freduser password [password]
- aaa authentication login default group radius local
- radius-server host 192.168.7.77 auth-port 1645
- radius-server timeout 5
- radius-server key [RADIUS shared secret]

! Configure ssh server

- crypto key generate rsa
- ip ssh time-out 60
- ip ssh authentication-retries 2
- ! Access list to ensure management traffic is sourced from
- ! the management station (192.168.7.23)
- access-list 7 permit host 192.168.7.23
- access-list 7 deny ip any any
- ! Configure management port
- line vty 0 4
- access-class 7 in
- transport input ssh

3.6 Layer two Design

In previous sections, I have described how security can be implemented in the layer 3 design via access lists and hardening the routers themselves. We must now address threats that exist at layer 2 and continue to enforce our security policy in the layer 2 design. One question we will want to consider is how to maximize the security of the switch ports themselves. If an attacker controlled a host on one of our VLANs, could she jump to another VLAN and gain access to a more sensitive VLAN? What about the possibilities of a misconfiguration providing undesired access to an intruder? To achieve the highest level of security we would configure only one VLAN per switch. This would minimize the chance of an attacker

jumping VLANs and reduce the chance of misconfiguration. If we can provide this kind of isolation of one VLAN per switch, it is the most secure, and highly recommended for likely attack points such as our Internet facing server segment.. A more recent study commissioned for Cisco by researchers at @Stake proclaimed that there was minimal risk in using VLANs when configured according to best practices. The designer will have to carefully weigh the costs and risks, and make a decision appropriate to her environment. Since the switch ports are the gateway into our network, we will want to implement physical security when possible, by controlling access to switch ports, and disabling unused ports. As most busy network admins may not be able to monitor every unused port, there are many other techniques that can be used to enhance security. One technique is to require the users to authenticate via RADIUS or LDAP before they are given access to any resources.

However, implementation of this feature involves a complex infrastructure, and is best suited to very large enterprises. Many other strategies for securing access to switch ports are available. Limiting the MAC addresses that are permitted to communicate on the ports is key to layer 2 security. A flood of MAC addresses, or even a single new MAC address could indicate an intruder, or ARP spoofing activities such as the *dsniff* utility.

Many switches can be configured with static or secure MAC assignments.

Creating a static MAC assignment ensures that frames for the designated ethernet address are always forwarded to the specified port, and it can prevent ARP spoofing attacks. To set a static port on a Cisco Catalyst switch (CatOS 6.3) the following statement is used:

set cam permanent aa-bb-cc-11-22-33 6/1 The preceding command will ensure that frames for the specified MAC will always be forwarded to the specified port. 12 Static MAC assignments are

especially advisable for critical hosts like gateways and firewalls.

Another good idea is to limit the number of MAC addresses that can appear on each port, either to one or an appropriate small number, or configure a timeout that prevents a new MAC from appearing until a certain time period elapses.

These features can be configured with the *set port security* statement on a Cisco Catalyst switch. The following statements show some of the options available with this command: Limit the number of permissible MAC addresses to 1 set port security 6/1 enable maximum 1 Limit the permissible MAC on port 6/1 to aa-bb-cc-11-22-33 set port security 6/1 enable aa-bb-cc-11-22-33 Limit the permissible MAC addresses to 2, and the aging to 30 minutes set port security 6/1 enable age 30 maximum 2 Limit the permissible MAC addresses to 1, aging to 30 minutes, and the violation action to restrict packets from insecure hosts (default is shutdown the port) set port security 6/1 enable age 30 maximum 1 violation restrict

3.6.1 Securing Layer two

We have surveyed some of the key strategies for securing our network from violations of our layer 2 policy. But we must take additional steps to secure the switches themselves from attacks, and from attacks against layer 2 protocols such as Spanning-Tree Protocol (STP), which could result in denial of service or availability situations.

Locking down the security on the layer 2 devices will follow the principles used to lock down the routers, such as disabling insecure default configurations, securing the management channel and implementing strong authentication via one-time passwords. Once we have hardened the switch itself, we will want to secure our infrastructure against attacks on the underlying layer 2 protocols.

Spanning-Tree Protocol (STP) is used by switches and bridges to establish their MAC address forwarding tables, and establish a tree-like topology which forwards frames via the fastest path and eliminates loops. Bridge Port Data Units (BPDUs) are exchanged by switches to share information about the topology.

STP is designed to dynamically adjust to changes in the topology, but it is vulnerable if random hosts start transmitting BPDUs and affecting the spanning tree.

This could happen if an unauthorized switch was attached to one of our ports, or a bridging protocol was enabled on a Linux host, for example. If our switch supports it, we can prevent random hosts from either forwarding BPDUs or affecting the spanning tree. Cisco Catalyst switches provide two features which address this problem, *STP Root Guard*, and *STP*

Portfast BPDU Guard. For optimum performance, we will want the root bridge of the spanning tree to be located near the core of the network on the highest bandwidth links.

The STP root guard feature allows us to enforce the STP topology, and prevent the root bridge from appearing on an edge segment, or on a lower bandwidth connection.

Root guard is enabled on ports where we don't want the root to appear. If superior BPDUs are received from a port with root guard enabled, the port will change from forwarding to listening state until the superior BPDU announcements are stopped. 14 Root guard is enabled as follows:

- set spantree guard root 5/1
- The root guard feature allows us to control ports where we do expect to receive
- STP announcements, and is configured on a per-port basis.

This makes it suited to ports which are connected to other switches. On ports designated for host

access, we will use the *spanning tree portfast BPDU guard* feature. 15 In a normal STP configuration, when a host starts transmitting on a port, a spanning tree calculation is performed which takes 30-50 seconds before the port enters the forwarding state and begins transmitting frames. The *spanning tree portfast* command is typically configured on ports where end stations are attached, and allows the port to immediately transition to the forwarding state, without the delay caused by the STP calculation.

However, a port configured with the portfast feature still participates in STP, and there is the possibility that a device communicating on that port will affect the spanning tree topology and the placement of the root bridge.

The spanning tree portfast BPDU guard feature addresses this issue, by disabling the port if a BPDU is received on that port. This feature is enabled for all portfast enabled ports as follows: set spantree portfast bpdu-guard enable

3.7 Advanced Technologies

I have discussed the physical and logical topology of our LAN, and techniques for building security into the layer 3 and layer 2 design. There is still much that we can do to make our design more secure. In this final section on Advanced Technologies, we will look at a few more technologies used by security professionals to detect and deter crackers.

3.7.1 Intrusion Detection Systems

1. In this section we will briefly consider Network Intrusion Detection Systems (NIDS) and how they can be used in our LAN to detect undesirable activity. Many experts would include IDS as part of the essential elements of securing any network. Network IDS can alert the system administrator to attacks on the network in real time by inspecting the traffic on the wire, and generating alerts if suspicious activities are identified. NIDS can be a regular computer running IDS software, such as the freeware Snort, an appliance type device running proprietary software, or even a specialized card built in to a switch or other network element. Host based intrusion detection, such as free or commercial versions of Tripwire, or various kinds of proactive log monitoring software, are also highly recommended, but outside the scope of this paper. Once we have selected a NIDS for use in our network, we will need to place the sensors logically within the topology. Unless we have lots of resources for maintaining our NIDS, and analyzing and responding to alerts, we will want to limit ourselves to a few well placed sensors. Because we have a switched infrastructure, we will need to connect the NIDS sensors to a specially configured monitoring port where all the traffic from a VLAN is mirrored. In a high bandwidth environment there will be physical limits to the IDS system that will need to be considered as well – a standard PC running IDS software will not be able to keep up with a highly loaded gigabit ethernet VLAN, for example. An alternate and more complex solution is to use network taps, a hardware component specialized for monitoring network connections. 16 Below is a figure which shows how the IDS sensors could be placed in our network:

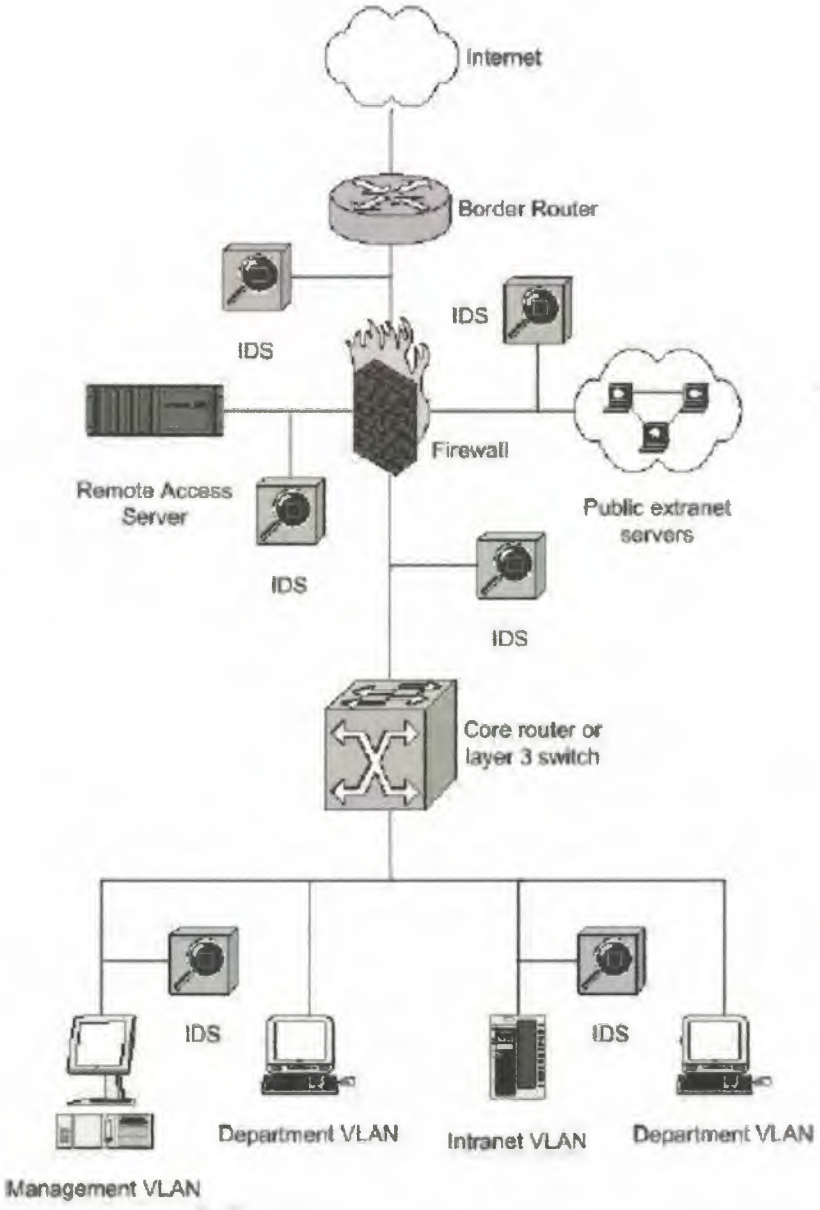

Figure 3: Location of IDS Sensors

We place a sensor on our Internet facing segment, because the public servers are a visible target to attackers. Another sensor is placed behind the firewall, to monitor traffic between the Internet and our internal LAN. If we had a remote access segment, for instance where a

dial-up server or VPN concentrator terminated, this would also be a good place for an IDS sensor.

Finally, we will want to locate a sensor on the more sensitive subnets within our network, the

intranet server subnet and the management subnet. An attack on either of these segments could have very serious consequences. We may also wish to place a sensor outside our firewall to monitor what kinds of attacks are being launched against us, but which are screened out by the firewall. This sensor, if used, will generate the most data and false positives, so the sensitivity should be adjusted accordingly.

3.7.2 Private VLANs and VLAN ACLs

In previous sections we discussed several strategies for securing our layer 2 and layer 3 design. However, as the sophistication of our defenses improves, it is inevitable that skilled attackers will find new techniques to defeat our defenses in the ever-changing "Information Warfare" environment. So the security professional must keep aware of emerging techniques to defend her network.

Two features offered by Cisco on their high-end switches are worthy of consideration in this regard, Private VLANs and VLAN ACLs. 17 Private VLANs allow the designer to enforce a security policy within a subnet. For instance if host A and host B are on the same subnet, typically there is nothing that prevents them from communicating with each other. However, there may be situations where this behavior is not desirable, such as on our Internet facing segment. If a cracker was able to gain entry to one of our public servers, we would logically launch attacks against other hosts on the public segment.

Private VLANs provide a means to prevent hosts on the same subnet from communicating with each other, while permitting required communication to their router and hosts on other networks.

Private VLANs are established by defining a primary VLAN and one or more secondary VLANs on a segment. Hosts defined on an "isolated" secondary VLAN will only be

permitted to communicate to their gateway, and will be prevented from talking to other hosts on the same primary VLAN. Note that host based firewalls could be used to achieve similar results, and are available built in to many operating systems, or from numerous software vendors.

VLAN ACLs (VACLs) are another security enhancement offered on Cisco's highend switches. VLAN ACLs can further enhance the security afforded by PVLANs by preventing undesired traffic sourced from the VLAN.

VACLs also prevents a compromised or misconfigured host from using the gateway to communicate to other hosts on the same PVLAN. Because the ACL processing takes place in the switch ASICs, Cisco's claim is that it can happen at wire speed, thus invoking no performance penalty in high throughput environments. Security is also enhanced because traffic is denied at layer 2, before it even passes to the router for processing.

3.7.3 Micro VLANs

Micro VLANs or Routing to the Desktop (R2D) is another emerging strategy that has been proposed. In this design, each host is placed in its own routed VLAN on a layer 3 switch. This design eliminates the vulnerabilities in spanning tree protocol, arp spoofing, and attacks on Hot Standby Routing Protocol (HSRP). If each port was assigned its own VLAN with a 30-bit subnet mask, there would only be one valid host IP address that could appear there. This would reduce the risks associated with IP address spoofing, or the introduction of rogue machines on the network. While the concept of Micro VLANs is radical, it is certainly feasible with hardware available today.

In specialized environments where a high degree of isolation and security are needed, Micro VLANs may fit the bill.

3.7.4 IPSEC

A final technique that should be considered is implementing security at the network level. Strong encryption and authentication implemented at the network level would prevent all

but the most determined attacker from compromising our hosts, even if he were able to penetrate our perimeter defenses.

IP Security (IPSEC) is an enhancement to the IP protocol documented in various RFCs by the IETF. IPSEC ensures that every packet transmitted on the LAN is encrypted with strong encryption algorithms. While IPSEC has been criticized for its complexity, it is emerging as the standard for network level encryption. 19 IPSEC is the underlying protocol used by many of the VPN solutions currently on the market. And it is finding use in high security environments, or in special applications such as management of network devices over insecure networks.

Within the last few years IPSEC has become widely supported in popular operating systems and broader adoption seems inevitable. Microsoft has included IPSEC in its ubiquitous operating systems, along with an easy to use configuration wizard.

CONCLUSION

- This thesis has examined several strategies for designing a secure Local Area Network. We have identified the need to define a security policy, and balance the organization's security needs with the available recourses.

- Next, we considered a basic topology that allows for the grouping of hosts by functions, and implementation security within the layer three designs.

- We looked at how to implement the layer tow network design securely, implementing layer tow security features and minimizing threats at Layer two. And finally we rounded out our discussion by expressing additional steps we can take to secure the LAN, such as network intrusion detection systems, private VLANs and IPSEC.

- The network architect must exercise careful planning, and attention to detail to maximize the security of the network while meeting the communication needs of the organization.

REFRENCES

1. DWDM Network Designs and Engineering SolutionsJeff Apcar MPLS and VPN Architectures, Volume II
2. Zaheer Aziz
   Troubleshooting IP Routing Protocols (CCIE Professional Development Series)
3. Mastering Network Security by Chris Brenton, Cameron Hunt
4. Network and System Integration for Dummies (With CD-ROM) Author: Michael Bellomo, James
5. Communications Systems and Networks Author: Ray Horak, Mark A. Miller (Editor), Harry Newton
6. Designing Storage Area Networks Author: Tom Clark, Thomas Clark Computer Networks, Fourth Edition by Andrew S. Tanenbaum;
7. Practical Storage Area Networking by Dan Pollack, Daniel Pollack
8. Business Data Networks and Telecommunications (4th Edition) by Raymond R. Panko
9. TCP/IP Illustrated 3 Volume Set by W. Richard Stevens, et al (Hardcover)

11. Storage Network Performance Analysis
    by Huseyin Simitci (Paperback)