Computer networking assignment

Local Area Network (LANA) Topologies In this project, a star topology will be used in setting up a LANA for each school in a small school district. Implementation of a LANA in a school will involve installation of a cabling system to distribute the network resources throughout the infrastructure, installation of wiring to support connections of computers and terminals to the network, installation of one or more network server machines in a central location, tutee simple, by creating a local area network within each school building or cluster of buildings.

A connection from that LANA to the local school county office will be established. At the county office a similar LANA should be installed, where centrally managed information resources exist. Connection from the county offices to the nearest Internet service provider that provides the best user support at the lowest cost will be most important. Local servers will be installed at schools sites to store local information. Primary technical support for network monitoring and problem solution and managing of the network will need to be established.

Different LANA technologies are implemented in many ways to facilitate a stable network. Two of these are Ethernet and Local Talk. Both are quite inexpensive and easy to install and maintain however, Ethernet is roughly 20 to 40 times faster than Local Talk. Therefore, Ethernet is recommended for all computer connections, when possible. This LANA will be implemented using the hierarchy set up. The physical layer will include repeaters, switches, and routers. A repeater is used to extend the distance that network traffic can travel over a particular kind of media.

Switches are used to form fast point to point connections for all the devices connected to them. Routers can route network traffic in a variety of ways and operates on layer 3 of the OSI model. The easiest way to install LANA cabling is to run cables direct from the switch to each computer. This is the cheapest method but does not allow flexibility. LANA cables are called CITE which is unshielded twisted pair and are identified with a category rating. The CAT-5/e/6 cable carries the network signal to each point through four wires often referred to as two twisted pairs.

The twisting of each pair in he cable Jacket reduces the chances of the cable picking up electrical interferences (Halberd, 2006). In this implementation, each school's LANA will be segmented into 2 networks, one for the staff and teachers and one for students. In each school there will be a maximum of 50 to 70 teacher or staff computers and around 100 student computers. Any trunk connections between buildings will be run in fiber optic cable to ensure protection from interference and damage due to lighting. This also allows gigabit Ethernet over fiber to be used for the uplinks.

All other cabling is to be CAT-6 tested to 1000 Mbps. Switches will be employed to provide full 1000 Mbps bandwidth to all users. " The LANA will be implemented using Ethernet BASSETT. Horizontal cabling will be implemented using CAT-6 CITE with a bandwidth of 1000 Mbps. Multimode fiber optic cable will be used for vertical (backbone) cabling. Cabling will conform to the TIA/ Ella-568-A and TIA/Ella-569 standards, and will use a star or extended star topology with an MID containing the POP and network devices with Dif where appropriate" (Lemon, 2003).

The wiring cabinet in each classroom will also house the switches, hubs or other devices for that room. Cables will run from switches in the wiring cabinet to provide access for 1 teacher computer and 24 student network computers. Each school will contain three servers which many teachers utilize computers for instruction. There will be a need for two servers including a server for such as student tracking, attendance, and grading. This server application server accessible to all users, and a third being a library server accessible to all users.

Wide Area Network (WAN) Design The wide area network (WAN) design will enable the network span over a large geographic area, such as the county, state, country, and the world. The WAN connects at least two sites in different geographical areas by transmitting data over a digital connection. The connection is established over digital telephone line that has the capacity to support the bandwidth that is paid for. When the school system wants to connect employees at the different schools' Élan's the WAN is then needed.

Each of the individual and smaller Élan's will be connected by the WAN to enable data sharing and central support of the county network and nodes. Wand's generally use much more expensive networking equipment than the Élan's do. This additional expense is the need for routers at each site and high speed connections to carry the data to the central data center. Use of the WAN will allow all employees or students at the school level in any of the classrooms, labs or offices to exchange files and data as if they were connected to one local network. The WAN has three main components.

The first component consists of the routers that connect the computers on the local Lana' to other workstations, Lana' and other network devices. Secondly, the WAN connections that makes up the actual connection between sites (Frame Relay, T 1, ADS, etc.). Thirdly, there are security strategies to revert people from accessing files and data traveling between sites if they have not been authorized to do so. This is prevented by the use of firewalls at the edges of the WAN that is Internet facing. " It is very important to choose the correct connection type when designing the WAN.

Most carriers offer three types of connections: circuit switched connections, packet switched connections and dedication connections. Analyzing WAN traffic patterns and requirements is the key to a successful WAN" (Tech, 2000). The router will handle all of the tasks of routing and forwarding data between systems. Typically, routers are designed to connect two or more logical subnets, thus allowing for a scale able network of a large geographic area. These network devices contain a very specialized operating system. These operating systems should not be confused with computer operating systems.

The specialized Ox's include Coco's ISO, Juniper Networks' JUNCOS, and Extreme Network's SOX. Each of these Ox's are designed for the specific hardware that they reside on and manage. Within each of these devices reside similar components to that of a personal computer. Most business class routers contain NAVAL, RAM, flash memory, and at least one errors. The higher end routers could contain several processors. In addition, some routers contain specialized application specific integrated circuits (ASIA).

Having this kind of internal processing power allows for parallel processing to take place to increase performance.

There are chassis based systems that have multiple Sais’s on every internal module and allow for a wide variety of LANA and WAN port technologies. Carrier or lines can be leased from service providers who facilitate the connections from client back to the carrier. The nodes are connected to the LANA and then to the WAN. The WAN connections are in place to allow for a seamless transfer of data across large distances. Additionally, smaller networks can be the connections through analog point to point connections and leased lines if throughput is not important. A point to point connection can also be made over a dedicated phone or serial line.

However, the communication equipment at each end has to be capable of maintaining adequate signal strength between the systems to be stable. An analog transmission necessitates the use of a modem to convert digital data into an analog form to be sent over a telephone line. On the other side of the communication another modem has be ready at the receiving end to change the analog signal back into digital data. An analog telephone line’s bandwidth is usually GHz. However, with more sophisticated encoding and compression techniques the transmission of data can be up to 56. Kbps over suitable clean noise free lines.

Institutions that do not necessitate the network to be available to all users at all times, dial-up services can be used to connect remote users or branch offices. Most PC’s are equipped with analog modems to allow users to dial-up and connect to the Internet or intranets. If dial-up or serial connections do

not meet the throughput needs, KIDS can be used. KIDS (Integrated Services Digital Network) lines are available in most areas of the country. Small organizations can take advantage of KIDS BRI service that can provide data transmission at 128 Kbps with the required equipment and software on each end of the connection.

KIDS lines use modulation and demodulation methods to transmit and receive data in a form that can be processed digitally. The available bandwidth for KIDS is Kbps per B channel of a BRI (basic rate interface) KIDS terminal adapter. WAN connections digital KIDS lines can match the bandwidth of a LANA if designed properly. The issues around these types of connections, whether analog or digital, is the latency (lag time). TTL lines are the most widely used connection lines. These lines are basic unit of the telecommunication T-carrier system. A TTL consists of 24 Kbps channels of throughput to reach 1. 44 Mbps of bandwidth. Each of the TLS channels may be used as a separate data or voice channel, depending on the needs of the customer. Otherwise the channels can be bonded together for higher transmission rates. The T-carrier products include the TO. TO lines are becoming more widely used and are the equivalent of 28 TTL lines (44. 736 Mbps). Some higher bandwidth intensive applications have incorporated the use of optical service carriers. These carriers employ SONNET (Synchronous Optical Network). SONNET was developed to connect long-distance carriers and to coalesce different standards.

Data rates are defined in terms of CO (Optical Carrier) levels. CO-I is the first level of CO with rates of 51. 84 Mbps. The most widely used CO level is CO-3 with a rate of 155. 52 Mbps. The largest and best known WAN is the Internet.

Parts of the Internet are also Wants in themselves. These segments are made up of VPN-based extranets. Wand’s are there are others that are built by ISP (Internet service providers) to provide connections from an organization’s LANA to the Internet. Wants are often built using leased lines for connectivity. Leased lines can be very expensive, as this is an ongoing cost.

Rather than using leased lines, Wants can be built using cheaper circuit switching or packet switching methods. Network protocols including TCP and IP deliver transport and addressing functions to networks. Different protocols (Packet ever SONNET, SD, ATM, and Frame Relay) are often used by service providers to deliver the links that are used in Wand’s Ionian, 1999). Fundamentally, WAN connections require several hardware devices to interface between a LANA and a carrier network to facilitate connectivity. When using TTL and frame relay connectivity, a router, CSS, and a DSL are required.

When implemented, these can be housed in separate hardware equipment or into a single integrated device. Once the hardware and connectivity exists, the common routing protocols (P, PIX, Appellate, etc.) are common are then available on the WAN. When using a frame relay for connectivity having the ability to facilitate an increase in bandwidth should be planned. More advanced WAN routers (edge routers) include firewall functionality for security detection and prevention. Any Internet facing router should include the firewall function to protect the internal network users and data from malicious attack.

The firewall function will reduce the exposure to external intrusions and breach of secure data on the internal network. The security features of most firewall able routers allow for the review of security policies and log and malicious behavior. By having this ability of detection, possible intrusions from the Internet are drastically reduced as support personnel can be prompt in addressing malevolent behavior. Required Data Transfer: Application usage: err day Application data transfer: . 25 Kbps Concurrent Users: 1 oho 1000 * . 25 = 250 Kbps per Max 1000 users Network Protocols There are many network protocols.

One of the most utilized is transmission control protocol (TCP). TCP is a set of rules used with the Internet Protocol (P) to send data in keeping track of the data packets routing them correctly through the Internet. TCP is responsible for numbering the packets and forwarding them on to the correct IP program layer. Transmission Control Protocol is able to operate above a wide area of communication systems from hard-wired connections to packet-switched or circuit-switched networks. The protocol layering is important to this type of transmission.

The layers begin with the communication network, and then the IP or Internet Protocol, after the IP is the TCP ranked one level below the higher level. The TCP also includes the source and destination host addresses as well as several other information fields. The TCP header supplies information specific to the TCP protocol. Network Remote Access In today’s age, most schools of any level have realized the need for remote access solutions which extend past traditional school hours. It has become necessary to give

staff and students the flexibility to work remotely with controlled accesses to resources.

Many public schools currently allow access to internal applications either through dialup or virtual private networks (VPN). Dialup access is the least costly, but VPN is the most widely deployed standard. Using PIN strategies give the IT staff ore options in developing security practices and offer the highest connection speed. However, it does increase the equipment costs to support this technology (Lewis, 2007) As teacher rely more heavily on new technologies, Internet access, modem support, and firewall protection for all the different campuses is crucial.

This network will support virtual private network (VPN) access rather than dial up access. VPN is used to give access via the intranet services and servers that are not freely accessible via the public Internet. The authenticating mechanism that will be used is a user name and mandatory strong password. The access is established via the VPN server that resides in the central data center located in the county office of the school system. To use the VPN, each school must possess the appropriate VPN software to distribute to the users (either teacher or students).

Once the users have the VPN client installed in their personal computer, the users will then have access back to their local network and server. When set up properly, VPN solutions are easy to use and sometimes can be made to work automatically as part of network sign on. Secure VPN tunnels across the Internet can connect computers at differing school locations eased on the user’s login credentials. In this way schools in different schools systems can

communicate securely and conveniently. The teachers will need access to their grade books and other files they use on the network.

Administrators can easily grant access to each teacher’s school information making it easier to remain informed of students’ progress. Parents and students will be able to access the school’s homework schedule online in real time and manage cafeteria online payments. Teachers and staff will be able to access email and intranet applications that they would normally use during the time they are at school. Miscommunication to sustain system reliability and ensure that users are using the system responsibly and within school guidelines.

Users should not expect that any files will be private, as all the equipment is owned by the school system. TCP/IP will be the protocol that is used with cryptographic protocol PIPES. PIPES will secure all packet transfers between the remote network and the client computer. TCP/IP is now a popular network protocol that enables communication between computers. The TCP/IP protocol is over 30 years old. TCP and IP protocols were developed by the U. S. Litany to allow computers to talk to each other over long distance networks.

IP is responsible for moving packets of data between nodes. TCP is responsible for verifying delivery from client to server. TCP/IP forms the basis of the Internet and is built into every common modern operating system such as the latest versions of Windows. In the TCP/IP protocol, the IP corresponds to Layer 3(Network layer) of the OSI model. The TCP protocol

corresponds to Layer 4 (Transport layer) in SO’. Both of these protocols are usually used together and are often referred to as one protocol.

As imputer networking continues to grow in popularity, a basic understanding of TCP/ IP becomes crucial to students and parents as well as to the members of the school community. Advantages of VPN Remote Access: Access to internal applications on the school network Authentication system to ensure identity Easier to manage and support Reduction costs- don’t have to buy servers and applications for each school (shared resources) Security to ensure that protected information remains private Less need for technical support at each school Ease of use Scalability Compatibility with broadband technology Privacy kook up students’ medical information.

E-mails can be automatically sent to parents, teachers, and staff notifying them of student absences, changes in schedules, school holidays, and other events. School staff becomes more efficient. Increased geographic connectivity Disadvantages of VPN Remote Access: Central point of failure-if something happens with the county office equipment Additional cost to ensure high availability (redundant systems- UPS and Can’s) Communication lines (TLS or Frame relay) needed from each school back to the county office’s data center can be costly. Nothing encrypted beyond the VPN server

Security requires a strong/complex password Technologies from different vendors do not always integrate well together With dial-up remote access, a remote access client uses the telecommunications infrastructure to create a temporary physical circuit or a virtual circuit to a port on a remote access

server. “ After the physical or virtual circuit is created, the rest of the connection parameters can be obtained. Connections are established by remote access clients that call the remote access programming interface, which, in turn, uses TAP to pass call connection information to the dial-up equipment.

After the physical connection is made, TAP is no longer used; other remote access components negotiate the connection with link, authentication, and network control protocols by communicating directly with INDIANA. “(MS Techno, 2008). When accepting calls, the remote access server gives instructions to each WAN omnipotent driver to indicate when it begins line up. Then the WAN omnipotent driver passes the line up through NDIS to the TAP sections. The INDIANA and the remote access components negotiate the rest of the connection. Some modems that can support dial up remote access are V. , VIA and other lower modems which are supported at connection speed of Kbps to 28 Kbps. Once connected via dial-up, users can then access resources on the local area network (LANA), such as email, network shares, and the Internet. With virtual private network remote access, a VPN client uses an IP intervention to create a virtual point-to-point connection with a remote access server acting as the VPN server. After the virtual point-to-point connection is created, the rest of the connection parameters can be negotiated. VPN offer a low cost, easy to deploy and harnesses the flexibility and ubiquity that the Internet offers.

This gives us the perfect balance between security and ease of use. VPN will help schools and other organizations to meet business, security and information technology goals of securely opening up systems to remote

users at an attractive level of investment. Using a VPN, allows students to be able to practice working on skills and assignments which were not completed while at school. This also allows students to prepare for excellence when it comes to state and federal assessments. It also solves the problems of running miles of wiring through concrete block walls.

VPN also link parents to teachers and provide teachers and arenas with student information when outside the school. Parents now have access to the schools' VPN which allows them to have access to their child's grades at any time. Security will continue to be a concern of school systems. As technologies progress, adequate security can usually be provided with good preparation, design, technology selection and management practices and at reasonable cost. VPN security contains several elements to secure both the school's private network and the demoralized zone (DMZ) network. The first level of security is usually a firewall that guards the

DMZ servers (Web server, application servers, etc.) and core networks. Schools should have a firewall between each school to increase the security and to silo off any intruders that may break through the edge routers and firewalls at the county's decanter (which is the connection point for the private network). The remote user will establish an authenticated connection with the firewall that has connections back to the core networks Active Directory user base (to centralize user administration). Strict security is important for all school districts to implement a system to protect school data such as student records etc.

Using a VPN can accomplish this by providing a secure communication system. Monitoring VPN traffic and firewall logs is crucial to proving a successful and secure remote access solution. Network Business Applications Today, it seems email is a lifeline to the business and government world. Email servers in a work setting can vary, but MS Exchange 2003 servers are predominately used. These servers provide POP, ESMTP, and NNTP services for an organization. Additionally, database servers are needed for a variety of fronted applications, but these servers are primarily Oracle or MS SQL database servers.