Network design essay

This was accomplished by breaking down all of the sections and building upon all previous assignments. This was a good course as I learned a lot about all of the deferent sections of building a network. The pros are now I know how to build a network on the design side from the ground up. I learned quite a bit about using a lot of the technologies associated with networking and It allowed me to learn quite a few new concepts.

Some of the downfalls about this course and what I have learned are I did not feel I accomplished much as there Is no hands on training associated with the course. I do not feel Like concepts and design Ideas are a great resource to actually learn how to use any of the systems but they do give a pretty good Idea. Cabling Spectrophotometer’s is a Local Area Network (LANA) technology with a transmission rate of 10 Mbps and has a typical star topology. Computers and devices must wait-and-listen for transmission time on the network as only one device can transmit at any one time.

In order to operate with this network strategy, Ethernet incorporates CAMAS/CD (Carrie Sense Multiple Access with Collision Detection). Each device on the network listens for the network to be clear before transmitting data. If more than one computer or device transmits data at the same time, then collisions occur. Once collisions are detected, all devices stop transmitting for a period of time until one of the devices senses the line is free and will then gain control of the line to transmit its data. Receiving devices Just sit there waiting and listening for transmissions that are meant for them, which are determined by an IP (Internet

Protocol) address. The main advantage to Ethernet is it is one of the cheapest networks to put Into service. Compared to other hardware for Token Ring, Ethernet equipment such as hubs, switches, network interface cards, and cable (ACTA common) is inexpensive. The mall disadvantage to Ethernet Is related to the collisions that occur on the network. Even though Ethernet cable (ACTA) Is fairly Inexpensive, It can become a cost Issue If designing a large network as each device or computer requires Its own cable connection to the central hub. Another disadvantage Is distance Limitation for node inspections.

The longest connection that can occur wealth an Ethernet network without a repeater Is 100 meters. Today’s Ethernet standards, 100 Mbps and 1000 Mbps, incorporate switched technology, which for the most part, eliminates collisions on the network. The IEEE (Institute of Electrical and Electronics Engineers) specification for Ethernet is 802. 3 with three-part names designating the different types. For example, BASES-T is for Token Remington was developed by IBM as an alternative to Ethernet. The network is physically wired in star topology, but is arranged in a logical ring.

Instead of a hub or switch like in an Ethernet network, a AMA (Molestation Access Unit) is used. Access to the network is controlled by possession of a token that is passed around the ring from computer to computer as data can only travel in one direction at a time. A computer that wishes to transmit data on the network takes possession of the token and replaces the token frame with data. The data goes around the ring and returns to the transmitting computer, which removes the data, creates a new token, and then forwards it to the next computer.

The IEEE specification for Token Ring is 802. 5 and it moms in two different speeds: 4 Mbps and 16 Mbps. The main advantage to Token Ring is there are never any collisions within the network, which makes it a highly reliable solution for high-traffic networks. The disadvantage to Token Ring is the network cards and AMA are more expensive than equivalent Ethernet hardware. FIDDLED (Fiber-Distributed Data Interface) is an architecture designed for high- speed backbones that operate at 100 Mbps, which are used to connect and extend Lana.

A ring topology is used with two fiber optic cable rings. It passes a token on both rings and in opposite directions. The specification for FIDE is designated by the American National Standards Institute as ANSI EXIT. 5. The advantage to FIDE is that it uses two rings for protection in case one ring breaks. When a break occurs, data is rerouted in the opposite direction using the other ring. It is also considered reliable because it uses a token-passing strategy. The disadvantage to FIDE is the expensive network cards and fiber optic cable.

In addition, the amount of fiber optic cable is doubled because it has redundant rings. Wirelessly Area Network (LANA) Topologies mesh topology has a point-to-point injection to every other device (node) within the topology. The point-to-point link is dedicated between each device so it will only carry traffic to the two devices that is connected by that link. The advantage of a mesh topology is it works on the concept of routes, which means that traffic can take one of several paths between the source and destination.

The network is also robust in that it will not be crippled if one path becomes unavailable or unstable due to each device being connected to every other device. The Internet uses a mesh topology to operate efficiently. The main disadvantage to a mesh apology is the fact that it requires a large number of cables, which is very expensive. A bus topology is a multiplying topology that entails each device being connected to a network. All devices typically connect to the backbone with a T-connector and coax cable.

The main advantages of a bus topology are that it is easy to install and is not expensive (cost effective) because it uses very little cable to build. The main disadvantage is if there is a problem with the one backbone cable, then the entire network will no longer have the ability to communicate. These networks are also very official to troubleshoot because any small problem such as a cable break, loose connector, or cable short can cause the outage. The entire length of cable and each connector must be inspected during troubleshooting.

Another disadvantage is the lack of amplification of the signal, which results in a limited network size based on the characteristics of the cable because of how far a signal can travel down that A ring topology means that each device is connected in a ring, or daisy-chain fashion, one after another. A dedicated connection only exists between a device and the device on each side of it. Data flows around the ring in one direction. Each device contains a repeater that regenerates the signal before passing it to the next device. The main advantage of a ring topology is that it is easy to install.

One disadvantage includes difficulty to troubleshoot because data flows in one direction and it could take time to find the faulty device when there are problems. The entire network could be taken off line if there is a faulty device or cable break within the ring. The star topology has each device in the network connected to a central device called a hub, which can actually be a hub or switch. All traffic must pass through the hub in order to communicate with any other device on the network. There is no direct communication between devices like in a mesh topology.

One advantage to a star topology is any failure to one cable or device connected to the hub will not bring the entire network down. Repairs can be done to individual nodes without disrupting traffic flow. Another advantage is expandability of the network. Additional devices can be added to the network without disrupting any of the current users. All that is required is an additional cable run from the device to the hub. One disadvantage includes cable costs because each device must have its own cable connected back to the hub. The other disadvantage is the hub itself.

Since all traffic runs through one device, it becomes the single point of failure. If the hub goes down, so does the entire network. Wide Area Network (WAN) Designs WAN, also known as a Wide Area Network, is an essential part to bigger corporate networks most government networks and companies with multiple sites as well. A WAN, basically, is 2 or more Lana (Local Area area. Although a WAN could cover very small distances, most Wants cover much argue geographical areas such as a country or possibly even the world. The largest WAN today would technically be the internet or the World Wide Web.

The internet is, in short, one giant WAN because it consists of many smaller Lana and servers. Most Wants can cover a fairly large geographical area, but some, such as the World Wide Web can cover the globe. The United States Government has quite a big WAN as a lot of their Lana are in other countries. They need to get data from one place to another almost instantaneously, and this is one of the quickest and easiest ways to be able to do so. To be able to get on the internet, a subscriber must go through an ISP (Internet Service Provider) and they will give the subscriber access to the internet for a certain price every month.

There are different ways to get access to the internet depending on the geographical location in which you live. A subscriber can go through dial up, which is one of the slowest methods, but it is also one of the most common. There is also DSL (Digital Subscriber Line) through most phone companies if they have access in the area and cable which is usually one of the fastest and most expensive methods o access the internet. The last common method is using a satellite to obtain access. This is usually the most expensive ways to access the internet because the equipment usually needs to be bought.

When talking about telephone lines, we start getting into analog versus digital signals and degradation over longer distances. A telephone system works on analog signals. These work by a computer transmitting a digital signal to the modem which converts the signal into an analog signal (this is the beeping heard when a computer dials up to access the internet) and later being converted by a different computer jack into a digital signal with the use of a modem. DSL is digital all the way, along with TTL and TO lines.

When using DSL or TTL/TO lines, a filter of some sort is used to filter out the digital and analog signals, so the phone and computer are receiving different signals. Companies usually use faster lines to access the internet or to have access to their other sites. Smaller companies can use DSL or Cable internet services, but when talking about larger corporations or the government, most use public systems such as telephone lines or satellites. Usually, when talking about larger companies and ongoing through a public system, we are talking much faster speeds that can hold many more users.

TTL and TO lines are usually used, satellites are commonly used and fiber-optic is becoming much more common. When getting into many users on a WAN, we need to start talking about Network Latency. According to Jawing. Com network latency is defined as Latency is a measure of how fast a network is running. The term refers to the time elapsed between the sending of a message to a router and the return of that message (even if the process Latency problems can signal network-wide slowdowns, and must be treated seriously, s latency issues cause not only slow service but data losses as well.

At the user level, latency issues may come from software malfunctions; at the network level, such slowdowns may be a result of network overextension or bottleneck, or DOS or Dodos activity. Dos or Dodos stands for Denial of Service and Distributed Denial of Service respectively. These types of attacks are usually by hackers or someone who does not want others to access a certain service. There was a recent DOS threat on the CNN weeping as some hackers wanted CNN to stop talking about a certain issue.

This works by one or multiple people talking all of the networks latency or bandwidth from them and thus causing other not to be able to access their site or services. There are other issues that may slow down a users PC as well. Not all issues revolve around hacker attacks. A lot of problems could be caused by malicious software, such as, Spare, Mallard, Viruses, or other programs that may be problematic. These can usually be taken care of by installing anti-virus software or even a spare removal tool.

The issue here is instead of the malicious software causing slowdowns on a PC, here are slowdowns due to the software protecting a certain computer in the background. Sometimes a simple fix to this problem is to defragmenter a hard drive. This can tremendously speed up a PC, because the files will be closer together and easier and quicker to access. On a network, a simple way to test latency is to use the trace route program. To do this, simply go to a command prompt and type tracer and then an IP address if internal or a website if external.

This will send out packets of information and check how much time has passed to receive a packet back. The time passed would be the latency time. Usually it says it only took a certain amount of milliseconds which does not seem like very much time, but it was only a tiny packet of information. The higher the milliseconds the higher the latency time. The higher the latency time, the longer it will take to do anything in a network. If a high latency time is present, there is bound to be lag somewhere down the line. In a WAN, the equipment that will be used is as follows.

In each LANA there will be PC's connected to a router somewhere (this is a ring topology example) and that router should be connected into a switch. There may be more but this is a basic example. Each of these Lana then connects to a central HUB somewhere which should interconnect all of the Lana. All of the information then travels to the central hub which is then separated out to the correct switch, router and then PC. There are usually central servers that can store and backup all of the data on the network as well, but this was an example of a crude network. Most companies also a very repetitious and redundant with their WANTS.

This is because they do not want a central failure point to bring the entire company to its knees. There are usually multiple switches that can tie the entire system together. If a huge corporations Wan decided to fail, the company could lose a few million dollars more than enough sense. A lot of companies use software called VPN software. This software will let users login from the outside into their computer inside the company. This is a very nice system because if an employee needs to do work from home, they have access to everything they working on onsite.

This is also helpful from an Information Technology perspective as it allows the Tech who is working on a remote problem login remotely and find out what the issue is, make any configuration changes and fix cost software related issues without actually having to be onsite. This works well when being on call from an offset location. There are other software packages that work well too. A lot of companies use Pachyderm to do this type of work and Bombard is another solution to be able to remotely login.

A WAN is an imperative part to any corporation, government agency or company with multiple locations, as it allows them to transfer data quickly, easily and over great distances at the click of a button. There seems to be more and more need for employees in the networking field today, because more and more corporations need o transfer data quicker and easier. There will be new technology soon that will improve our current technology such as fiber optic. Network Protectorate’s are many solutions to remote access and the most common and one of the most cost efficient methods is the VPN (Virtual Private Network).

VPN technology is already built in to most operating systems and is very easy to implement. With bigger environments and corporations, a consideration for concentrated VPN hardware should be in place because of the simultaneous users and stress on the servers. There are a few different types of VPN including Pipes, PPTP and SSL. Once the connection from remote access has been made, you need to make sure the files are readily accessible for the user logging in remotely. One way to do so is to use Samba which is an open source file access system. There are other ways to allow access as well.

Using remote desktop connection, the user has the ability to log directly in to their PC and use it as if they were sitting at their desk, rather than away from the company. Login remotely and find out what the issue is, make any configuration changes and fix Network Remote Accessions companies need to be able to access their work from any locations, including home and while traveling. The solution that allows them to access the network is one of two ways to access their network. The first is through a VPN (virtual private network) that allows the user access to remotely log in easily and quickly.

The other way is through a dial up remote connection; this way is a bit easier to set up but can become very costly in the long run. The problem with being able to do this is it can be very costly and can eat up much of the IT departments time to set up, configure and implement this system into the current hardware. The definition from what's. Mom about a VPN is 0 virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost. VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (LOTT). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a " tunnel" that cannot be " entered" by data that is not properly encrypted.

An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses. AAA VPN, also known as a Virtual Private Network is a helpful tool that allows users of a specific domain to be able to log in to their PC from anywhere in the world with the help of another PC. With this tool, they would log in with a special ice of software, using their user name and password to gain access to all functionality of the PC they want to log in to.

This allows for a lot of comfortable solutions, such as if an employee is sick, they may still have an option to work from home. This allows a flexible company schedule as well because if a user needs to access a document from their home PC, they can essentially log in to their work PC and download the document. Network Business Applications second way to access ones computer from a different location would be using a dial up service, with this you can basically dial in o access all of their resources available within the server.

Using this is a very secure and easy route to go, and allows the user access to files they may desperately need. Another good thing about using a remote connection to access a server is if the user is on a business trip, they have the ability to access all of their much needed documents easily and securely with out much fuss. The explanation between these two pieces of technology is Tooth 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 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. There are many advantages and disadvantages to using a dial up remote connection over VPN. The biggest advantage I have been able to find is, it is easier to set up and maintain while using VPN makes you set up and maintain individual accounts for both the VPN and the users name and password on the system.

Another advantage of dialing up in to the system would be the fact that no matter where the user is all they need to do is plug into a phone Jack and they should be able to log in. The disadvantage of this is depending on where the user is long distance charges may apply and it could rank up a pretty penny or two. Another disadvantage is although the system is cheaper in the short term, the system may be more expensive than VPN in the long run. There are also other methods of using VPN.

One specific way is certain Sips (Internet Service Providers) and other third party support companies are assisting in setting p the VPN and supporting it without a great deal of time spent on it by the current department. This may or may not be more cost efficient than setting it up yourself, but it does remove a lot of the headache that Van’s can give due to different errors. There are also many advantages and disadvantages to using a VPN over a dial up system. One of the biggest advantages to this system over a dial up system is in the long run this is a much cheaper system than a dial up system.

This system is a little bit quicker than a dial up system as well. This system is cheaper than a dial up yester because using a dial up system, long distance fees may apply, with the virtual private network, you do not need to worry about this as the user may call into a local internet service provider to gain access. Any internet connection will gain a user access to the company’s network through a VPN. Through all of this, there still needs to be security measures put in place to keep unwanted users off of the system while allowing employees or other authorized users access without down time.

Van’s can work well with firewalls, all the IT department would need to do is allow the ports to be accessed by the VPN and the user should eave full access. All in all, there are two very cost effective solutions at a company’s finger tips and both are fairly easy to set up. The company needs to decide if they want to save money up front and make it easier so they do not need to set up multiple accounts per user, or if they would rather have a better solution and save more money down the road. The choice also depends on the amount of users logging in at any given moment.

Backup and Disaster Recoverability, back ups and disaster recovery are all important very parts of all networks in today’s world. The problem with today is information on how to hack, destroy and program any type of malicious software (or are roughly 1. 4 billion people on the Internet or that at least have access to the Internet in the world, which is about 25% of the world’s population. All of these people have extremely easy access to hacking networks, creating mallard and destroying any personal or private data a user may have and wish to keep.

There is not really any way to stop these people from harming our personal software and data from their side, this is why a user needs to make sure they have security on the user’s side. There are other things that happen besides people trying to maliciously harm a user’s files and data. Accidents can happen and destroy data as well. There could be many things that can harm a user’s data such as a fire, earthquake, power surge or worst case scenario, some sort of electro magnetic pulse (AMP). This is where data back ups and disaster recovery come in nicely.

There are many companies that specialize in helping a user or company back up their data and store it off site such as Singular (mostly used in bigger company settings). There are other ways to store a user’s data as well. One way is to make a physical copy of everything needed on Cad’s, DVD’s, Flash Drive or some other type of media and store it at a friend’s house or some other person’s house they trust. This keeps a hard copy of all of their data off site Just in case something happens and it can now be restored. There are a few other companies as well that offer on line backups.

For this a user downloads their software and it automatically backs up to a few different location for redundancy which allows the customer more safety and easier access to all of their files. One of the first steps to a business that wishes to be very secure in all that they do is o set up a backup and disaster recovery plan to start it all off. Like I stated earlier, there are many way s to do it. If this is a larger company they probably want to hire someone internally to make a physical back up of all the data and send it to an off site company for storage.

They should also keep another copy close to them at all times, preferably away from where the physical data lies. They should put it on the opposite side of the building than where the file server is. If anything happens to the servers, they can quickly and easily use their backed up copy of all the data and cover it on to the servers in which they lie. Most companies have 2 or 3 backup units on site for redundancy and this allows that if one of those go down as well there are still a couple others in which they can restore all of the data from.

Although this can become a little more expensive than Just a regular back up system, sometimes it can be well worth it. Network Carcinogenicity to deep. Com Tote first step in drafting a disaster recovery plan is conducting a thorough risk analysis of your computer systems. List all the possible risks that threaten system uptime and evaluate how imminent they are in our particular IT shop. Anything that can cause a system outage is a threat, from relatively common man made threats like virus attacks and accidental data deletions to more rare natural threats like floods and fires.

Determine which of your threats are the most likely to occur and prioritize them using a simple system: rank each threat as low, medium, or high. For example, a small Internet company (less than 50 employees) located in California could rate an earthquake threat as medium probability and high impact, while the threat of utility failure due to a power outage old rate high probability and high impact. So in this company’s risk analysis, a power outage would be a higher risk than an earthquake and would therefore be a higher priority in the disaster recovery plan. Another big part of any security system development is the company (or department) needs to look at their budget and how much they are willing to spend on their system. A company can get a basic security system for their network (including firewall) for fairly cheap and this may do most of what is needed, but larger companies are going to need to spend quite a bit more money than that of a small company. Most larger companies spend quite a bit because they usually have higher priced clients that they can not afford to lose and all of their data is invaluable to the company.

Some companies actually have their own Information System Security employees to monitor the network in case of any type of attack. They also make sure all of the anti-virus and anti-mallard software are running and updating properly. Lastly, another thing most companies forget about after they have their equipment and software installed is there is more than Just the implementation of the hardware and software to save them. They need to make sure everything continues to run and update itself from newer and bigger threats.

These companies need to make sure they continually test and check what needs to be done to continually maintain a network that can not be broken in to. There are people out there that can be hired to try and break into a companies network. They get paid and let the company know what needs to be fixed so others can not break into it as well. In conclusion, a company can be nothing or brought to it’s knees with out it’s network and servers. There are many things that can cripple a company without the help of man.