The Building of a WAN with multiple locations and Redundancy

Paper Contributors

Jamie Ashe, Brian Bergstrom, Latosha Franklin, Charles Dowd, and David Bass

American InterContinental University

Week 4 Group Project

Instructor Michael Pry

Class ITCO251-1701B-01

Abstract

In this project, we will talk about the Local Area Network, host to host switch using different cables and wireless options. We will talk about the LAN back bone and the use of fiber optic cables. Wide Area Network design and the use of a primary connection and a backup for redundancy. We will give a summation as to how the design addresses availability, reliability, and performance. We will give recommendations regarding network security such as hardware and security policy. Finally, we will discuss high level disaster recovery and business continuity. We will also talk about the items needed and the cost to have this type of Wide Area Network.

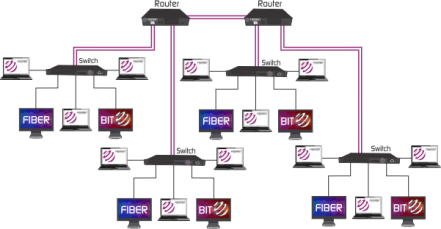
Contributors to the Group 4 Project

* Local area network (LAN) (Host to switch using a hybrid of cables and wireless option). **Charles Dowd** Turned in and contributed.
* LAN backbone design (utilizing fiber optics). **David Boss** Turned in and contributed.
* Wide area network (WAN) design with a primary connection and backup for redundancy. **Jamie Ashe** Turned in and contributed.
* IP addressing scheme for the organizations network (Class B private network address). **Eliane Livulo** assigned did not turn in did not contribute.
* Summation as to how design addresses availability, reliability, and performance requirements. **Latosha Franklin** Turned in and contributed.
* Describe recommendations regarding network security such as hardware and security policy. **Brian Bergstrom** Turned in and contributed.
* Suggest high level disaster recovery or business continuity plan. **Brian Bergstrom** Turned in and contributed.

The Building of a WAN with multiple locations and Redundancy

Our proposal for your new LAN networks are going to consist of Cat6 (Category 6) or Cat5e (Category 5 enhanced) cable running from all host devices to switches in the wiring closet. The devices include computers, printers, VoIP (phone systems) and any other devices that you want wired. Wired is always more secure, faster, and more reliable than wireless. There are some significant differences between Cat5, Cat5e and Cat6. Cat5 is becoming outdated because of its speed disadvantage – it can only carry speeds from 10Mbps to 100Mbps. You may be able to get faster speeds if the cable is very short, but in our situation, that isn’t the case. Cat5e, however, is made to support speeds of up to 1000Mbps “gigabit” speed. Cat5e, also, cuts down on crosstalk, which is interference that that is sometimes found in Cat5 cables. Cat6 is a huge step up from Cat5e – is capable of speeds of up to 10Gbps. Since we are starting from scratch, I recommend Cat6. It isn’t much more expensive and you won’t have to replace it later. I’ll tell you now, rewiring an entire building is expensive and time consuming, which leads to down time on your end (Gordon, 2013). On to switches – as we know, switches are like routers. They learn addresses and send/receive the correct data the correct device. As I mentioned before, all devices will be connected to switches via Cat5e or Cat6 cables. These switches will now be connected to routers with multi-mode fiber optic cable. We have chosen fiber optics for the backbone of this entire system because there are so many advantages and expansion capabilities. Fiber optics are the future and it’s best to implement them now than having to rewire the whole backbone of your system later. They say 82% of organizations are utilizing the cloud in some way today. Fiber optics makes it capable to access stored data and applications from the cloud. Some other advantages of fiber optics, other than speed, are reliability, stability, cost savings and more. Fiber optic cables are stronger than copper wire, they are less susceptible to bad weather and electrical noise has no effect on it. Fiber optic cable doesn’t lose signal strength like its counterparts. It can be run massive distances without needing a repeater (Collins, n.d.). As you can see, there are many advantages to fiber optics. One big one that I didn’t get into detail on was cost savings. I know you’re thinking, “how can this expensive cabling save us money?” Well, it is said that business without fast access to the internet, or the cloud, have employees with a lot of downtime. In turn, you are paying employees to sit and wait on pages to load or programs to open, etc. The switches, within the closet, will be connected to routers via fiber optics. We will, also, implement a few wireless access points around the building in strategic places – these will also be fiber optic. This way anything that can’t be wired can still have internet access. If you have some people that work from home, we will need to implement a VPN (Virtual Private Network), so they can have encrypted access to the network.

The backbone of a network is very important because it is what each device will use to connect to other devices and the internet. Think of the backbone being the network highway of your company and each user has a car to drive on this highway. The fiber optics cable will be the roads that these cards drive on with stops like a switch to make sure the data gets where it is going. Each user has an address which will be assigned via IP addressing so we can identify the source of the problems quickly. Within the company with will use parallel backbone to ensure efficiency and redundancy. With multiple devices connected to switches which have their own subnet mask to be able to identify each sector if something would break. The subnet mask could vary from room to room or a section of cubicles. These to save cost will all be a single connection from the switch to the network interface card installed in each machine. The switch to the router will be connected twice to allow for redundancy so an entire group of subnets does not go down. As well we can connect another switch directly to the router to run wireless routers so there is Wi-Fi capability. With choosing only to use duplicate connections on the switches and routers this will allow the cost to go down considerably as well as the amount of cabling used also. Below is an image showing the basic structure of the parallel system



.

The design of our WAN will have a primary network and a secondary network for redundancy. Multiprotocol Label Switching (MPLS) virtual private networks (VPNs) have long been ideal for the enterprise WAN. Secure, reliable, and high-performing, they offer business-grade traffic control features particularly well-suited to carrying real-time and business-critical data. Combine these characteristics with the single-operator nature of MPLS VPNs and end-to-end network service-level guarantees. Both networks will come from an ISP, however instead of having one ISP we will be going with two entirely different ones, which is why we are putting the second ISP as our backup. For our overseas offices, we have built Hot sites in case something where to happen to one of our office buildings. The second office buildings have been placed in the same geographical areas as the original buildings.

The version of MPLS that’s generally used to encapsulate connection-oriented frame relay and ATM services is called pseudo Wire Edge to Edge Emulation (PWE3). PWE3 defines point-to-point tunnels across the MPLS backbone, and thus works well for circuit-oriented networking protocols. PWE3 can also be used to support connectionless LAN protocols, but it’s not the preferred solution.

For connectionless protocols (primarily Ethernet) there’s a different specification, called virtual private LAN service (VPLS). VPLS addresses some of the specific challenges with extending Ethernet across the metropolitan area or WAN, most notably scalability and availability. Another emerging spec is the ITU’s transport-MPLS (T-MPLS), which is designed to simplify deployment of Ethernet services

It’s worth noting that MPLS isn’t the only game in town when it comes to Ethernet services, though. Several vendors —including Nortel, Extreme and Siemens — are promoting an alternative approach called Provider Backbone Transport, or PBT, for metropolitan area Ethernet.

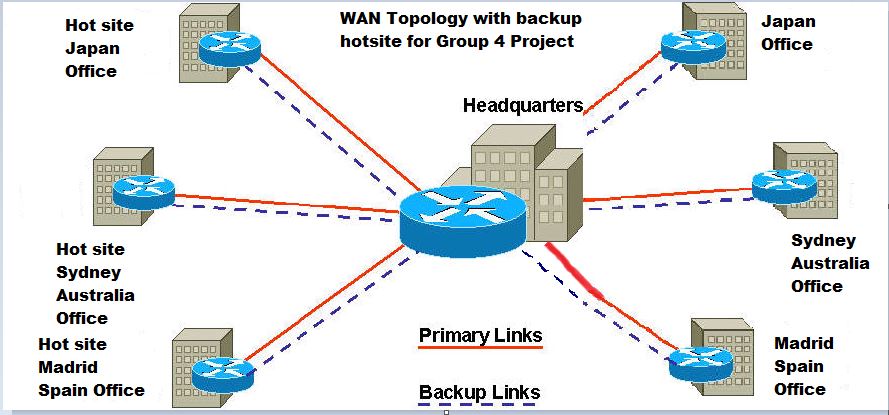
PBT is based on using existing IEEE 802.1 VLAN tags to deliver Ethernet services across a provider network.

Finally, a variant of MPLS called Generalized Multiprotocol Label Switching (GMPLS) gives routers the ability intelligently signal the optical layer, enabling providers to establish, change or tear down optical links in real time. Thus, service providers can provision “optical wavelength” services based on MPLS (Johnson, 2007)

The second part of our design will a cable back up. This type of network is inexpensive to build. All our computer would CAT6 cables ran from the computer to the ethernet port in the walls. From there we would run our CAT6 from the ethernet port in the wall to the switches that we would be plugging our computer into. We would be able to use patch cables to run the connection from the switch to the routers. From our routers, we would run fiber to the servers to get our 10Gbe speed. Our organization has several buildings or sites connected in a campus or metropolitan area, 10 GbE can be a cost-effective way to link these sites. This is because 10 GbE is a full-duplex protocol and is fully compatible with any Ethernet-based network. The 10 GbE standard, which also supports single-mode and multi-mode fiber systems, is expected to be compatible with twisted-pair copper, and can connect to synchronous optical network ([SONET](http://searchnetworking.techtarget.com/definition/Synchronous-Optical-Network)) and synchronous digital hierarchy ([SDH](http://searchnetworking.techtarget.com/definition/SDH)) wide area networks (Kirvan, 2017). A secondary Ethernet infrastructure greatly simplifies the entire network management process, because every device uses essentially the same protocol to communicate. However, situations where multiple protocols coexist in the WAN mean that network management and diagnostic systems must be compatible with all protocols in use for network administrators to analyze network performance.

The hot sites would be set up in the same manner as the original buildings that are currently being used. The wiring and the amount of equipment would be the same so that if something did happen to one of the original sites, the move to the hot site would be a smooth and easy transition.

Below is a typology of what our WAN network would look like, along with the Hot sites shown.



Designing the address availability is about anticipating, detecting, and automatically resolving hardware or software failures before they result in service errors, event faults, or data corruption which could result in downtime (<https://msdn.microsoft.com/en-us/library/aa291866(v=vs.71).aspx>). It’s important to design an availability that keeps in mind of possible failures in the system and have a good recovery technology that is also quick. The technology aspect of it includes multiply routes to data and application services. It’s also important to plan for possible downtime, upgrades, maintenance changes, backups, or any service or activity that temporarily removes the application from service.

Reliability represents the probability of components, parts, and systems, to perform their required functions for a desired period with failure in specified environments with a desired confidence (<http://www.weibull.com/hotwire/issue26/relbasics26.htm>). Reliability does not account for any repair actions that may take place. It also does not reflect on how long it will take to get the unit under repair back to working condition.

Performance requirements are important to have so systems will have something to abide by to meet their performance targets. Performance requirements must be clear and specific. Incorrectly defined performance specifications can lead to many issues.

To assess the performance of a system the following must be clearly specified:

* Response Time
* Workload
* Scalability
* Platform

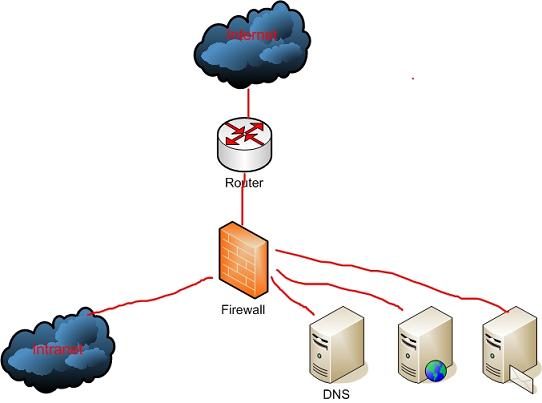
<http://www.1202performance.com/atricles/how-to-write-performance-requirements-with-example/>

Response time is an important to have clearly identified. The general advice on response time is a 0.1 second limit for having the user feel that the system is reacting quickly. 1.0 second limit for the user’s flow of thought to stay uninterrupted. About 10 seconds for keeping user’s attention focused on the dialogue. The workload profile is an important performance requirement because the system depends on this to determine how the load is delivered to the system. The scalability requirement is needed to determine any increase in the system’s workload. However, the issue with scalability is that it may not be economically viable to test the scalability as often as it requires because it often requires additional hardware. A platform is also needs to be taken into consideration because it underlies the hardware and software (operating system and software utilities) which will house the system.

It is important for the network administrator to monitor the security of the network. Lots of things can happen to a network if it is unprotected and not cared for properly. Hackers are always looking for small vulnerabilities to infiltrate themselves into a company network to steal sensitive consumer information that can do a lot of damage for both the company and the people involved. That is why it is important to practice good security measures to keep valuable information safe.

Everyone in the company should be very familiar with the company policy regarding even the most basic computer use rules. Simple things like creating a good password and not sharing your password may seem like common sense, but it’s simple mistakes in those areas that can allow unauthorized access on the network. Much of the security breaches that happen in companies are not external, but internal, meaning the attack was done from inside the company. In 2016, “IBM found that 60% of these attacks were carried out by insiders” (Zadelhoff, 2016). Who has access to what should also be made clear and monitored. No one should have administrator access to the router or network unless they are qualified personnel approved by the company. Employees should report any suspicious activity they see immediately. Waiting can cost eventually.

How the network is configured is also a very important factor to consider. Isolating subnets is way of controlling where a virus or malware might go so it does not spread throughout the entire network (Parker, 2006). This is especially key for larger organizations.



(Parker, 2006).

The router is the first thing something will encounter when entering the network. It is vitally important the administrator keeps a tight lock and key on access to it virtually and physically. Unauthorized access again can cause a lot of damage to the network and cost the company a lot of money in repair costs. Following safe practices saves money overall, even if extra money is spent on keeping security lock tight. By the year 2020, “organizations are expected to spend $101.6 billion on cybersecurity (Vanlan, 2016). A company that spends little on security will be very unsecure and may lose business due to customers getting their information hacked so security breaches occurring on a regular basis.

Before anything gets inside the network, it has to go through a firewall. “A firewall is specialized device, or a computer installed with specialized software, that selectively filters or blocks traffic between networks” (Dean, 2013, p. 508). Each building should have one as it is the last line of defense before the breach can occur. Securing the firewall might be a pain, blocking certain access to other things, but it is necessary for security to run smoothly across the board. One hole, and intruders can take advantage and make one regret not investing in it.

Conducting what is called a posture assessment is another great idea to assess the level of security a company has. A posture assessment is “a thorough examination of each aspect of the network to determine how it might be compromised” (Dean, 2013, p.495). This could mean hiring an independent party to try and hack the network to test and asses the vulnerability of the network at each level. When an accredited third party does the assessment, it is known as a security audit. This should be done on a regular basis as threats are growing increasingly sophisticated as the days go by. Keeping everything up do date and secure will prevent any unauthorized attempts from happening.

There are two common types of security risks hackers can take advantage of: people and hardware. “By some estimates, human errors, ignorance, and omissions cause more than half of all security breaches sustained by networks” (Dean, 2013, p.496). That is why it is very important that all personnel are educated about the proper procedures and what to look out for. Someone claiming to be an authority will probably never ask for your login credentials. These credentials should never be given out except to authorized parties within the company. Acquiring credentials to a well-protected network is known as social engineering because the attacker gets creative when trying to obtain such information. The hacker is counting on employees and users to be ignorant. Educating everyone about these kinds of threats makes them aware and prevents passwords from getting into the wrong hands.

Hardware is the second thing that is very vulnerable. Physical access must be heavily protected and secured. This involves the Physical, Data Link, and Network layers of the OSI model. NIC cards, routers, and switches all are included in these layers. An example would be an intruder listening in on transmissions through a switch on something called a protocol analyzer. This method is very sophisticated and requires certain expert level in skill. Transmissions can also be intercepted and redirect sensitive information to another location unknown to anybody but the hacker (Dean, 2013, p.498). masking internal subnets can also be a good practice. Otherwise, intruders can read private addresses. Passwords for switches routers and other hardware should not be easily guessed and probably should be long and complicated to make it more secure and harder to hack. Storing the information in a safe place is also critical. It might be best to write it down or print it out instead of store it electronically. Another risk is to have open ports. Having them open just gives an intruder an invitation in (Dean, 2013, p.498). Educating the proper staff on these procedures and rules is critical so the entire company can be on the same page.

Security is a very expensive thing to have, but in the long run, it saves the company a lot of time and money. Education and regular practice can prevent mistakes from happening and can help improve the overall security of company data.

When disaster strikes or there is a major security breach, it is always a good idea to have a backup plan. Backing up company data at multiple locations is not only safe, but the quickest way to restore valuable data or downtime. Regular backups to the database should be done regularly. Aside from the actual backups themselves, it is important to create an actual plan of what to do so everyone does not freak out and do further damage. The IT staff needs to study and practice the plan to make sure they are prepared for when tragedy or security breach does happen.

The first thing a company needs to do involving disaster recovery is assembling a disaster recovery team. These must include key points of contact that each may be assigned certain roles to help get the network back up and running. The team should not only have members of the IT department, but all departments up through the highest management personnel (Dean, 2013, p.674).

Documenting everything about the network is also necessary so the team knows where everything is supposed to go and how things are configured when working properly. This includes inventory of all hardware such as desktops, printers, routers, switches, servers, etc. This information is good to have because then things can be easily spotted that need to be fixed is damaged (Department of Homeland Security). Of course, if these devices contain passwords, be sure only authorized IT staff have access to them and not Tom representing the sales team. Tom may not have the router password, but he might have the password to access any software that department uses. Working together as a team is critical in disaster situations because if things are miscommunicated, things can go awry very fast.

Three different types of backup methods exist when backing up data. The first is backing up data to optical media such as a USB drive or DVD. Blu-ray DVDs cans store up to 128 GB of data, making them much more useful than just watching movies (Dean, 2013, p.670). Make sure the device is recordable, so data can be placed onto it. This may work for small company data, but for larger companies, one might need another form of backup.

For larger organizations, tape backups may be appropriate. This involves backing the data up to magnetic tape that uses a tape drive that is connected to the network. Large environments may have what is called a storage library in a warehouse somewhere, where a physical copy can be retrieved (Dean, 2013, p. 671). This method is easy to implement, but is often very slow compared to other methods.

Most networks these days use network backups which means they back all their data up onto another network (Dean, 2013, p.672). This is done online through cloud storage. This is probably the quickest and safest way of backing things up because if all the hardware is gone from one location, it can easily be backed up and recovered from anywhere. This is the backup implementation that is best to use for our company because we have locations all over the world. Having the same backups as other parts of the world is critical as then the data is the most up to date no matter where employees may travel.

The next decision in the plan is to decide how much of the data needs to be backed up. An archive bit is a tool that helps determine just that. The bit is turned on when a file is created, telling the system the file needs to be archived. There are three types of backups that can be done: full backup, incremental backup, or differential backup. Full backups backup all data regardless of changes. They then switch the archive bit to off after it is done. In incremental backup, it only backs up the changed files since the last incremental or full backup meaning those files that still have the archive bit checked. This makes it quicker to backup so a full backup is not needed, taking less valuable time. Differential backups are similar except they do not uncheck the archive bits after the backup is complete (Dean, 2013, p.672). Each backup will be different for each situation. However, developing backup rotation scheme can be useful, so all types of data can get backed up on a regular basis, leaving backups to practically run themselves at the time of recovery.

References

Collins, T (n d). *11 Huge Business Benefits of Fiber Internet Connectivity.* Retrieved from atlantech.net:https://www.net/blog//11-huge-business-benefits-of-fiber-internet-connectivity

Gordon, W. (2013, April 10). *Ask LH: What’s the difference Between Cat5e And Cat6 Ethernet Cables?* Retrieved from lifehacker.com: [https://www.lifehacker.com.au/2013/04/ask-lh-whats-the-difference-between-cat5-cat5e-and cat6-cables/](https://www.lifehacker.com.au/2013/04/ask-lh-whats-the-difference-between-cat5-cat5e-and%20cat6-cables/)

Designing for Availability – Microsoft

[http://www.1202performance.com/atricles/how-to-write-performance-requirements-with- example/](http://www.1202performance.com/atricles/how-to-write-performance-requirements-with-%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20example/)

<http://www.weibull.com/hotwire/issue26/relbasics26.htm>

<https://msdn.microsoft.com/en-us/library/aa291866(v=vs.71).aspx>

Johnson, J, 2007. MLPS Explained. *Network World.* Retrieved from <http://www.networkworld.com/article/2297171/network-security/network-security-mpls-explained.html>

Kirvan, P ,2017. Ethernet advantages. *Tech Target.* Retrieved from <http://searchenterprisewan.techtarget.com/tip/Ethernet-advantages-and-disadvantages-for-WAN-connectivity>

Performance By Design

Reliability Hotwire

*Retrieved 4/19/2017*

*Retrieved 4/19/2017*

*Retrieved 4/20/2017*

Types of Backbone Networks. (2014, November 04). Retrieved April 25, 2017, from http://fiberbit.com.tw/types-of-backbone-networks/

# Works Cited

Dean. (2013). *Network+ Guide to Networks, 6th Edition*.

[Bookshelf Online]. Retrieved from https://online.vitalsource.com/#/books/9781133608196/

Parker, D. (2006, August 16). *Network design and defense.* Retrieved from TechGenix: http://techgenix.com/Network-design-defense/

Vanlan, J. (2016, October 12). *Here's how much businesses worldwide will spend on cybersecurity by 2020.* Retrieved from Fortune: http://fortune.com/2016/10/12/cybersecurity-global-spending/

Zadelhoff, M. v. (2016, Septmebr 19). *The biggest cyber security threats are inside your company.* Retrieved from Harvard Business Review: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company