Fundamentals of Information Technology

Jeffery Morse

Brandman University

Author Note

For correspondence concerning this paper, Jeffery Morse can be reached at

jmorse@mail.brandman.edu

Abstract

 This paper covers the Information Technology Plan for Biggie’s Logistics. It is a very inclusive plan that includes the establishment of LAN, WAN, WLAN, Cell Connectivity, Security, Topology, Cryptography, Security Layers, Network Hierarchy, Email, iCloud, Form factors, WordPress, Linux, Ubuntu, SQL Servers, VoIP, Video Conferencing, Category 5 and 6, and the security measures taken to meet the government requirements of its contracts. It also includes basic ideas to help one relate networking, networking topology and the internet in general.

Keywords: WAN, WLAN, Cell Connectivity, Security, Topology, Cryptography, Security Layers, Network Hierarchy, Email, iCloud, Form factors, WordPress, Linux, Ubuntu, SQL Servers, VoIP, Video Conferencing, Biggies Logistics.

Fundamentals of Information Technology

 The purpose of this paper is to present an Information Technology Plan for Biggie Logistics. This Strategic Plan will define initiatives and objectives that align with the business goals of Biggie Logistic to update the company from its old hard copy technology to current digital copy technology. To improve the balance between demand for technology and available for its staff, customers, and executive. Further, systems will be designed with annual financial tasks in mind while making systems available for managerial accounting, reports and processes. This Strategic Plan provides a type of roadmap that will serve as the instruction manual for Biggie Logistics to close the gap between its current strategic plan and the coming updated strategic plan. Also address, are the Information Technology needs required to address immediate and long-term future technological issues that may arise from advancements in networking equipment.

 While it is never an easy task to establish a digital presence, or change from hardcopy technologies to digital technologies, it is the felt that these changes are needed and designed to ensure scalability and growth well into the coming eras. This is the information age. Today the Internet plays a big role in productivity and success in business. We will begin our plan with a look at the Internet. What is the internet and how is it to be used to increase profitability? Looking ahead this Strategic Plan will also cover the type of network infrastructure, network topology, wireless solution, government contractors “confidentiality” needs, as well as security needs, risk management and finally the final recommendations.

 The departments that will be included in this Technology Plan are summarized here. Budgeting and accounting, payroll and purchasing, human resources, sales, automation of timecards, vehicle logistics tracking and route inquiry, employee communications, inventory storage and logistics information, cell phone and other personal business appliance use and connectivity. The commitment of all departments is essential for the success of this IT Plan for all employees to realize the associated benefits. All departments must work together to balance daily departmental operations while embracing companywide changes resulting from the coming initiatives in technology.

**Networks and Networking**

 Networking in the business world means something else than it does in the IT world. However, the term still relates in principle. In the business work “working a room” is referred to as networking. It is the idea that one connects to possible sources or customers in an effort to establish a memorable presence that results in future benefit. Imagine a man named Topol enters a room with networking in mind. The approach he takes will determine his time and success. Topol can approach this in several ways. He may circle the room going from one person to the next, or he could choose to walk the hallway stopping in each of the separate rooms. Alternatively, Topol may choose to stand at the door and make introductions as people stroll past, or he may choose to stand at a central location and choose who to connect with returning to his hub at the end of each networking effort. All these represent different styles of Networking Topology. In this section, we will be looking at Networks and Network Topology. What is a network/networking? Further, we will be investigating infrastructure; choosing our internet and intranet communications design.

 Wired networks come in some basic categories. There is the Local Area Network (LAN), and the Wide Area Network (WAN). All LAN’s have three components: network adapter cards (NICs), network operating software, and cabling (Baum, 1998). Let us use Topol again to help us explain. If the scope of Topol’s networking included all employed by one specific company we may relate this to a Local Network (LAN). On the other hand, if Topol scope in networking were state or government-wide we might refer to this as a Wide Network (WAN). Coincidentally, if Topol had a worldwide scope we might call this a World Wide Web (WWW). Understanding the difference is not only imported in design but also security. For now, the LAN will be the focus. A LAN can also fall into two basic Groups: peer-to-peer, or client-server. Peer-to-peer is basically like when Topol circle the room going from one person to the next. While this used to be standard for Daisy –Chain and Ring style networks, this is limited by bandwidth. These are antiquated and are no longer used. The second type is the Server-Client subgroup. In this group, there are servers that perform specific processes and client workstation for each user. Secondly, the Server-Client configuration includes bus, mesh, and star. In years past the bus configuration was the one that the major corporations relied most heavily on. In this configuration, there would be one Main-Frame Server that connected to a bus or single heavy wire. All workstations would connect individually to this wire. One might imagine the problems when all the clients were connected at once. Topol standing at the door might get briefly connected to every person walking through, however, regulation all that info is almost impossible. Mesh is just as it sounds. Imagine everyone at the party trying to connect with every other person at once—what a “Mesh”! Today with the advent of twisted pair cabling-- A cable consisting of two wires twisted around each other, used especially for telephone or computer applications, and with the invention of the network router-- A device which forwards data packets to the appropriate parts of a computer network (Oxford, 2017) we have graduated to much more efficient types of networking solutions (Zhlfeng, 2012)(Haddadi, 2008).

 In addressing the needs of Biggie Logistic our network will need to be scalable(updateable), inclusive(be broad in aspect), and secure. This is the information age. Our network will be inclusive by handling communications both in the intranet (LAN) as well as on the internet (WAN). Inclusivity will also include databases, video capabilities, voice capabilities, email, web pages, and web portals. By including web based and cloud based applications, we will be positioning Biggie for the scalability for the future while ensuring inclusivity. In addition server selection will be partially made according to scalability. Just how we accomplish this will be covered in the pages that follow. All this will have to be available both for LAN, as well in a wireless local area (WLAN). For these reasons, we will be incorporating a hybrid topology. The server-client/star topology with backups for both data and power. “The main advantage of Client-Server networking is its ability to change rapidly as computing needs vary (Baum, 1998).” Simply put, as the industry advances Biggie's network work be left in the dark ages. As a result, we in the Star topology hybrid we will be using category 6 cabling, Ethernet Cards capable of 1000baseT or Gigabit as it is called, and finally the networking protocol will start with 802.x protocols. These are currently industry standard and will help to supply our needed security (Pfaffenberger, 2001). Further, we will be utilizing a system of security called demilitarized. In short, the network will be employing several firewalls of different types to help ensure the standard of security called in contractual obligations. Finally, it is also important to diversify static IP address (Chowdhury, P. K et al, 2007). An IP address is a set of numbers that actually identifies the address of a client or server on any network. We type in or request “google.com” but in actuality, this request goes to a Domain Name Service Provider (DNS) or (NS) who intern relates the name to an assigned address. Just as the White House has 1600 Pennsylvania Ave NW, Washington, DC 20500 as its address, a user or workstation on a network does. This address is in subgroups assigned to each Subnet -- Xxx.xxx.xxx.xxx (referred to as IPv4). Just like the White house address each part represents a narrower scale. For instance, Washington DC –tells which state and city, the zip 20500 which area of the city, Pennsylvania Ave—which street, and 1600 the specific house. Likewise, each number has specific meaning in the address, 192.168.3.1, for instance, says 192 – home private network; 168 – the subnet of that network; 3 – the assigned area by the router; the specific item under that router or switch. By having this many numbers it was thought that we would never run out, but alas, we did. IPv4 had to be expanded to IPv6, which basically is expanded to a set of addresses that is almost inexhaustible. On the downside, IPv6 is still not fully interpreted so, as a result, we will be sticking with IPv4 addressing scheme.

**The Internet**

 When speaking of connectivity to the internet we have a few choices as well. Connectivity choices include T1-T4 direct connections. Fiber Optics by SureWest, Comcast Cable, ATT DSL, and Succeed net Dialup – Microwave, and finally HughsNet Satellite. Such companies are referred to as ISP or Internet Service Providers. We will not be using Satellite as it has stability issues. Microwave is expensive but is an alternative. Dial-up is too slow for today’s high Mbps connections, DSL though close, still has some issues due to wire gauge. T1-T4 are what most colleges use, however, they are very expensive. This leaves fiber-optics and Comcast Cable. The cable model is the standard choice, however, if SureWest another company has an optical internet connection in the same price range it would be the best choice. Optical offers 100 Mbps upload and download speed compared to 10-60 with a standard cable modem. The price of service here will be the deciding factor. For now, we will say the standard cable modem from Comcast. We will need static IP assignment, which is customary for businesses. Also to our benefit, they come in packages of five. For security purposes, it is important to diversity these connections (Chowdhury, P. K. et al, 2007). These numbers are External IP addresses (WAN) assigned by Comcast. They will be assigned as follows:

* IP 1, port 80 and 437 for Internet web connections – Web Server, Bastion Server, Intruder Protection.
* IP 2 Logistic Web Based Data Interface – Data Base Web Portal, Network Wireless Connectivity for Logistics buildings, handheld inventory.
* IP 3 – Routed nonpublic --VPN to Cloud, and Backup Servers.
* IP4 Cell Phones and other Wi-Fi connectivity – Wife Interface for all employees.
* IP 5 VoIP Gateway, phone, and video conferencing technologies.

All five of these address come through one router supplied by the service provider. Understanding the network installation and topology is crucial. Here is a diagram.

 The Modem/Router/VoIP/Firewall is in one unit. All 5 Static IP connection come through the cable/optical cable connection. Connection 001 is the Web Connection. The after the Comcast firewall and router the cabling connects to the first external hardware firewall; to the Web Service Router; and then to two Linux Severs each running VMware. Here we must begin to think of a Server not as hardware but as software. Software servers can be run in a virtual environment. VMware is an operating system like Windows, MacOSX, or UNIX which support the installing of Virtual Machines. Instead of one machine running one software, we install three separate server operating systems on one machine. They all act as though they are their own entity although they are actually running virtually on only one machine. Three separate servers in one box. This virtual ability is only limited by memory capacity and CPU speed. There are two machines each running three servers. Server one is intruder detection. Under Linux software to identify attempted attacks and non-privileged user penetration. Basically, this monitors all activity and then upon suspicious activity it send a warning to the administrator, and kicks or locks out the suspected offender. This server also acts as a Proxy server to filter URL addresses. Second is a bastion server. This is basically a dummy server design to fool anyone who gets through the two firewalls and the intrusion protection. Finally, the third server is the actual web server contain the WordPress Web-Site for the company. All three servers are running on the Linux platform, with software Unix Fire Wall (ufw), and iptable firewalls active. For this section, we have four different firewalls: One Comcast, One External Hardware, and Two software per server. In addition, we have the intruder detection as well as the dummy server. All this combined is called out militarized zone as it is heavily controlled.

 A word about WordPress. In this technology plan, we have chosen to host our own webpages. This saves Biggie money. Since the servers are needed and already there it only makes sense to not spend more money on outsourcing. WordPress is the most dynamic and editable platform, and it is free. PHP based it remains on the cutting edge, this also allows a dynamic viewing of any device (Borhani, 2014). This means we will get a Domain Name from a Domain Name Registrar like Godaddy, or Google. The Domain name BiggiesLogistics.com will be registered with them. As a result, the Domain Name Servers (DNS) on the internet will route all request for that domain name to our static IP 001. When the Uniform Resource Locator (URL) of Https://www.biggieslogistics.com is typed into a browser that request is routed to IP 001 to our Web Sever. As a result, our WordPress external site is brought up.

 IP 002 is for Logistic Wi-Fi and database access. This portal will be turned off with the DNS provider and not accessible from the internet without a VPN in place. Virtual Private Networking is a tunneling protocol that directly links two networks. While not activated at set up this could be established easily later. If Biggie scaled up in the future by purchasing another location activating this service would link the networks of the two locations as one network. This is a great solution because we sidestep any internet connectivity thus keeping the network security intact. To add to this, if it is desired that there be a web-based portal available for employees to use this too can be made available through this easily (Odiyo, 2011). By using a separate IP than the web page servers it is less likely to be attacked. For now, this IP is assigned for LAN access to the Data Base tier. The data server we chose is SQL. This is really the industry standard and easily runs our 802.x protocols. Further, money can be saved by using the free version called MySQL without any security issues. SQL and MySQL both run fine under Linux. We choose Linux over Microsoft due to the extensive charges employed by the company. When using Microsoft Server one must pay a per-user fee -- and they are not cheap. Also in an attempt to avoid virus’s and malware system wide the choice is made to steer away from C+ compiled Operating systems as they are compromised at a much higher percent compared to other operating systems. The SQL server is behind the last demilitarized zone. A demilitarized zone is a zone on the network after two firewalls (Nakamoto, 2011). In this configuration, we have one we have two. The first stop we covered militarized zone. Next, after the second hardware firewall, we have our LAN connections, and then after a Third hardware firewall the heart of our business the database server. This database server can connect to the LAN by way of the Ethernet or to our handheld devices in the warehouses through a wireless router coming off of the last router. For added security, in addition, is a local SQL backup up server. The security measures hear will be addressed later.

 IP 003 is nothing but a backup channel. Used only in VPN. This is for cloud backup and synchronization. Backup of the website, database, and business critical files. Also, dropbox connections for all employees who require them with secure drop box technologies by apple -- i.e. iCloud. This goes to three separated places. First a clone of the web page. The Names Service provider will have alternative addresses listed in case of failure or earthquake. The three resolving locations are the in-house primary server, the in-house backup server, cloud-based clone. The second place is the apple iCloud server with account access. Finally, a Cloud database backup for the SQL databases. Protocols for security are discussed later.

 IP 004 is for the Wi-Fi router that comes directly off of the first router from the militarized zone. This keeps all cell phones off the main LAN thus reducing attacks and the chance of infiltration from malware. Since it is a leg off of the militarized zone the Proxy Server/ Intruder Server will be configured to actively monitor this IP as well. All personal mobile devices belonging to employees can only connect through this gateway.

 IP 005 is reserved for Voice over IP (VoIP). This is the company’s new phone and video conferencing channel. VoIP is highly secure and allows for a broad range of connectivity alternatives.

 Finally, to address communications a bit more we need to address our workstations. The workstations are all Apple based. Mostly Mac Mini’s are sufficient. The MacOSX platform is the least hacked and is almost virus free. Due to the nature of “Scripting” (the language that it is compiled in), it is very hard to successfully infect with malware. To add to this, MacOSX is a brother to Linux and UNIX. This communication with all the service will be less likely to fail. Another plus is each computer can have its own iCloud account with Apple. Apple iCloud can be configured with 2 tier access qualification making it almost impervious to social hacking. This will allow employees drop boxes and centralized email.

 Email and office communication is a topic that needs to be addressed. This technology plan calls for a three-tiered system. For external emailing and communications since Biggies is hosting its own web page and purchasing BiggiesLogistics.com we now have access to email addresses in the nature of User@BiggiesLogistics.com. This service will be a paid service provided by the Name Service Provider. Since mail servers are the main source of temptations to hackers Biggies will not have a mail server in this configuration for external networks. Each employee will be set up with a forwarding from the Names Service provider to their mail iCloud account. Automatically User@BiggiesLogistics.com forward to User@iCloud.net. Internally, WordPress provides a Mailbox, chat box, and video conferencing for each employee. Also provided are employee scheduling, timecards, and just about everything else one can think of. However, it is recommended to use the VoIP for video conferencing as it is much more secure. To tie it all up in a nice bow we add the Mail App in iHome, which is standard in OsX. The Mac Mail app can be configured to automatically retrieve emails from all the account one has to one area, as well as make them available at user@iCloud.net. It should be noted that iHome is free with the purchase of the MacMini’s and iCloud accounts come free with the setup. For bigger files too large to email Biggie can create a File Transfer Protocol (FTP) area on the web server. By encryption, this area can be made public or private.

**Wireless**

 The wireless solution recommended is separated into two basic tiers. Both are Wi-Fi-based utilizing 802.x protocols. The problem is that the warehouses need to have connectivity to the database as well as to the network. The SQL data is considered high security. This added with the needed Wi-Fi for personal mobile appliances dictates the need for a two-tiered approach. Discussion has been presented about both areas, however, here more information is provided. There is an alternative to this configuration using today’s cell phone technology. While using cell phone technology is attractive it is felt that the costs associated with mainstreaming data are a costly expense that may be discarded. However, cell phone plans are included as part of the overall technology package, they are not for main data activities unless there are no other options. While cell phone technology and service topology are beyond the scope of this paper, it is noted that today’s cell phones are pretty secure. Wi-Fi service for the personal mobile appliance (PMA) is provided through the Comcast/router/firewall switch. This is on a separate IP address and has no gateway to the business LAN. If access is desired later a web-center with a web port may be established. In this way, connectivity is maintained while company security is fully addressed. To add to this all PMA Wi-Fi is set with a security no less that **WPAWPA2-PSK (TKIP/AES) which is a high breed of the old obsolete standard and the new.** While this is not impenetrable, even if hacked the attacker only gains access to the internet, not the LAN. Due to a variety of reasons, stronger security has not been implemented yet in all wireless infrastructure (Varshney, et al 2004). Protocols for Wi-Fi include Open (none), Wired Equivalent Privacy(WEP) 64 or 128 which is proven obsolete, wireless protected access (WPA) was the standard until nullified by hacking, **WPA2-PSK (TKIP) which the new standard with the old encryption and finally WPA2-PSK (AES) which is the new standard with the new encryption.**  The limitation of Wi-Fi first and foremost is distance. Other limitations might include noise, bandwidth, and electronic failure, or obsolete encryption unable to connect to the new standard. On the upside, since PMA access is not needed in anyplace other than the main building only the installation on one repeater is required. The base Wi-Fi router on one floor and the repeater on the other.

 The second Wi-Fi connection is for the PMA related to business logistics and inventory. Barcode scanners, palm pilots, and other mobile company equipment that must have access to the database and LAN will be serviced off of a separated wireless router attached to the final switch in the database tier of the network. This is a closed wireless network. Only specific mobile devices with unique static IP addresses and unique Mac address listed in the router will be recognized. By employing device profiles

Intelligent routing device configuration can communicate accordingly. Problem areas such as viewing area, browser capabilities, input methods, and storage capabilities can also be addressed (Varshney, et al 2004). Confidentiality, authorization, non-repudiation authentication, integrity, and accessibility, convenience, speed, ease-of-use, and standardization are all issues when considering wireless technologies. Security is paramount so by employing WPA2-PSK(AES) security protocols we address these issues. Further, by controlling connections we keep bandwidth at maximum. WPA2 is a wireless transport security layer (WTLS). The translation between secure socket layers (SSL) is far more secure than any other available protocols. There will be a section on security later. For now understand that the topology is still a Star / Client-server highbred using 8.011e with non-reporting and controlled access (Chandra, 2005).

**Security and Confidentiality**

 U.S. government contracts require campuses to have confidential data security throughout the campus and to implement countermeasures to help prevent any information loss. First, it might be beneficial to review the areas of concern. Confidentiality is a non-occurrence of the unauthorized discloser of information. In other words, no one except the sender and the receiver should have access to the exchange of information. Integrity is the non-occurrence of the manipulation of information by unauthorized personnel. Plainly put, no one except the sender and the receiver should be able to modify the information. Authentication is the ability to ascertain the origin of a request. Hackers should not be able to masquerade or ghost. Non-repudiation is the ability to prove that a sender is the real source of a given message. The sender should not be able to deny sending the message. Finally, service reliability is the ability to protect the communication session against DoS. A Denial of Service attack is when a hacker sends more requests for access then the server can handle. This results in a crash in the system as the system power is taken up by denying the requests.

 Security is sub-grouped by layers. Layer one is encryption. XTS is an [XEX-based mode encryption with ciphertext stealing. It is](https://en.wikipedia.org/wiki/Disk_encryption_theory#XTS) a block cipher used in full disk encryption and is already very widely supported. This is the encryption that Linux (Ubuntu) uses when selected. Layer two is the encryption when sending communications to the network. EAP-TLS. EAP or Extensible Authentication Protocol keeps authentication in check but when combined with Transport Layer Security it is still considered one of the most secure. In fact, this is not only the protocol for the Wi-Fi but also can be chosen for the entire network. To add, EAP-TTLS – the extra “T” is for “Tunneling” is what is used for the VPN technology that is available in this system. Layer Three security is speaking to the servers. Transport Layer Security (**TLS**) and its predecessor, Secure Sockets Layer (**SSL**) are the security measures we will be using. While local connection might be made in TSL all external connection are referred to SSL. SSL uses cryptography when sending data. When handshakes are made from server to client and back certificates are transferred.  Only trusted third-party certificate authorities are used to establish the authenticity. Once the authentic is accepted packets for cipher are sent and received. Data changed in any way is dropped thus security is upheld. Basically, this is the same security of any financial institution. However, there is a yearly fee involved. Layer four is the last layer of security when transmitting data. This is [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) and the [User Datagram Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP). These control flow of data uni-direction or bi-directional and allow the assignment of Ports (Chandra, 2005). Open ports are a big security problem, while many ports must be open most can be closed. In addition, this can combine this with port logging so there is a record of all access. Port 80, 443, 21 will be open. Others will be opened only as needed. It may sound like an impenetrable fortress, but there will be hackers who are successful in penetration these defenses.

 To summarize security. Linux employs all the layered security just mentioned. Add to this the countermeasure efforts of demilitarized firewall configurations, bastion server, Intruder detection server, and a proxy with URL trace routing, reporting, logging, and URL Filtering; the multiple software firewalls including ufw, and iptables, the diversified static IP configuration, the diversified Wi-Fi configuration – and monitored login authentication; the cloud-based 2 tiered authentication of the external email provided by apple with no mail server locally save only WordPress, The Wi-Fi for the LAN and dbase not on an open IP or port with the highest available encryption and authentication of WPA2-PSK(AES), the web server running in strict SSL-only mode I believe we have covered just about everything. The last thing in the way of security is to mention online GPS tracking for Logistics in-route. Since Biggie’s is choosing to use Apple Product’s the expense of data links for trucks is no longer needed. Apple phones will easily run apps tracking trucks in real-time. Further, inquiries can be made as to average speed, estimated arrival times, as well as teamster logbook entries.

**Computer Hardware, Software, and Databases**

 Workstations in Biggie are Apple – Macintosh. Mac-Minis form factors are comparable to the price of standard PC’s and are much more reliable and for the most part virus free. For those that need more power, there is the MacBook Pro that can be purchased. Software for each is the following: MacOSX latest version, OpenOffice Suite which includes all the software that MS Office does but for free of charge, Chrome Browser. MySQL will be the SQL dbase software. MySQL has established itself as the free go to dbase. MS-Access is on the way out. Other databases though good are not as well known. This makes HR risk management more difficult. Vfront is a form generating front end provider. After the forms are created for inputting and searching data, for the generation of reports Vfront will be rarely used. Lastly, SQL-leger is the main accounting software for the company. This software will run off the MacOSX platform and integrates easily with MySQL dbase. It is comparable to Quick books and the learning curve is not that big. The major plus is that any report it does not have can be either created through a form using Vfront, or straight from within MySQL itself. Primary database management functions can be handled by PHPMyAdmin through a web port.

 Four for the servers are Dell PowerEdge T430 Tower servers or comparable. Each server has dual quad processors, 2 TB storage, 16 gig ram and 2 Gigabit NICs. The fifth is a 10 TB backup server with one Gigabit nic, and one CPU. Two of the T430 are set with VMware and are clones of each other. Server configuration is for another time, however, the two T430’s are running multiple Linux servers as stated earlier. Each Linux load is a different server 1. Web Control Panel. 2. Web Server with FTP server, and Vfront. Vfront is a purchase but a necessity for dbase form creation for the SQL server. Creating forms for the dbase is a long and time-consuming process which will require several meeting to determine format and information. Vfront is HTML or PHP and is server based and will run off the web server inside the WordPress Local site. WordPress will be loaded with WordPress Multi-site as the external web page and the internal LAN are different front ends. . 3. Proxy Server. 4. Bastion Server. 5. Intruder Detection. The other two servers will be running MySQL one main and one backup. Finally, the backup server is loaded with timed backup software, which it comes with, for nightly backups.

 Hardware Firewalls. While there is a firewall in the Comcast modem the firewall for directly after the modem is the first line of defense for the demilitarized configuration and sits directly behind the modem on IP 001 which feeds the Web Server router. The Second hardware Firewall is after the Web servers between the LAN router and the Web Servers. It may be possible to combine the LAN router and the second hardware firewall. The third hardware firewall is between the LAN router and the SQL switch. Don’t forget each router may have another hardware firewall, and the Web Servers have an additional 2 software firewalls.

 Routing includes the Comcast router, each port assigned its own Static External IP. Additionally, the VoIP is routed from here as it the PMA Wi-Fi. A Web router for the web servers handling ports 80, 443, and 21. All external traffic requesting those ports will be routed to those servers. The LAN router handles all intranet traffic assignments will be 192.168.x.x. It will be possible to subnet or workgroup according to department. The SQL switch is extended off of the LAN router for SQL specific ports. The final router extends off of the SQL switch. This router assigns the Wi-Fi connections to the mobile appliances needed in the warehouses. Each warehouse will a Repeater or Wi-Fi amplifier as needed. This is a closed WPA2 authentication. Appliances must be set-up for connection.

 Emergency precautions include the following. 1. A battery backup for WEB and SQL servers. This will ensure servers don’t shut down in the event of small power fluctuations. 2. A backup generator will be used in the event of extended times of electric service failure. This ensures that in the event of an earthquake systems don’t fail. An offsite Web server also is available through a third party hosting to handle overflow or local failure. Finally, the VPN back-up is a continuous backup for SQL, and Web servers to an offsite backup hosting provider. Personal mail for employees is continuously backed up on apple iCloud along with pictures, bookmarks, and notes.

**Risk Management and Education**

 We have confronted and put in place several safeguards in the way of risk management. However, the first line of defense is always proper training and instruction. Classes on proper online behavior in the workplace is a must. Security of passwords and LAN access must be taught and monitored. I suggest ongoing classes as a requirement. Learning how to properly use equipment is a stress relieving venture. Classes on OpenOffice, for instance, can ease the transition. To add to this many may not even know how to use word processors and need help in basic keyboarding. This technology upgrade comes with the creation of staff positions. Network administrators for creating smooth and secure access both wired and wirelessly, PHP programmers, Linux gurus, web administrators to run the web pages and portals. SQL managers to manage or rebuild the database if it crashes. Though it may be possible to have one person wear several hats, too many hats on one person is the wrong approach. In the case of sickness or other problems being stranded without someone knowing the system is all bad. To add to this accounting and bookkeeping will need classes in SQL-ledger, Vfront, and MySQL. Technicians that know how to replace Cat 5 cable ends, as well as replace internal computer hardware is a must when things fail.

**Summary**

 This plan has presented a technological outline for the future. Everything from what a network is to the specifics of software has been discussed. It is felt that this is just the beginning of a transformation that is sure to bring its share of stressful nights. However, when all said and done this plan will not only propel Biggie’s Logistics into the present but aligns Biggie’s for future scaling and progress. Gone are the times of flying 3 hours to a conference in other cities. The video conferencing ability alone may pay for the upgrades in time. After the learning and adjusting time draws to a close this company will begin to enjoy ease in all aspects. By monitoring logistics in route the company may save money by avoiding logbook time and weight errors. Accounting that once took three or four people now only takes two. With readily financial and managerial reporting at the click of a mouse costs will go down, government contracts are fulfilled and there is only room to grow.

References

Baum, Frederic S. (1998) *The Basics of Local Area Networks* The American Bar Association http://www.jstor.org/stable/23774121 Accessed: 12-04-2017 18:13 UTC

Borhani, A. H., Leitner P., Lee, B., Li X., Hung T., (2014) "*WPress: An Application-Driven Performance Benchmark for Cloud-Based Virtual Machines*", Proceedings of the 18th IEEE International Enterprise Distributed Object Computing Conference (EDOC), pp. 101-109, 2014.

Chandra, P. (2005). *Bulletproof Wireless Security : GSM, UMTS, 802.11, and Ad Hoc Security*. Amsterdam: Newnes. <http://search.ebscohost.com/login.aspx?direct=true&AuthType>= ip,uid&db=nlebk&AN=130240&site=edslive

Chowdhury, P. K., Reaz, A. S., Atiquzzaman, M. and Ivancic, W., "Performance Analysis of SINEMO: Seamless IP-Diversity Based Network Mobility," 2007 IEEE International Conference on Communications, Glasgow, 2007, pp. 6032-6037. doi: 10.1109/ICC.2007.999

Haddadi, H., Rio, M., Iannaccone, G., Moore A. and Mortier, R.,(2008) "*Network topologies: inference, modeling, and generation*," in IEEE Communications Surveys & vol. 10, no. 2, 15, July 2008. doi: 10.1109/COMST.2008.4564479 **Online ISSN:** 1553-877X

Nakamoto, G., Schwefler, J. and Palmer, K., (2011) "Desktop Demilitarized Zone," MILCOM 2011 Military Communications Conference, Baltimore, MD, 2011, pp. 1487-1492. doi: 10.1109/MILCOM.2011.6127516

Odiyo, Benjamin., Dwarkanath, Mukunda (2011) *Virtual Private Network* beod2131, mudw2335}@student.uu.se Nov 2011

Oxford Dictionary 2017

Pfaffenberger, B. (2001). *Linux Networking Clearly Explained*. San Diego: Morgan Kaufmann.

Varshney, U., Malloy, A., Ahluwalia, P. and Jain, R. (2004) *‘Wireless in the enterprise:*

 *requirements, solutions and research directions*’, Int. J. Mobile Communications, Vol. 2, No. 4, pp.354–367.

Zhlfeng Tao, Arhngton, lVlA (US),DI Wang, Troy, NY(U$), Jlnyun Zhang’ (2012) *RANKING NODEs IN NETWORKS WITH TOPOLOGIES ARRANGED As DIRECTED,* United States Patent (10) Patent N0.: US 8,270,313 B2 Tao et al. (45) Date of Patent: Sep. 18, 2012