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 all networking topologies and designs that might be used in an upgrade from hardcopy paper business management to digital cloud based or network based business management for Biggie's Logistics. Security measures are defined to meet the government requirements of Biggie's Logistic government contracts. Also included are basic ideas to help one relate to 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 is a Strategic Plan that 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 Technology 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 addressed is the information needed in order to report on 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. The Internet plays a big role in the productivity and success of a business. This plan will begin with a look at Networking and the Internet. What is a Network? What is the internet and how is it to be used to increase profitability? This Technology Plan will also cover types of network infrastructure, network topologies, wireless solutions, government contractor "confidentiality" needs, as well as security needs, risk management, and final recommendations. Information Technology or "IT" is defiantly the business world of today.

First steps will include meetings to address any questions involving this plan. Adjustments will be made to this plan accordingly. Secondly, training will begin on various

topics of concern to ensure employee competency on the new hardware, software, as well as any security measures that may need to be addressed. Thirdly, compiling a hardware software list and the purchase of those items on the list will be tasked to admins and purchase agents. Next Comcast accounts and Domain Names will be purchased and setup. Lastly, the network install, setup, configuration, software installation, and employee accounts will be addressed.

The departments that will be included in this 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, the cell phone and other personal business appliance use and connectivity. The commitment of all departments is essential for the success of this plan. All employees will realize the associated benefits of Information Technology. Biggie's departments must work together to balance daily departmental operations while embracing companywide changes resulting from the coming initiatives in technology.

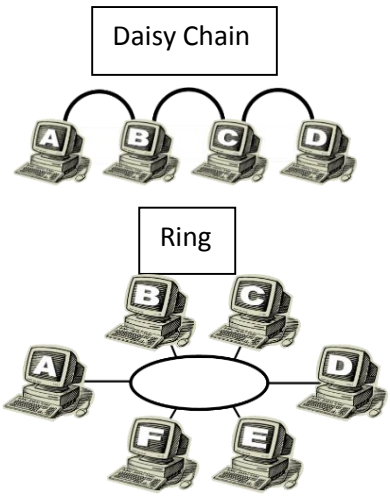
Networks and Networking

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 world "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 might walk the hallway stopping in each of the separate rooms. Alternatively, Topol may stand at the door and make introductions as people stroll past, or he may stand at a central location and choose who to connect with returning

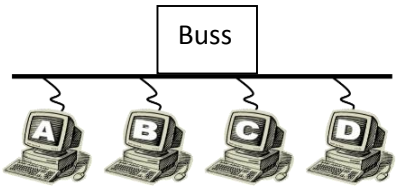
to the center of the room, his hub, at the end of each networking effort. All these represent different styles of Networking Topology. In this section Networks and Network Topology will be looked at. Explaining what a network is--in basic terms--in order to understand them and relate to the world's biggest network—the Internet. Further, we will be investigating infrastructure; choosing our internet and intranet communications design.

Topol will be a great example in an effort to bring clarity to understanding networks. When speaking of networks, wired networks come in two 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). Topol's scope in networking a room may include all employed by one specific company. This relates to a Local Area Network or (LAN). On the other hand, if the scope of Topol's networking included an entire state or government one may refer to this as a Wide Area Network or (WAN). Coincidentally, if Topol had a worldwide scope one might call this a world-wide-web of networks or (WWW).

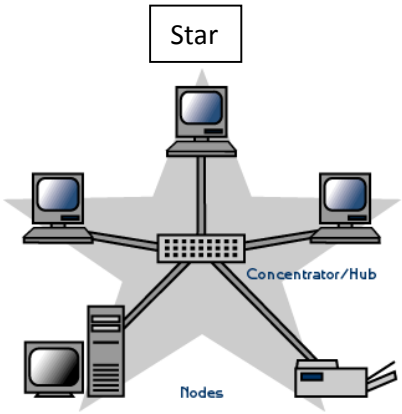


Understanding the difference is not only important in design but also in security. For now, the LAN will be the focus. A LAN also falls into two basic Groups: peer-to-peer, or client-server. Peer-to-peer is similar to Topol circling the room going from one person to the next. While this used to be the standard topography for Daisy–Chain and Ring style networks, today these have far too many limitations. Like a freeway, information travels on bandwidth. Older topologies just run out of room on the freeway. As a result, these antiquated network topologies are no longer used (Zhlfeng, 2012; Haddadi, 2008). The second basic group

is the Server-Client group. In this subgroup, there are servers that perform specific processes and client workstation for each user. The similarity is everyone coming to Topol instead of him going to them for an exchange of information. Secondly, the Server-Client model includes Bus, Mesh, and Star. In years past the "Bus" configuration was the one that the major corporations relied most heavily. In this configuration one Main-Frame Server is connected to a bus--or single heavy wire. All workstations would connect individually (Zhlfeng, 2012; Haddadi, 2008).



One might imagine the problems when all clients are connected at once. Topol, standing at the door, might briefly connect to every person walking through, however, regulating all that information at just the one point is near impossible. Mesh is just as it sounds. Imagine everyone at the party trying to connect with every other person at once—what a "Mesh"! The Star topology is most prevalent today. Biggie's will be incorporating a hybrid version of this. Star topology is made possible by the advent of twisted pair cabling--a cable consisting of two wires twisted around each other, used especially for telephone or computer applications, and by the invention of the network router--a device which forwards information (data packets) to the appropriate destination on the network (Oxford, 2017; Zhlfeng, 2012; Haddadi, 2008). Because of this, today's networks have graduated to much more efficient types of solutions.



In addressing the needs of Biggie's Logistic network scalability (staying compatible), inclusivity (being broad in aspect), and security are all included. Scalability ensures that as new products and technologies come upon the scene Biggie's networks will remain compatible. This is the information age. The network inclusivity is shown by handling communications both on the intranet (LAN) as well as on the internet (WAN). Inclusivity demand means inclusions of databases, video capabilities, voice capabilities, email, web pages, and web-portals. By including web-based and cloud-based applications, we will be positioning Biggies for scalability in the future while ensuring inclusivity. In addition, server selection will be partially made according to the needs of scalability. Just how this is accomplished will be covered in the pages that follow. In addition, all this will be available both for LAN as well as the wireless local area (WLAN). For this reason, 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, p16). Simply put, as the industry advances Biggie's networks will not be left in the dark ages. In fulfilling this the Star topology hybrid will be using category 6 cabling. This also saves Biggie's money as this cabling is already installed. Further selections include Ethernet Cards capable of 1000baseT or Gigabit as it is called, and finally networking protocol of choice will be of 802.x variety–explained later. These are currently industry standards and will help to supply the needed scalability as well as added security (Pfaffenberger, 2001).

For defense against attack utilization of a system of security called "demilitarized" zone configuration, also explained later, will be installed. In short, the network will be employing several firewalls of different types to help ensure the standard of security called for in contractual obligations of defense. IP diversification is a great security measure (Chowdhury, Reaz,

Atiquzzaman, and Ivancic, 2007) and is important. By separating connection out through several different addresses access by hackers is limited.

Understanding IP Addressing

An IP address (Internet Protocol Address) is a set of numbers that actually identifies the address of a client or server on any network (Chowdhury, P. K et al, 2007). When one types in or requests "google.com" the request goes to a Domain Name Service Provider (DNS) or (NS) who in turn relates the name to an assigned IP address. Just as the White House has 1600 Pennsylvania Ave NW, Washington, DC 20500 as its address, a user or workstation on a network has an address. This address is in subgroups; each subgroup is a Subnet address -- Xxx.xxx.xxx.xxx referred to as IPv4 (Internet Protocol Version 4). Subnetting allows the creation of multiple logical networks that exist within a single network. Without subnetting, one could only use one network per Class (Cisco, 2006). However, because of sub-netting, one can use each sub-group, and just like the White house address, each group will narrow in 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 a 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; 1 the specific item under that router or switch. By having many numbers it was thought that addresses would never run out, but alas, they did. IPv4 had to be expanded to IPv6, which basically increases the set of available addresses to an almost inexhaustible amount. On the downside, IPv6 is still not fully integrated so, as a result, Biggie's will be sticking with the IPv4 addressing scheme (Cisco, 2006; Perkins, 2010). Diversification means that Biggie's will own more than one IP address.

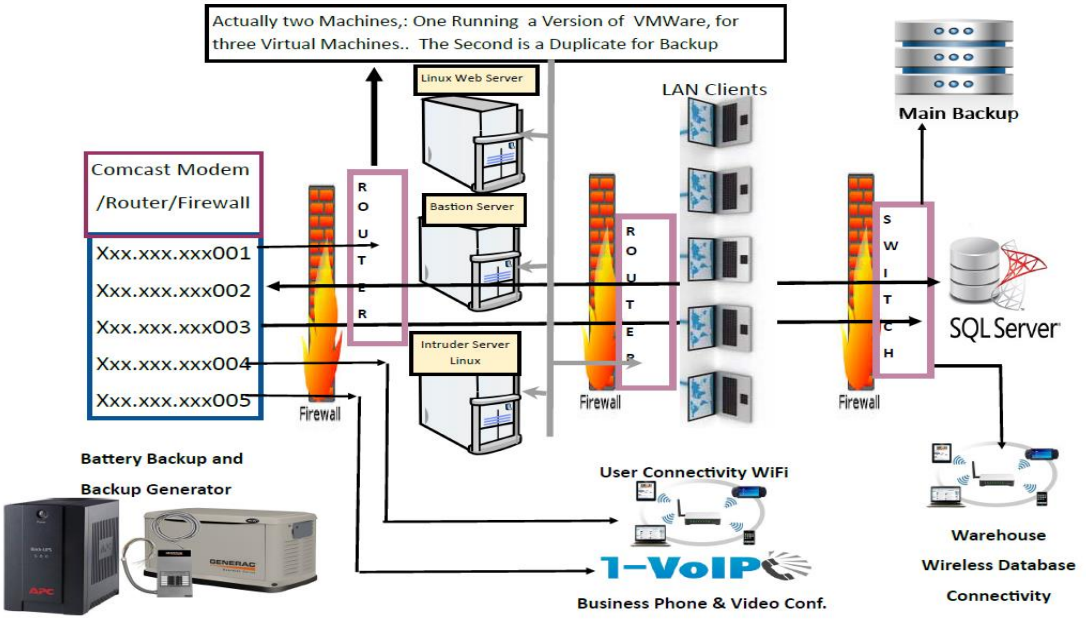
The Internet

When speaking of connectivity to the internet we have a few choices. Connectivity choices might include T1-T4 (direct high-speed telephone connections), Fiber Optics by SureWest, Comcast Cable, ATT DSL, and Succeed net Dialup or Microwave, and finally, HughsNet Satellite connections just to name a few. Such companies are referred to as ISP's or Internet Service Providers. If one has ever watched DirectTV in a storm one may attest to why Biggie's will not be using Satellite. Stability issues as well as it's price structure is a problem for business networks. Most Satellite connections are charged by the Gigabyte like cell phones with starting prices around $400. Microwave technologies are not only expensive but very limited in availability. Dial-up touts $19 per month, unfortunately, dial-up speeds are just too slow for today's high Mbps connections. This limits functionality greatly. Videos spend more time buffering than playing when using dial-up. DSL, though close, comes in at about $100 per month, but also has Gigabyte restrictions. Further, DSL still has some issues due to wire size as it uses the older telephone lines. T1-T4 are what most colleges use, however, this is very expensive at a price point as high as $1200 a month. This leaves fiber-optics and Comcast Cable for around $150 per month. The Cable Modem or Fiber-Optics model is the standard of choice. If Sure West or another company has an optical internet connection in the same price range as the cable modem this would be the better choice. Upload and download speeds are far greater; Bell is currently boasting Optical connections at 1000 Mbps upload and download speed compared to 10-60 with a standard cable modem (Bell, 2017). Unfortunately Optical is not available everywhere. For now, the standard cable modem from Comcast is the one Biggies will have. The price point is comparatively less than T1 lines at about $150--including the five IP addresses, the VoIP, unlimited data, and they include some hardware.

We will need static IP assignment, which is customary for businesses. Static means the IP address stays fixed. Most purchased connections are dynamic or can change at any time. To Biggies benefit, static IP's come in packages of five. As stated earlier, for security purposes, it is important to diversity these connections (Chowdhury, P. K. et al, 2007). External IP addresses (WAN) are assigned by Comcast to Biggie's Logistics. They will be assigned as follows:

- IP 001, port 80 and 437 for Internet web connections–Web Server, Bastion Server, Intruder Protection.
- IP 002 Logistic Web Based Data Interface–Data Base Web Portal, Network Wireless Connectivity for Logistics buildings, handheld inventory.
- IP 003 Routed nonpublic--VPN to Cloud, and Backup Servers.
- IP 004 Cell Phones and other Wi-Fi connectivity–Wi-Fi Interface for all employees.
- IP 005 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, and Firewall are all in one unit. Each of these will be explained as the paper progresses. All five Static IP connections come through the cable/optical cable connection.

Connection 001 is the primary Web Connection. After the Comcast firewall and router the cabling connects to the first external hardware firewall; to the Web Service Router; and then to two servers--each running VMware. Servers referred here as the actual physical machine, but it is important to understand that the term "Server" can be either hardware or software. Software servers can be run in a virtual environment. These are operating platforms, or software engines that control and oversee specific areas of the networking environment. VMware is an operating system like Windows, MacOSX, or UNIX which supports the installing of these "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 all three 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 to identify attempted attacks and non-privileged user penetration. Basically, this monitors all activity and then upon suspicious activity, it sends 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 to prevent employees from infecting the system by navigating to known attack sites. 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 and contains the WordPress Web-Site for the company. All three servers are running on the Linux platform. Each instance of Linux includes a software Unix Fire Wall (ufw) as well as iptable firewalls. So far 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 a "demilitarized zone" as it is heavily controlled.

A word about WordPress. In this technology plan, we have chosen to host our own web pages. This saves Biggie's money. Since the servers needed are already there it only makes sense to spend no further money in outsourcing. WordPress is a free dynamic and editable platform. PHP based, it remains on the cutting edge. WordPress is scalable and allows dynamic viewing of most any device (Borhani, 2014). We will purchase 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 the Biggie's owned 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 and to Biggie's Web Sever. Thus, the WordPress external site is brought up. WordPress can easily support portal login with Captcha security measures. Captcha is an area on the login page that requires one to type in a challenge code shown on the screen. This warts off machine (brute force) attacks. Dropbox connections for all employees who require them with secure drop box technologies by apple -- i.e. iCloud are also supplied through this IP.

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 (VPN) is a tunneling protocol that directly links two networks. While not activated at set-up this could be initiated easily later. If Biggie's scaled up in the future by purchasing another location activating this service would link the two networks as one. This is a great solution because internet connectivity is sidestepped--thus keeping the network security intact.

To add to this, a web-based VPN portal can be made available for employees for telecommute purposes is desired (Odiyo, 2011). By using a separate IP than the web page servers it is less likely to be hackers will have successful attacks. For now, this IP is assigned for LAN access to the Data Base tier.

The data server chosen is SQL. This is really the industry standard and easily runs on 802.x protocols. Further, money is saved by using the free version called MySQL without any security compromises. SQL and MySQL both run fine under Linux. The SQL server is behind the demilitarized zone. A demilitarized zone is a zone on the network between two firewalls (Nakamoto, 2011).

Choosing Linux over Windows Server also saves money due to the extensive charges employed by Microsoft. When using Microsoft Server one must pay a per-user fee--and they are not cheap. In an attempt to avoid virus's and malware system wide the choice is made to steer away from C+ compiled operating systems such as Window as they get compromised at a much higher percent compared to other operating systems. In this configuration, we have two hardware firewalls. After the first is the demilitarized zone. After the second hardware firewall the LAN connections. After a third hardware firewall, the heart of the business, the database server. This database server can connect to the LAN by way of the Ethernet or to handheld devices in the warehouses through a wireless router coming off of the last router. This WLAN is not open, but all appliances are paired through Mac addresses. For added security is a local SQL backup up the server. Other security measures hear will be addressed later in this paper.

IP 003 is nothing but a backup channel. Used only in VPN. This is for a cloud-backup and web page synchronization. Also backup of the website database, and business critical files. Synchronization of a clone of the web page on a host provider. The Names Service provider will

have these alternative addresses listed in case of failure or earthquake. The three resolving locations are 1. The in-house primary server 2. The in-house backup server 3. The cloud-based clone. 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. Phone services with voice mail, marketing, call waiting for each employee are easily setup. Fax lines and video conferencing all kept secure and separate from the LAN while at the same time supplying web-based access to voicemails, phone logs, phone books and more.

Workstations

To address communications a bit more we need to address our workstations. The workstations are all Apple based. For the most part, 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 also very hard to successfully infect with malware. To add to this, MacOSX is a brother to Linux and UNIX. This means that communication with servers will be less likely to fail. In addition, each computer has its own iCloud account with Apple included. Apple iCloud can be configured with two-tier access qualification making it almost

impervious to social hacking. This will allow employees drop boxes and centralized email services.

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 email address structure is User@BiggiesLogistics.com. Since Biggies is hosting its own web page and purchasing BiggiesLogistics.com access to service provided by the Name Service Provider makes this available. Since mail servers are the main source of temptations to hackers Biggies will not have a mail server in this configuration but instead will take advantage of DNS mail servers. Each employee will be set up with a forwarding from the Names Service provider to their employee iCloud mail account. Automatically User@BiggiesLogistics.com will forward User@BiggiesLogistics.com to User@iCloud.net. The mail app on each Mac-Mini is configured to collect mail from all sources just as Ms. Outlook does. Internally, private email is handled by WordPress Mailboxes, chat box, and video conferencing for each employee. It is possible to forward these emails to iCloud but not recommended for security purposes. Also provided are employee scheduling, timecards, and just about everything else, one can think of through the WordPress Employee Portal. However, it is recommended to use the VoIP for video conferencing as it is much more secure. It should be noted that iHome is free with the purchase of the MacMini's and iCloud accounts come free with the setup of iHome along with several other personal apps. 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. This is an option if everyone in the company needs access to the file. Otherwise, the use of Dropbox is recommended.

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. 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 already, 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 too expensive. 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 and can include encrypted channels if needed.

Protocol History

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. 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).

Tier One

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 direct 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 will be*** *WPA2-PSK (TKIP/AES)* which is a high-bred 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). This is the connection for employee cell phone and iPad etc.

Tier Two

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 and will be using ***WPA2-PSK(AES) security protocols***. Only specific mobile devices with unique static IP addresses and unique Mac address listed in the router will be recognized. By employing device profiles one can ensure that the wireless area is not hacked. As a result, each appliance will have to be setup and paired with the wireless network by the network administrator. By employing intelligent routing with device configuration all wireless devices can communicate securely.

Problem areas such as viewing area, browser capabilities, input methods, and storage capabilities are 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 availably at maximum. In addition, by having paired access only the network can remain closed to non-pair appliances. Confidentiality is a topic that will be addressed later in the training area further.

Security and Confidentiality

U.S. government contracts require campuses to have confidential data security throughout the campus, to implement countermeasures, and to actively take steps to 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. All of

these must be addressed in two areas. 1. Hardware, software, and data transmission. 2. Information as it relates to people—this we cover in training.

For hardware, software, and data confidentiality are handled by security layers. In Linux security is sub-grouped by layers. Layer one is encryption. XTS is an XEX-based mode encryption with cipher text stealing. It is 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 (TCP) and the 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. Also, the requirement of the Captcha on internet side WordPress portal logins is in place.

Integrity is handled in several different ways. For the LAN integrity is handled by the security measures already introduced such as the firewalls, demilitarized zone, and the intruder detection system to name a few. Further integrity is upheld by the fact that the LAN a closed wired system and the WLAN is by pairing MAC addresses and is not open to unpaired appliances. The last effort for integrity is the diversified IP addresses. If a hacker did break through the portal the IP for that portal is different than the IP for the LAN, this keeps network integrity. Lastly, authentication is handled by using WPA2 security protocols, as well as SSL. To add to this there will be additions to authentication security in the training area.

Non-repudiation is handled by the fact that all LAN and WLAN connection are assigned by Mac address. This gives the ability to "traceroute" to a specific IP which is assigned to a specific employee. In addition, the Intruder defense system will log external IP addresses and block attackers. DoS is handled in the same way. Denial of Service is generally a machine attack. This is blocked by Captcha, logged by Intruder systems, and dropped from IP tables. As a result, the offending IP address is blocked.

All this security is great but what is to stop someone from just waltzing in and walking off with a server? The server room and building must also be secure. Servers will be kept in a sound limiting double insulated room that is kept at temperatures suiting proper server function. Keyless entry lock systems will be installed that require an employee badge swipe and a unique security code. To add video surveillance will be installed. Only designated employees will have

access. In added security, every employee must swipe in and out at the security desk in order to enter the working area. Working area doors can be unlocked from the security desk by a "buzz" button. This system will not only keep track of who is on campus but will also double as a time clock. The backup server will store video surveillance and the SQL server will store door security events. The video will be held four weeks on the server. Door events should be held up to six months. Backups of video and events will be stored on DVD hard copy after the storage time elapses.

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 with Captcha; 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 following: MacOSX latest version, OpenOffice Suite which includes all the software that MS Office does free of charge, Chrome Browser (includes flash stock).

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 and would make HR risk management more difficult. Vfront is a form generating front end provider for SQL. Any forms not provided by the main data base front program can be created for inputting and searching data as well as for the generation of reports. Vfront is not free 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 meetings to determine format and information. Vfront is HTML or PHP based and is server side--off the web server. Lastly, SQL-leger is the main accounting front 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 steep. A major plus is that since it is SQL based any report lacking can be either created using Vfront, or straight from within MySQL itself. Primary database management functions can be handled by PHPMyAdmin or through a web port.

Dell PowerEdge T430 Tower servers or comparable will be utilized. Each server has dual quad processors, 2 TB storage, 16 gig ram and 2 Gigabit NICs. A fifth server 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 considered a different server and is equipped with 1. Web Control Panel. 2. Web Server with FTP server, and Vfront. WordPress will be loaded with WordPress Multi-site. The external web page and the internal

LAN Employee Portal are different WordPress pages off the multisite platform. 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, as well as external backups and synchronization.

Hardware Firewalls. While there is a firewall in the Comcast modem the firewall directly after the modem is the first line of defense for the demilitarized configuration and sits directly behind the modem on IP 001 this 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 installed, and the Web Servers have an additional two 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 pair the Wi-Fi connections to the mobile appliances needed in the warehouses. Each warehouse will have 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 do not 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 as well as 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.

Software Compatibility is an area that may need to be addressed. Since Biggies workstations are Mac/Apple some employees may need training on the MacOSX platform. At first, employees may experience a learning curve if an employee is accustomed to the PC/Windows environments. However, since one of the main requirements is security, and the prevention of inside as well as outside attacks is a reality there is need to leave behind the Windows Platform. Upper languages such as C++ (which is what Windows is written in) create open opportunities for would-be attackers. By using systems birthed from Unix scripting we severely limit the advent of Malware, virus's, and backdoors for hackers. Most all programs that are available for Windows are available for Mac. To add to this, if it is absolutely necessary MacOSX can emulate the Windows environment through programs such as Wine.

Personal computers will not be able to connect to the LAN through the network. Each appliance is assigned its connection through Mac addressing and unassigned appliances will not be allowed. By employing this standard all communications can be tracked to specific appliances. If there is an internal breach of security an administrator will easily trace the offending appliance to it's assigned, employee. Personal computers can connect to the Wi-Fi provided from IP004. This is a separate IP address for network outward bound connections and only accesses the internal network through the demilitarized zone.

Risk Management and Training

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. It is suggested that ongoing classes be a requirement. Learning how to properly use equipment is a stress relieving venture. Classes on OpenOffice and MacOSX, 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 in the event of failure. Though it may be possible to have one person wear several hats, too many hats on a single person is the wrong approach. In the case of sickness or other problems being stranded without someone knowing the system is all bad. In addition, accounting and bookkeeping will need classes in SQL-ledger, Vfront, and MySQL. Further, technicians that know how to replace Cat 5 cable ends, as well as replace internal computer hardware is a must when things fail.

Confidentiality, Integrity, and Authentication need to be addressed. Training about password protection is a great idea. Passwords are not to be written on paper or readily available. Additionally, passwords are never to be exchanged between employees. Employees are not allowed to work from workstations other than the ones assigned to them. Wireless appliances for warehouse use must be checked out and signed for. Each session will be logged under the employee which checked out the appliance. Passwords must be at least eight characters long with

Uppercase, lowercase, numbers, and at least one special character. Further, passwords will be changed every 3 months. Employees can also opt for fingerprint scanners in lieu of passwords.

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 align Biggie's for future scaling and progress. Gone are the times of flying three 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

Bell (2017) available packages http://www.bell.ca/Bell_Internet/Internet_access

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

Cisco (2006, August 10) IP *Addressing and Sub-netting for New Users*, http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

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.

Perkins, C. E. (Nov 2010) *IP Mobility Support*, RFC5944 WiChorus Inc. 3590 N. 1st Street, Suite 300 San Jose, CA 95134 USA, https://tools.ietf.org/pdf/rfc5944.pdf

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