Network Upgrade for B & B Manufacturing

Matthew J Rondel

Western Governors University

**Table of Contents**

[Summary 3](#_Toc134058461)

[Review of Other Work 5](#_Toc134058462)

[Changes to the Project Environment 8](#_Toc134058463)

[Methodology 11](#_Toc134058464)

[Project Goals and Objectives 13](#_Toc134058465)

[Project Timeline 16](#_Toc134058466)

[Unanticipated Requirements 17](#_Toc134058467)

[Conclusions 17](#_Toc134058468)

[Project Deliverables 18](#_Toc134058469)

[References 20](#_Toc134058470)

[Before and After Network Topology and Site Map 21](#_Toc134058471)

[Appendix B 22](#_Toc134058472)

[Network Inventory and Passwords 22](#_Toc134058473)

[Appendix C 23](#_Toc134058474)

[Notes and Samples of material covered in training session 23](#_Toc134058475)

# Summary

B&B Manufacturing is a medium-sized company of 275 employees located in Valencia, CA. The company consists of 5 adjacent buildings including administration, assembly, manufacturing, and maintenance. Their network is a combination of multi-supplier hardware that lacked standardization, and network separation and it included equipment that had been deemed end-of-life by the manufacturer. Since the Biden Administration had pushed to bring more manufacturing jobs back to America, the company had experienced unexpected tremendous growth. Due to this growth employees complained about slow connections to on-premise resources such as file stores and ERP systems. Along with this growth the company had also stated they want to replace an aging phone system with an IP-based one.

As a former employee turned managed service provider (MSP) I was hired to assist with documenting, proposing, standardizing, and upgrading the network infrastructure. This process included creating a network diagram of the current network infrastructure, discussing future needs with upper management and suggesting future expansion such as the desired IP phone system. Finally I then proposed and installed a solution that would provide them with a secure and reliable network with room for future growth.

Phase one of the project began with interviewing the on-site IT staff and upper management to determine the needs and expectations of the network, as well as discussing future growth of the company and IP phone system requirements. While these interviews took place, notes of the existing infrastructure were taken and a site survey was performed to confirm the locations of existing equipment.

Phase two of the project consisted of determining what equipment to replace and designing the network, including the new IP address schemes DHCP polls, and VLANS. Once the logical design was completed a list of equipment was created for each building and location. Once this list was finalized it was emailed to the purchasing department and the equipment was ordered.

Phase three began with receiving, verifying, and configuring the new equipment. The new hardware was powered up and was thoroughly tested. All ports, protocols, and services gathered from phase 1 were taken into account and access control lists were configured on the switches. Recommended Quality of Service (QOS) settings were configured on the equipment for the future phone system.

Phase four was carried out one building at a time beginning with the core of the network in Building 2’s main distribution frame (MDF), and then advancing to each intermediate distribution frame (IDF) within each building. Throughout this document, the main distribution frame (MDF) refers to the central connection point for each of the buildings to the rest of the network and IDFs refer to the smaller network closets within the buildings across the corporate campus. The justification for this method was that it reduced the possible downtime of each of the buildings and ease problem isolation that might arise and could be addressed without affecting the company as a whole.

Phase five was when the full switchover from the old equipment to the new equipment took place. Once all of the equipment had fully switched, over connectively tests were performed from both MDFs and IDFs to insure links were good. After these tests were concluded the old equipment was removed from their locations and returned to the IT department for disposition. Once the equipment was returned then the IT staff was trained on Cisco network basics and troubleshooting. After a monthly period of checking uptime with a rate of 98% of the network equipment and of the meeting project objectives, the project was deemed a success and concluded.

# Review of Other Work

Review 1

Using network segmentation is a must for any company doing business today. The “flat” networks of the past are no longer an adequate design when taking into account for security. In a white paper from Cisco they explain the benefits of network segmentation. They state that organizations gain several advantages when network segmentation is utilized. First, the attack surface is reduced. A flat network does nothing to prevent attackers from quickly exploiting their access and moving laterally once they have breached the perimeter.

Network segmentation prevents this lateral movement, limits insider threats, and can secure devices that may not support on-device security capabilities (such as IP-security cameras) by isolating them from the public internet. Ultimately, a layered network that has implemented segmentation represents a much more difficult target for attackers to navigate.

Performance and availability can be improved via network segmentation. Utilizing subnets results in fewer devices and resources on each segment. This makes it easier for network administrators to monitor and maintain quality of service for business-critical resources (such as VOIP systems). From a security perspective, attacks often display themselves as operational problems, so reducing the noise to a limited segment of the network can enable network and security teams to quickly determine if an availability issue is malicious and react quickly if it is.(Removing the Complexities from Network Segmentation, 2019)

Review 2

According to Cisco’s implementation guide on Quality of service (QoS) a typical network operates on a best-effort delivery basis, which means that traffic all traffic has equal priority and equal chance of being delivered in a timely manner. There are many specifics you need to take into consideration when configuring QoS on your network as Cisco suggests.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, a standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to occur closer to the edge of the network, so that the core switches and routers are not overloaded with this task.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the Diff-Serv architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control that you need over incoming and outgoing traffic.

By configuring the quality of service (QoS), you can provide preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput. (Quality of Service Configuration Guide, Cisco IOS XE Amsterdam 17.2.x (Catalyst 9300 Switches), 2022)

Review 3

Like the health care industry most machine shop equipment is still using devices running legacy operating systems because many devices cannot be updated, and purchasing a new device or series of devices may be prohibitively expensive. These devices run on unsupported versions of Windows operating systems, such as Windows XP or Windows CE mobile. Microsoft stopped support and security updates for Windows 7, Windows Server 2008, and Windows Mobile since January 14, 2020. These end-of-life operating systems are vulnerable and are the perfect vector for an attacker to exploit and possible gain full access to a company’s network and data.

In a white paper by Cynerio, an IT firm specializing in securing the health care industry states: Network segmentation divides a network into multiple parts, known as segments. Each segment acts as an isolated fragment of the network. If a corporate network is segmented discerningly, most traffic stays between devices and applications within each segment, with much less traffic crossing segment boundaries. Hence, segmentation improves network monitoring, performance, and security.

One of the most common ways to segment your network is using Virtual Local Area Networks (VLANs). VLANs operate at level 2 of the OSI model (the data link layer) and break down the physical network down into logical networks. VLANs can also be used to attain network segmentation for security purposes by applying access control lists (ACL) rules.

A large unsegmented network, such as B & B’s presented a large attack surface which is difficult to manage and protect. Applications and hosts in an unsegmented network have access to the entire network. As a result, attackers who gain access to a network can move laterally to access critical data and resources beyond their original entry point.

Network segmentation creates internal barriers, making it more difficult for attackers to penetrate the network and cause damage. Moreover, segmentation isolates sensitive data from malicious insiders to ensure that critical information does not fall into the wrong hands. (Network Segmentation for Hospitals: Challenges and Technology Solutions, n.d.)

# Changes to the Project Environment

During the phase 1 meetings with the IT department, it was estimated that the original network environment was installed in the late 1990s but it was long before any of the current staff members had started working there. During that time the company was much smaller and while it still occupied its 5 buildings most of them were used as equipment storage at the time. During the past year when the Biden administration wanted to bring more manufacturing jobs back to America. Funding to add more equipment started to come in and talent had to be acquired. More computer workstations were ordered and set up along with printers and shop floor terminals. Prior to the hiring surge the only recent network equipment that was added in the past was a company-wide Wi-Fi system and IP-based security cameras. This increase in employee demands on the network was causing the network to go down several times a week and thus causing a huge loss in productivity. During the walkthrough, it was discovered that all of the backbone parts of the network were unmanaged switches that did not allow any network separation or changes to their configuration. With the fact that the network was barely handling the new growth the mention of upgrading to a VOIP-based phone system would guarantee that it would not make the network perform better.

The original network environment was a flat network lacking IP segmentation and security. The problem with this setup is that if a broadcast packet is forwarded out from an end device in one building, then the broadcast packet would be sent to every other building and device connected to the network. One of the issues in the past the On-site IT staff mentioned is that they had experienced a network loop and had crashed the company network and taken it down for a few days. A network loop is caused when a patch cable gets plugged in from one network port directly to another. This causes packets to reflect back to the source which locks up the switch. Within the administration building (building 2) in the MDF there were 3 NETGEAR unmanaged 24 port JFS524 10/100 switches serving as the “core network”. The primary issue with this is that an unmanaged switch comes with a fixed configuration and does not allow any changes to its configuration.

Attached to these NETGEAR switches were a Linksys SRW2024 power-over-Ethernet (POE) switch connected to the IP cameras. This same switch had a cat 5 cable going underground via a conduit to building 3. On another of the NETGEAR switches there was a post-it note taped on both ends labeled “to building rear IDF”. On the lowest of the NETGEAR stack, a SonicWALL Firewall was found connected to the internet service provider’s modem. All of these connections were connected via 100 Mbps (megabits per second).

The rear of the building had contained the IDF and two more NETGEAR switches connected with (unmarked speed) Ethernet cable along with another Linksys POE switch for cameras. One of these NETGEAR switches had Ethernet cable going underground through the conduit to Building 1. In Building 1’s MDF there were three more NETGEAR switches along with one of the same Linksys POE switches. One of the NETGEAR switches went out to two IDFs and another went through the underground conduit to Building 4 and then to two IDFs within its building. Each IDF contained the same number of switches found in the MDF. Building 4 was a direct copy of Building 1 with the same number of devices in each IDF and MDF. Exploring Building 3, more NETGEAR and one Linksys POE were found along with a conduit to Building 5. Once again Building 5 contained the same quantity and manufacturer of switches all connected via the same speed Ethernet. Although this equipment was still functioning, the network was fully saturated and running at maximum capacity and could not keep up with the volume of devices and growth over the current year.

The new equipment had been installed in all buildings with significantly more speed than the former network had. All buildings were interconnected with redundant fiber connections so in the event one fiber connection failed the other would continue to pass traffic. Along with the new physical changes Virtual Area Networks (VLANs) were configured to separate traffic for cameras, guests, WI-FI, clients, and the new future phone system.

After the project was completed network stability was noticeable as the system just worked. Employees were able to browse folders in the network file shares and did not have to wait. Shop floor technicians were able to upload and download files with ease and didn’t have to worry about file corruption or network timeout.

# Methodology

As the project manager, I had chosen the waterfall methodology model as this is a well-defined project management methodology suitable with a clear goal that will not change. The waterfall model comprises of 6 phases: Requirements, System Design, implementation, Testing and Integration, Delivery and Deployment then Maintenance. This is a common model to follow with projects such as this it has sequential phases that begin when the preceding stage ends.

The requirements phase of the project was fulfilled by gathering relevant stakeholders from the company. These meetings discussed the current state of the network, past issues, the issues to overcome, and a plan for the future phone system. This phase set into motion the system design phase, where the information gathered, a new network design was developed to include the number of switches required, the performance of those switches, and how they would be configured.

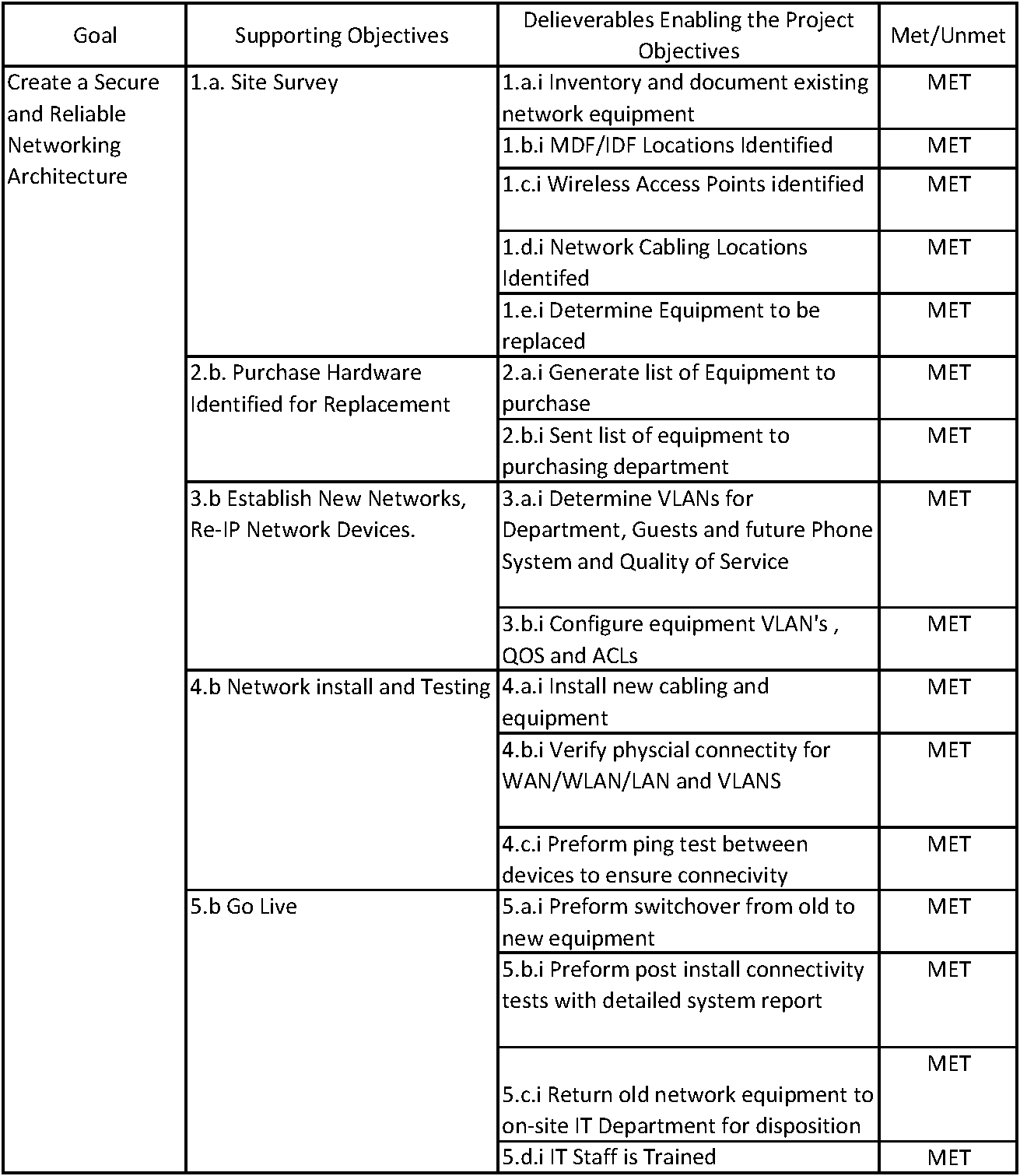
The system design phase consisted of taking into account the findings from the walkthrough and meetings with staff members. This information gathered on job functions and tasks along with the needs of day-to-day activities shaped both the VLAN and ACL system design. When the walkthrough was performed and observing the existing network and how it was utilized with the IP-based security cameras and observing how the buildings were interconnected established a need for redundant connections and integrated equipment.

The implementation phase commenced by the creation of an equipment list from the system design phase then ordering the equipment from the company’s preferred supplier. This equipment was delivered to the receiving department in building 2 and grouped according to the installation location. Once this equipment was received and added to the IT asset inventory, it was unboxed then configured according to its destination and adhering to network best practices according to Cisco.

The testing and Integration phase began by the installation of the new core switch in line with the current hardware and verifying connectivity with the existing firewall and internet. Once connectivity tests were successful, delivery and deployment phase began and new equipment was installed at each building’s MDF. New equipment was powered up and connected to the network backbone. Once connectivity with the core was established the endpoint devices such as printers and client computers were connected. After endpoint devices were verified, the next IDF was connected and repeated until each building was on the new network. Verification of endpoint devices included test prints, connecting to the internet, traceroute and ping, and verifying IP-cameras were recording, and shop floor terminals would connect to the MRP database.

Once all the devices were switched over to the new network and the delivery and deployment phase was complete this brought it to the maintenance phase. The original network had resembled the swamps of Dagobah with cables all over the walls ceilings and floor. Clean cable management is a key component of not just good airflow but also assists in easier troubleshooting when problems arise. All of the former networking equipment and cables were removed and new ones were labeled. Instead of using harmful Zip Ties Velcro straps became the only acceptable method of keeping cables together.

# Project Goals and Objectives



The primary goal of this project was to implement a secure and reliable networking architecture with room for future growth. The new network had VLANs for network separation throughout the manufacturing floor, maintenance, and administration, along with wireless separation for corporate visitors or suppliers who visit the facility. This network was also equipped with high-speed redundant fiber connections so in the event, if one of the lines fails then traffic will still pass through. Implementing VLANs and upgrading to fiber paved the way for the future phone voice-over IP-based phone system the company stated it had plans to install. This was the project’s primary goal consisting of five supporting objectives. The goal was met through the successful completion of the following five objectives:

Objective 1. a – Site survey. The first objective was to have a site survey conducted throughout the facility’s five buildings. Detailed notes were taken on the building’s MDF and IDF locations, what equipment was installed and how it was connected, and at what speed. During the site survey, all WI-FI access points were documented to determine how and where they were utilized. This was needed to determine how the existing network was used and where the problems reside. One of the primary problems with the original network environment was that it was a “flat” network with no IP security or IP segmentation. Therefore, the original environment of the network was deemed unsafe by modern standards and needed to be redesigned. This objective was met when an inventory of the existing network equipment was completed along with the documentation, labeling, and testing of all the cabling performed.

Objective 2. b. Purchase hardware identified for replacement. After the notes of the survey were taken and compiled, a list of what equipment to replace it with was generated and was sent to the purchasing department.

Objective 3. b. Establish new networks, Re-IP network devices and create new DHCP pools. After the last objective was completed and the equipment was received the next phase in this process was that a new network design had to be created for the company. The network design was created to be secure, redundant, and adhere to industry practices. The switches were configured with the new network scheme along with VLANs configured for data, voice, manufacturing, and a guest network. By following best practices recommended by the network equipment manufacturer Quality of Service (QoS) and Access Control Lists (ACLs) were configured for the future phone system.

Objective 4. b. Network install and testing. Fortunately for B & B, all of the MDF and IDF racks that contained the original equipment allowed for the new hardware to be installed alongside the old switches. This enabled both old and new to be running in tandem and allowed the new switches to be connected to the internet. Between each building there were an old set of Ethernet cables that was marked as “do not use” and this served as an easy method through which to pull the new fiber lines. As the new fiber was run and connected ping connectivity checks were completed by wired devices such as desktop computers and printers – both wired and wirelessly.

Objective 5. b Go live. The fifth and final objective was to go live by switching over to the new equipment. This switchover was performed by simply taking the fiber that was pulled throughout each building, connecting it then disconnecting the old. Once all of the new equipment was connected and all of the lights were green, detailed connectivity checks were performed to insure connectivity was good.

Once all the connectivity checks were completed and confirmed. All of the old network equipment was removed and returned to the IT department for disposition. After the equipment was returned a meeting was set up for a two-hour training with the IT department on networking troubleshooting and basics. This objective was met when the two-hour training session with employees was completed.

# Project Timeline



The original project timeline was started on 1/20/23 and started on time as planned. Once the project kickoff meeting had concluded site survey and taking an inventory of the existing equipment took place on the same day. There were no significant delays in the project until the cable installation took place. During this time it was discovered that one of the lines connecting two of the buildings was damaged and had to be dug out and repaired and concrete had to be poured and set. As a result, this delay caused the project to slip while this line was being unburied and worked on. While this work was taking place all cables that needed to be installed and everything was put in place so when the last piece of the milestone could be completed it could move right to the next. A second delay did occur but did not cause any minor delay. While a phone call was made to their service provider about a planned outage they mentioned how the company was experiencing a network upgrade and the service provider noted a free upgrade to support the new bandwidth. While work was still in wait on the concrete company the service provider sent out a technician and installed the new equipment. These delays all lead to a total of 14 days of delay to the project.

# Unanticipated Requirements

During this project, two obstacles caused the project to take longer than expected. The first was discovered during fiber installation between buildings 2 and 3. During this phase, it was discovered that the ground conduit had collapsed and the cable could not be pulled through. To rectify this, the concrete had to be removed, the conduit line repaired then new cement poured. This damaged conduit caused a delay in the project by 2 weeks because the cabling was over a frequently used driveway.

The second unanticipated requirement occurred when the circuit and ISP modem had to be upgraded to support the new bandwidth needs of the company, otherwise, this would be a choke point in the network. Since this was discovered during the beginning of the installation phase this did not affect the schedule as this upgrade took place at the same time. As for the circuit and modem upgrade, this was at no cost to the customer as this was included with their business internet plan.

# Conclusions

When implementation was complete, B & B Manufacturing had a stable reliable, and redundant network. Employees no longer had trouble logging in or accessing network resources. The success of this project was determined by the positive and helpful response from the administrative and on-site IT staff. A major determining factor of the success of this project is that not a single network crash or slowdown – even during peak business hours- had occurred since the installation of the new equipment. Administrative staff commented on how the network shares did not “pause “or “hesitate” when opening frequently used folders like before. Tool crib and shop floor attendants commented on how quickly and more responsive the system preformed.

The network upgrade project was vital to prevent unreliable connectivity issues from occurring throughout the manufacturing floor. This new network allowed manufacturing employees to sign off on jobs to move them further down the assembly line without dropouts or freezes. It also helped the shipping department which relied on the wireless network to scan finished boxes for UPS shipments. As for suppliers and visitors, the new integration of VLANs helps keep the company network safe from any possible risks from unmanaged devices. When the time comes for the company to select and install the VOIP equipment provider they will be confident the network is ready for whomever they choose. I followed up with the IT department once a week for a month to verify that the network is functioning and performing as expected. This project was considered a success when the network had maintained an uptime (using the show version command) of 98% for a week over the course of the month with random sampling made across distinct switches.

# Project Deliverables

Appendix A contains before and after logical network diagram. Included in the diagram are the switch model, connection rates between the switches, and if the link is Ether channel (a fiber redundant pair).

Appendix B contains the list of hardware, hostnames, model numbers, and passwords that was given to the IT department. This document along with IP addresses, VLAN configurations, and configurations was stored in a fireproof safe in the IT department’s office.

Appendix C contains a small sample of the training material and notes used for the training session on network basics, material such as: How to update the Cisco operating system software (IOS), how to create backup files of the running configurations and how to create user accounts and change the default passwords.

# References

Grady, J and Oltsik, J (2019, October) Removing the Complexities from Network Segmentation

ESG White Paper Retrieved 5/1/2023, from

https://www.cisco.com/c/dam/m/en\_us/solutions/enterprise-networks/removing-the-complexities-from-network-segmentation/pdf/ESG-White-Paper-Cisco-Oct-2019.pdf

Cisco (2022, February 9) Quality of Service Configuration Guide, Cisco IOS XE Amsterdam

17.2.x (Catalyst 9300 Switches) Retrieved 4/22/2023, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-2/configuration\_guide/qos/b\_172\_qos\_9300\_cg/configuring\_qos.html

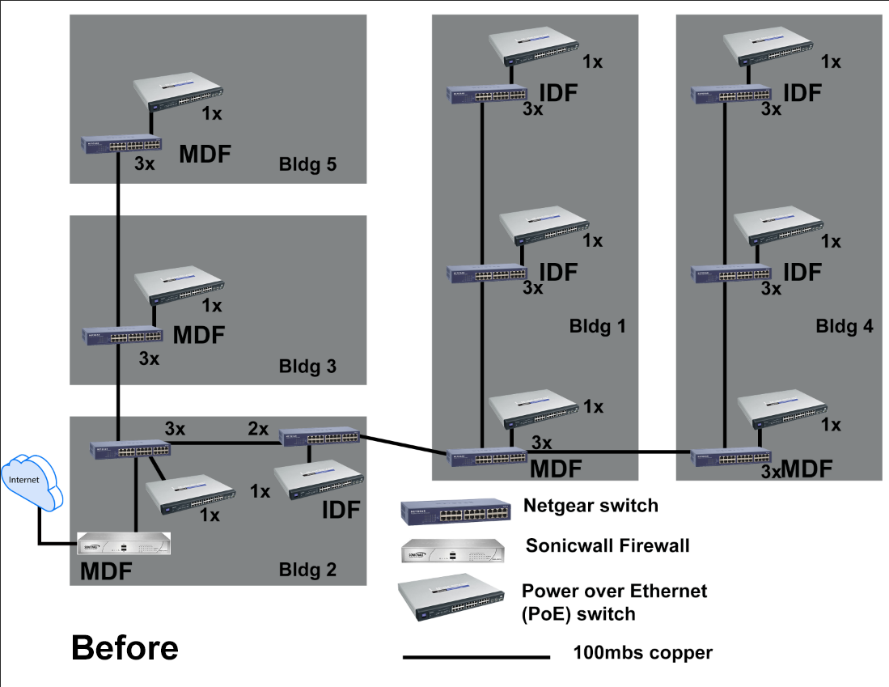
White Paper: Network Segmentation for Hospitals. (n.d.) Cynerio Retrieved 4/19/2023, from

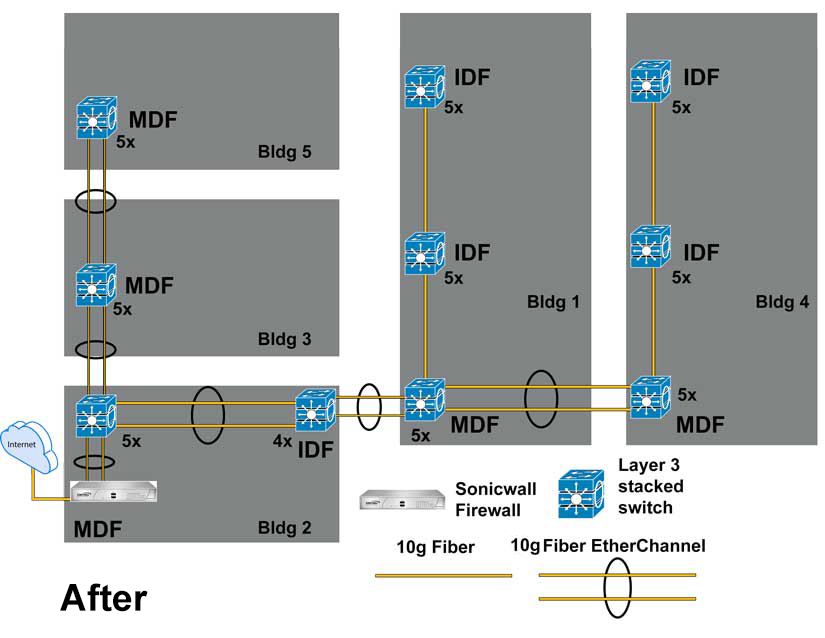
https://www.cynerio.com/white-paper-network-segmentation-for-hospitals

**Appendix A**

# Before and After Network Topology and Site Map

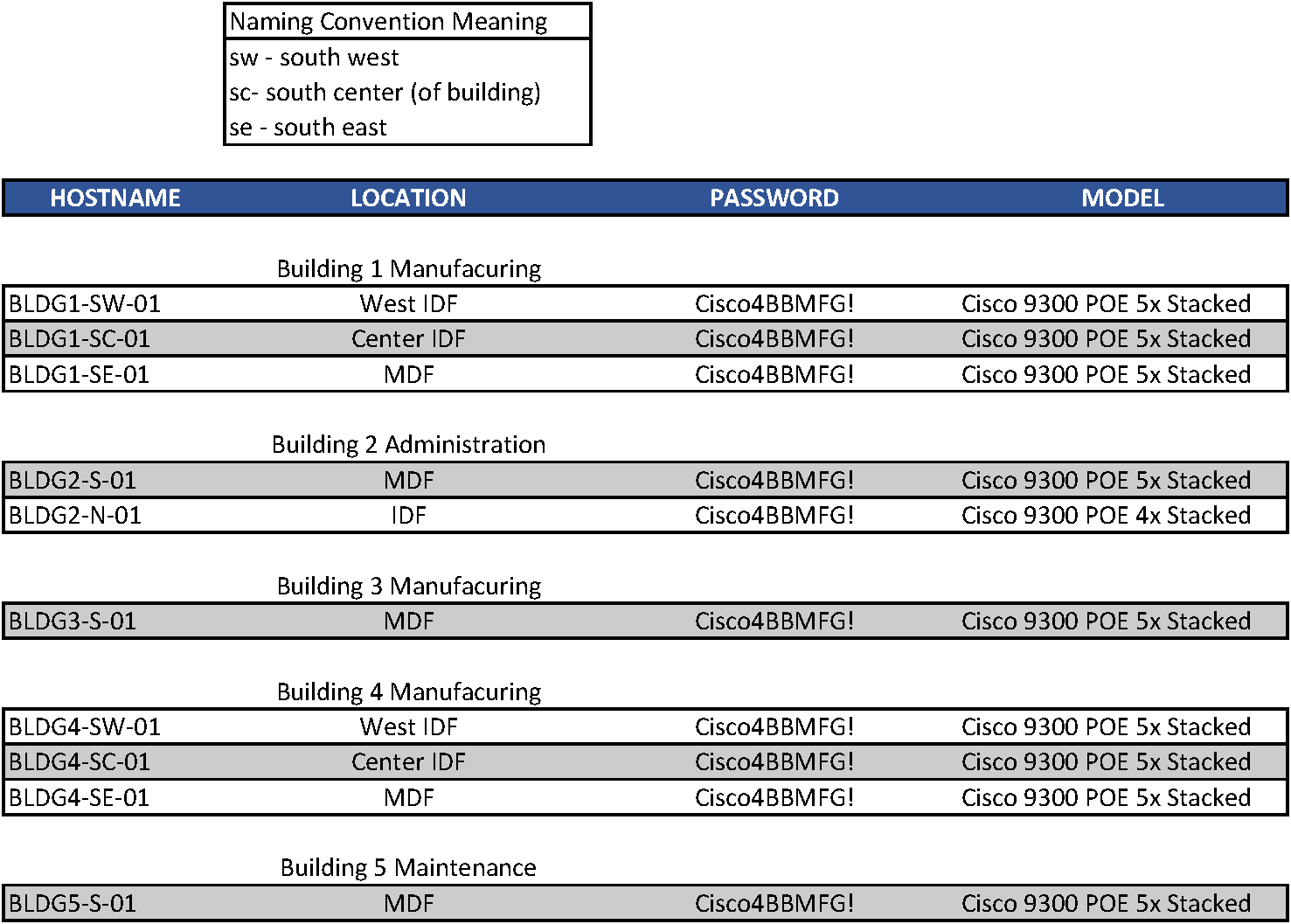
Appendix A contains a before and after network topology diagram and site map. Included in the diagram are the switch model, connection speeds between the switches, and if the link is port channel (redundant pair). The notes on how the network changed throughout the project are included for points of reference.





# Appendix B

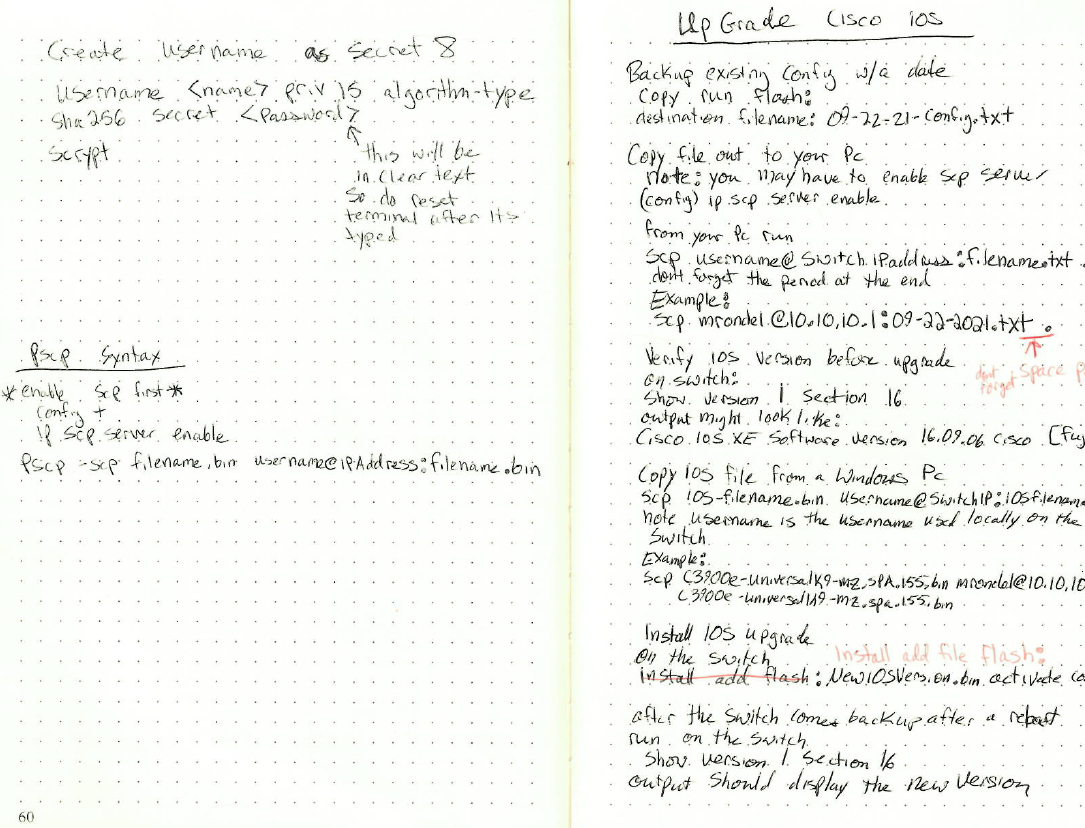
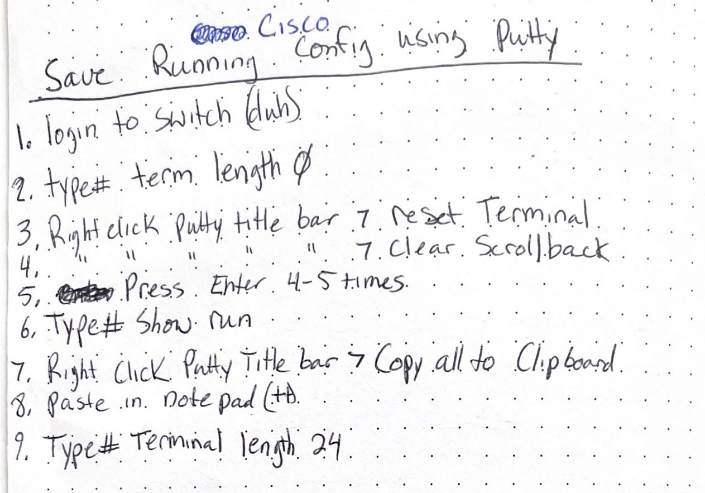
# Network Inventory and Passwords

Below is the list of hardware, hostnames, model, and passwords that was given to the IT department. This was the document stored in their fireproof safe. Note that this was the default password used on the devices part of the training was showing them how to change these passwords to what they prefer.  


# Appendix C

# Notes and Samples of material covered in training session

Below are notes and sample of materials covered training session with IT department. Topics included were saving configurations using putty, how to upgrade the firmware, the OSI and applying it to troubleshooting.

**  
**