Network Upgrade for B & B Manufacturing

Matthew J Rondel

Western Governors University

[Summary 3](#_Toc133113964)

[Review of Other Work 4](#_Toc133113965)

[Changes to the Project Environment 7](#_Toc133113966)

[Methodology 10](#_Toc133113967)

[Project Goals and Objectives 12](#_Toc133113968)

[Project Timeline 14](#_Toc133113969)

[Unanticipated Requirements 15](#_Toc133113970)

[Conclusions 16](#_Toc133113971)

[Project deliverables 16](#_Toc133113972)

[References 17](#_Toc133113973)

[Appendix A 18](#_Toc133113974)

[Updated network topology diagram and site map 18](#_Toc133113975)

[Appendix B 19](#_Toc133113976)

[List of network equipment, and hostnames 19](#_Toc133113977)

# 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 mix of multi-vendor hardware that lacks standardization, and network separation and it includes equipment that has been deemed end-of-life by the manufacturer. Since the Biden Administration has pushed to bring more manufacturing jobs back to America, the company has experienced tremendous growth. Due to this unexpected growth employees complained about slow connections to on-premise resources such as file stores and ERP systems. Along with this growth the company has 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 technology with upper management and on-site suggesting future expansion such as the desired IP phone system, then proposing and installing 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 what equipment was needed for each building and location. Once this list was complete 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 equipment was powered up thoroughly tested 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 switches for the future phone system.

Phase four was carried out then one building at a time beginning with the core of the network in Building 2’s main distribution frame (MDF) and then progressing to each intermediate distribution frame (IDF) within the 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 minimized the 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 is when the full switchover from the old equipment to the new equipment took place. Once all of the equipment was 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 how to troubleshoot and network basics.

# Review of Other Work

Review 1

Network segmentation improves security by controlling the flow of data between different networks. This is most commonly accomplished with virtual local area networks (VLANs). They should be implemented within all networks including home, business, and the internet. Effective network security requires the protection of wired and wireless networks with firewalls, anti-malware software, intrusion detection systems, access control, and more. Trend Micro, global cybersecurity recommends (Trend Micro, 2023)

Review 2

Technology standardization is the process of positioning your applications and IT infrastructure to a baseline of standards that fit your business strategy, security policies, and goals. Standardized technology reduces complexity and offers benefits such as cost savings through economies of scale, ease of integration, improved efficiency, and better IT support. It also simplifies your management of IT.

Not every company’s IT needs to look the same. Some companies have internal IT departments, some have managed IT service providers, and some even have a combination of both. No matter how your IT department is structured, having the most standardized systems allows for your IT providers to work quickly and efficiently. It ultimately creates a better work relationship with your IT provider. It ends up being a win-win for everyone. Your IT provider can address and fix problems quickly and give you the results you desire. (Importance of IT Standardization Biz Technology Solutions, 2023).

Some people think it’s risky to work with one vendor, but we felt confident moving toward our single-vendor integration with Cisco. Cisco offers a wide range of high-quality solutions with high interoperability, we can get support in every country where we operate, and they offer transparency of documentation and certification. They are leaders in networking, and they are constantly working to improve solution functionality. (Boksan, 2022)

Review 3

Flat networks provide fast and reliable connectivity for all connected devices, and security efforts generally concentrate on isolating internal networks from external networks. This traditional approach, however, is no longer satisfactory to securing modern enterprises' complex web of interconnected systems and organizations. Flat network architecture has led to high-profile cybersecurity incidents like the WannaCry ransomware attack and breaches at large financial services firms.

The National Institute of Standards and Technology (NIST) defines network segmentation as "splitting a network into sub-networks...by creating separate areas on the network which are protected...to reject unnecessary traffic. Network segmentation minimizes the harm of malware and other threats by isolating it to a limited part of the network."

Network segmentation is a powerful but underutilized security measure, and it is one of the cornerstones of a successful information security program. It directly addresses the reality of today's threat landscape--that you cannot prevent a cyber breach, but you can isolate one. (Kambic and Fricke, 2020)

Review 4

Aneurin Bevan University Health Board (ABUHB), a network of hospitals in Wales serving multiple areas with two-thirds of the staff directly involved in patient care.

We are currently in the middle of a digital transformation to bring patient care closer to home. We aim to treat patients at the nearest hospital or resource centre (sic) in their area or dispatch healthcare workers to assist them in their homes. To do this, we'll use IoT, remote monitoring, and mobile solutions that will enable people to get the healthcare they need where they are, thus limiting the number of patients that have to travel to one of our hospitals. This approach is not only cost-effective but also provides a superior patient experience (Mahoney, 2020).

With new regulations coming into effect to better protect user privacy and protect against cyberattacks they turned to Cisco.

We wanted to standardise (sic) our network equipment, and network security, and be able to provide greater assurance from a trusted vendor. As ABUHB's head of ICT, it was up to me to find the perfect partner, and the top name on my list was Cisco (Mahoney, 2020).

At first, when they started talking with Cisco the case didn’t stack up but over time once Cisco understood the scale of their initiative they were on the same page. They started with a refresh of LAN and WI-FI at two of the hospitals then moved onto IT and telephony networks across all other sites.

Cisco DNA Center is the core of our network refurbishment process. It has taken us from manually configuring and managing individual switches and switching ports to working with a visual, rules-based engine. Cisco DNA Center allows us to install any physical device and configure it remotely using a single pane of glass. We had to install and configure 250 Cisco Catalyst 9500 and 9300 Series Switches alone at Grange University Hospital, and it would have taken days, if not weeks, to set them up by hand. (Mahoney, 2020).

In addition, they have adopted Cisco Unified Communications Manager (UCM) as their IP telephony service for all of their locations

Cisco had given them the tools to create a robust and reliable network and built a solid foundation that will accelerate the digital transformation of their patient services for years to come.

# Changes to the Project Environment

During the phase 1 meetings with the IT department, it was estimated that the existing network was sometimes installed in the late 1990s but it was long before any of the current staff members had started working there. During this 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 this 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. The only network equipment that was added in the past few years was a company-wide Wi-Fi system and IP-based 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 current network design was a flat network with no IP segmentation or security. The problem with this setup is that if a broadcast packet is sent out from an end device in building 1 then a broadcast packet is sent to every building and network 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 the packets to reflect the source which locks up the switch. They had a very fundamental setup. Within Building 2, in the MDF there were 3 NETGEAR unmanaged 24 port JFS524 10/100 switches serving as the “core network”. An unmanaged switch comes with a fixed configuration and does not allow any changes to its configuration.

Attached to these NETGEAR switches was 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 contained the IDF and inside contained two more NETGEAR switches connected with category 5 cable along with another Linksys POE switch for cameras. One of these NETGEAR switches had a cat 5 cable going underground through the conduit to Building 1. In Building 1’s MDF there were 3 more NETGEAR switches along with 1 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 1 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 capacity and could not keep up with the volume of devices and growth over the current year.

The new equipment was 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 VLANs (Virtual Area Networks) 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 choose the waterfall methodology model as this is a straightforward, well-defined project management methodology suitable with a well-defined goal that will not change. The waterfall model consists 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 clearly defined stages that begin when the preceding stage ends.

The requirements phase of this project was satisfied by gathering relevant stakeholders from across 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 led directly into the system design phase, where based on the information gathered, a new network design was developed to include the number of switches needed, the performance of those switches, and how they will be configured.

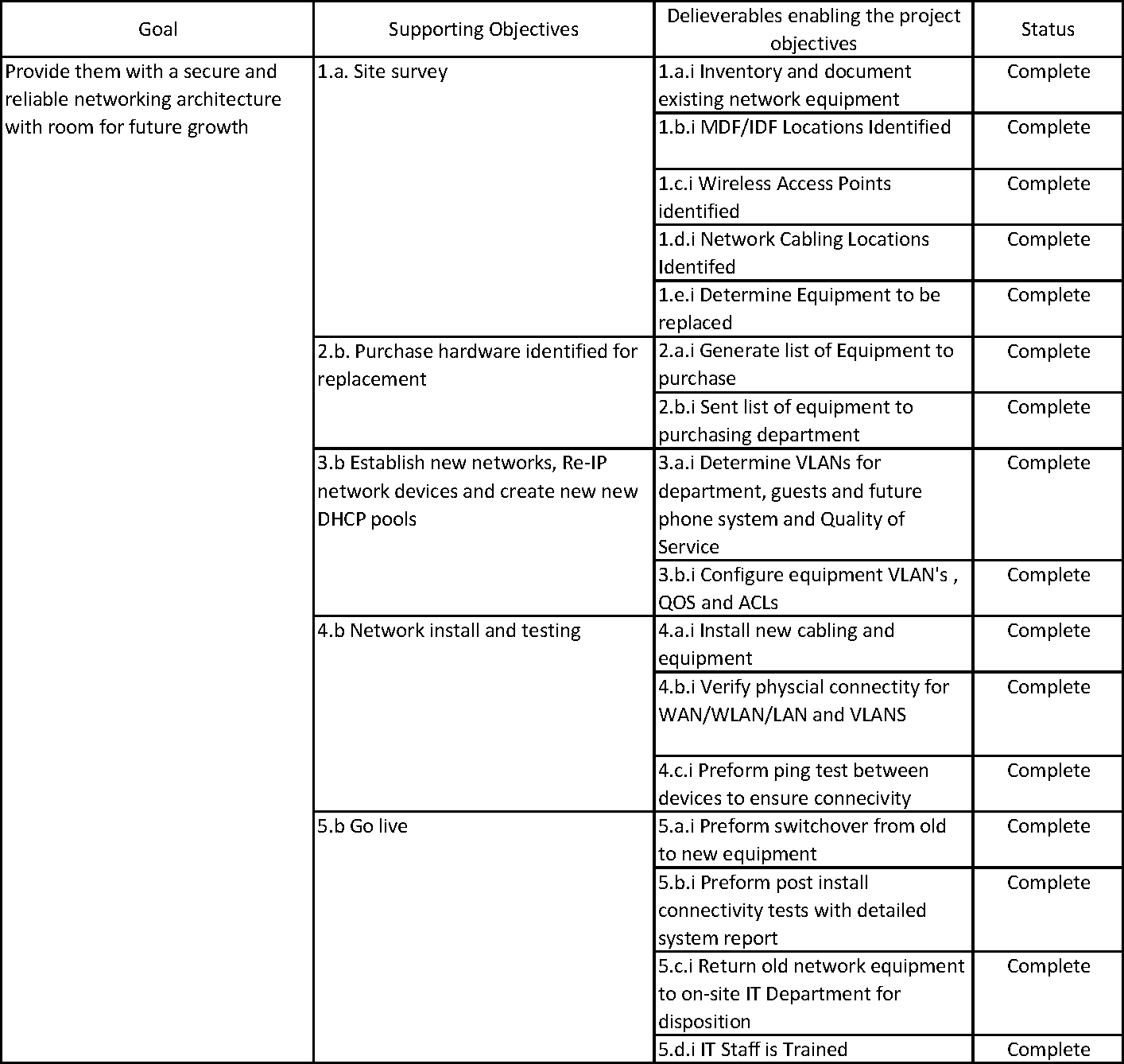
The system design phase consisted of taking into account the findings from the walkthrough and meetings with staff members. This information gathered on job functions and tasks along with the needs of day-to-day activities shaped both the VLAN and ACL system design. When the walkthrough was performed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

The implementation phase began by generating a list of equipment needed from the system design phase and 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 and configured according to the destination and network best practices according to Cisco.

The testing and Integration phase began by installing the new core switch alongside the current hardware and verifying connectivity with the existing firewall and internet. Once connectivity tests were successful delivery and deployment phase commenced 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 us to the maintenance phase. The former network 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 now has Virtual area networks (VLANs) throughout the manufacturing floor, maintenance, and administration, along with wireless separation for corporate visitors or suppliers who visit the facility. This network is also equipped with high-speed redundant fiber connections so in the event, one of the lines fails traffic still passes through. Implementing VLANs and upgrading to fiber paved the way for the future phone voice-over IP-based phone system the company stated it has 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 main problems with the current network was that it was a “flat” network with no IP security or IP segmentation or VLANs. Therefore, the current design of the network was not needed and thus needed to be redesigned. This objective was met when an inventory of the existing network equipment was complete 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 sent to the purchasing department.

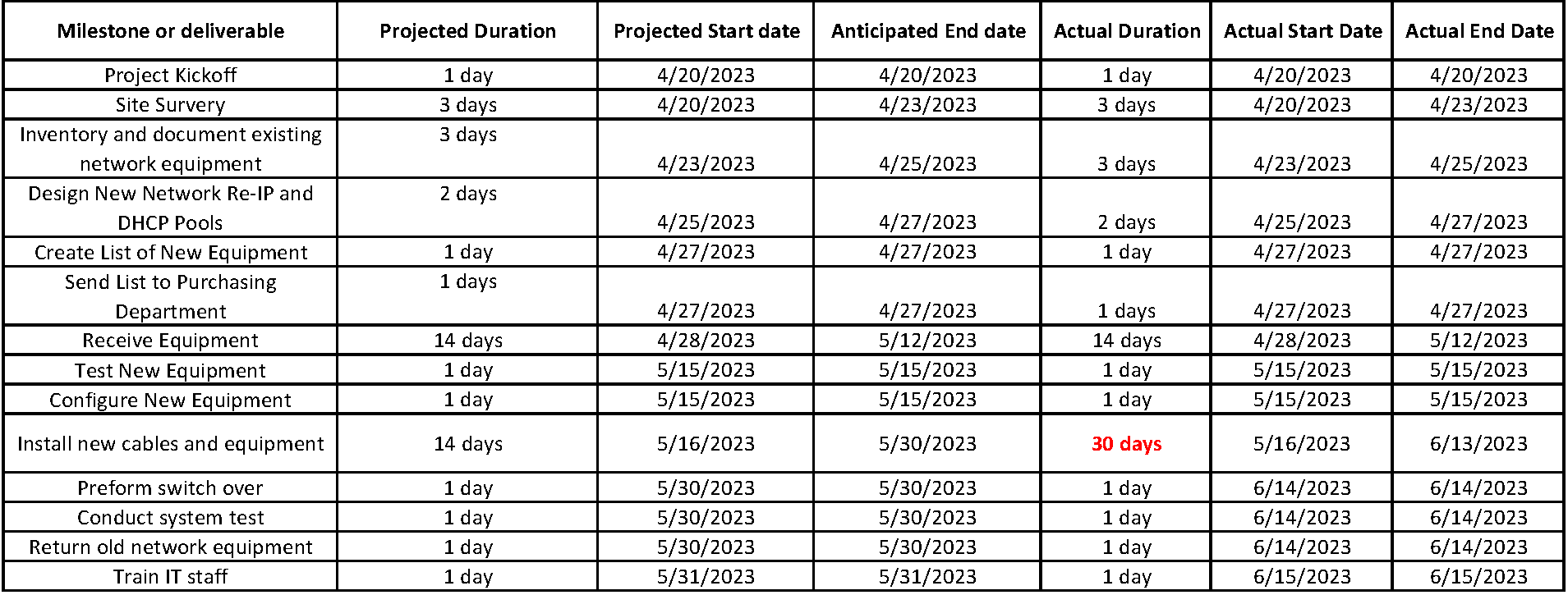
Objective 3. b. Establish new networks, Re-IP network devices and create new DHCP pools. After the last objective was completed and the equipment was received the next step in this process was to create a new network design for the company. This network design was created to be secure, redundant, and 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 existing equipment allowed for the new equipment 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 was 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 to start on 4/20/23 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 signing 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 “hesitate” when opening frequently used folders like before. Shop floor and tool crib attendants commented on how quickly and more responsive the system felt.

# Project deliverables

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

Appendix B is the list of network equipment and hostnames. Both of these documents along with IP addresses, VLAN configurations, and passwords was stored in a fireproof safe in the IT department’s office.

# References

Mahoney, M (2020, November 25) *Using Cisco Software-Defined Access to Deliver Patient Care Faster*.

Upshot by Influence. Retrieved March 10, 2023, from

https://upshotstories.com/stories/using-cisco-software-defined-access-to-deliver-patient-care-faster

Trend Micro (2023). *What are Network Security Basics?* Retrieved March 17, 2023, from

https://www.trendmicro.com/en\_us/what-is/network-security/network-security-basics.html

Biz Technology Solutions (2023, September 29) *Importance of IT Standardization* Retrieved March 9,

2023, from https://biztechnologysolutions.com/importance-of-it-standardization/

Kambic, D and Fricke, J (2020, October 19) *Network Segmentation: Concepts and Practices.* SEI Blog

Retrieved March 13, 2023, from https://insights.sei.cmu.edu/blog/network-segmentation-concepts-and-practices/

# Appendix A Updated network topology diagram and site map

# Appendix B List of network equipment, and hostnames